



MDev DPIA

A Data Protection Impact Assessment Framework for Medical Device Software Developers for Meeting GDPR Security and Privacy Requirements in the Internet of Medical Things

Ceara Treacy, B.Sc. (Hons), M.Ed., HDip

Dundalk Institute of Technology

Department of Visual and Human-Centred Computing

Supervised by:

Prof. Fergal Mc Caffery

Dr John Loane

Ph.D.

April 2022


Declaration

Declaration

We, the undersigned declare that this thesis entitled MDev DPIA - A Data Protection Impact Assessment Framework for Medical Device Software Developers for Meeting GDPR Security and Privacy Requirements in the Internet of Medical Things is entirely the author's own work and has not been taken from the work of others, except as cited and acknowledged within the text.

The thesis has been prepared according to the regulations of Dundalk Institute of Technology and has not been submitted in whole or in part for an award in this or any other institution.

Author Name: Ceara Treacy.....

Author Signature: .....

Date: 20/09/2023.....

Supervisor Name: Prof. Fergal McCaffery.....

Supervisor Signature: .....

Date: 20/09/2023.....

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisors, Professor Fergal McCaffery and Dr. John Loane. You both have provided an abundance of patience, support, and encouragement throughout this project. Without your guidance, persistence and generosity of time this project would not have been completed. Thank you!

I would like to thank my two children, Thomas and Pierce, my heart and sources of eternal joy. Thank you for your support, cups of coffee, and hugs. I want to acknowledge your patience and everything you have missed out on to provide me space and time to complete my studies. I love you both.

Thank you also to my parents, Gerry and Ann, for always stepping in when needed and their endless support with all that I decide to do, wise and unwise. Thank you, dad, for all the delicious dinners and bread. I would also like to thank my sister Theresa for standing in as a second parent, always having a generous listening ear and urging me along with cheer and laughter. Thanks to my eternal friends Fiona and Nicki, for all they have done and will do, big love. Thank you to my sisters Niamh and Ger, and my brothers Kevin and Ryan, for their encouragement and support. I am thankful to Fiona and Kevin who took time to review parts of this thesis.

A big thanks also to my DkIT colleagues, past and present, for their advice, support and not taking everything so serious all the time.

Finally, I would like to thank STATSports, and particularly the CSA, SD2 and SD1 who took part in this research, for all their invaluable input and feedback. Thank you, Dr. Kim Wuyts, for sharing your knowledge, experience and time. I would also like to thank the industry experts and SME who provided invaluable feedback during this project. Lastly, I am grateful to Lero - the Irish Software Engineering Research Centre – for providing me with research funding.

Table of Contents

Declaration.....	i
Acknowledgements.....	ii
Table of Contents.....	iii
Table of Figures.....	x
Table of Tables.....	xiv
Abstract.....	xvi
Related Peer Reviewed Publications.....	xvii
Document Map.....	xviii
Part 1 Study Background.....	1
1 Introduction.....	2
1.1 Overview.....	2
1.2 Research Problem Defined.....	4
1.3 Research Context.....	5
1.4 Towards A Data Protection Impact Assessment Framework for Medical Device Software Developers for Meeting GDPR Security and Privacy Requirements in the Internet of Medical Things – MDev DPIA.....	7
1.4.1 Step 1.....	9
1.4.2 Step 2.....	11
1.4.3 Step 3.....	11
1.4.4 Step 4.....	13
1.4.5 Step 5.....	13
1.4.6 Step 6.....	14
1.5 Research Questions and Objectives.....	14
1.6 Research Approach.....	17
1.7 Research Contributions.....	20
1.8 Document Structure.....	23
2 Literature Review.....	24
2.1 Introduction.....	24

Table of Contents

2.1.1 The Internet of Medical Things (IoMT)	27
2.1.2 Data Flow.....	28
2.1.3 Data Security and Privacy in the IoMT	32
2.1.4 Summary.....	39
2.2 Requirements for Security and Privacy in the IoMT	40
2.3 Challenges for Developers Implementing Security and Privacy in the IoMT	45
2.4 General Data Protection Regulation (GDPR)	48
2.4.1 Data Protection Impact Assessment (DPIA)	51
2.5 Standards for Data Security and Privacy.....	54
2.5.1 AAMI TIR57:2016 Principles for Medical Device Security - Risk Management	56
2.5.2 ISO/IEC 27005:2018 Information technology - Security Techniques - Information Security Risk Management.....	58
2.5.3 ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework.....	59
2.5.4 ISO/IEC 27701:2019 Privacy Information Management System (PIMS) Standard	60
2.5.5 ISO/IEC 27033-3:2010 Information technology - Security Techniques - Network Security Part 3: Reference networking scenarios - Threats, Design Techniques and Control Issues	60
2.5.6 ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications.....	61
2.5.7 ISO/IEC 27034:2011+ - Information technology - Security techniques - Application Security	61
2.5.8 Summary.....	64
2.6 Introduction	65
2.7 Threat Modeling for Software Development	65
2.7.1 STRIDE	66
2.7.2 LINDDUN	67
2.7.3 NIST SP 800-30 Revision 1	68
2.8 Existing Frameworks.....	69
2.8.1 Process for Attack Simulation and Threat Analysis (PASTA).....	69
2.8.2 IEC 80001-2-2:2012 - Guidance for the Communication of Medical Device Security Needs, Risks and Controls	71

Table of Contents

2.8.3 IEC/TR 80001-2-8:2016 Application of risk management for IT-networks Incorporating Medical Devices — Part 2-8: Application guidance — Guidance on Standards for Establishing the Security Capabilities Identified in IEC 80001-2-2.....	73
2.9 Security and Privacy Controls.....	75
2.9.1 NIST SP-800-53 Rev.5:2020.....	76
2.9.2 ISO/IEC 15408-2:2008.....	78
2.9.3 ISO/IEC 15408-3:2008.....	79
2.9.4 IEC 62443-3-3:2013.....	81
2.10 Summary and Conclusion.....	81
Part 2 Research Methodology.....	85
3 Research Methodology.....	86
3.1 Introduction.....	86
3.2 Epistemology/Ontology Approach - Constructionism.....	88
3.3 Research Philosophy Approach - Pragmatism.....	88
3.4 Research Approach - Deductive and Inductive.....	89
3.5 Methodological Choices - Qualitative.....	89
3.6 Research Strategy - Action Research.....	89
3.6.1 Conditions Required for Action Research.....	91
3.6.2 Canonical Action Research.....	92
3.6.3 Diagnosing.....	94
3.6.4 Planning.....	96
3.6.5 Action Taking.....	97
3.6.6 Evaluating.....	98
3.6.7 Report Research Results.....	99
3.7 Time Horizon – Cross-Sectional.....	99
3.8 Techniques and Procedures Choices.....	99
3.8.1 Introduction.....	100
3.8.2 Questionnaire.....	100
3.8.3 Focus Groups and Semi-Structured Interviews.....	103
3.9 Methodology Approach Summary.....	106
3.10 Research Quality.....	108

Table of Contents

3.10.1	Reliability.....	108
3.10.2	Internal Validity	109
3.10.3	External Validity	111
3.10.4	Construct Validity.....	111
3.11	Summary	112
Part 3 Development and Validation of the Framework		113
4	Development of the Framework	114
4.1	Overview	114
4.2	Introduction	114
4.2.1	The SME and Background to the Software System	118
4.3	Cycle 1 – Defining the problem	120
4.3.1	Appreciate the Problem	121
4.3.2	Study Literature and Expert Advice	123
4.3.3	Develop the Framework	127
4.3.4	Evolve the Framework.....	129
4.3.5	Action	130
4.3.6	Evaluate Experience	131
4.3.7	Assess Usefulness	132
4.3.8	Report Research Results	133
4.4	Cycle 2 – GDPR Requirements.....	134
4.4.1	Appreciate the Problem	135
4.4.2	Study the Literature & Expert Advice	136
4.4.3	Develop Framework Aspect	136
4.4.4	Evolve the Framework.....	138
4.4.5	Action	140
4.4.6	Evaluate Experience	140
4.4.7	Assess Usefulness or Exit.....	142
4.4.8	Report Research Results	143
4.5	Cycle 3 – Framework Properties and Risk Assessment.....	144
4.5.1	Appreciate the Problem	145
4.5.2	Study the Literature & Expert Advice	146
4.5.3	Develop Framework Aspect	147
4.5.4	Evolve the Framework.....	153

Table of Contents

4.5.5 Action	157
4.5.6 Evaluate Experience	158
4.5.7 Assess Usefulness or Exit	159
4.5.8 Report Research Results	160
4.6 Cycle 4 – Development of the Framework Security and Privacy Controls	161
4.6.1 Appreciate the Problem	162
4.6.2 Study the Literature & Expert Advice	163
4.6.3 Develop Framework Aspect	164
4.6.4 Evolve the Method.....	167
4.6.5 Action	169
4.6.6 Evaluate Experience	169
4.6.7 Assess Usefulness and Exit	170
4.6.8 Report Research Results	171
4.7 Summary	172
5 Validation of the Framework.....	174
5.1 Introduction	174
5.1 Stage 1: Selecting the Type of Interview	176
5.1.1 Semi-structured Interview	176
5.1.2 Focus Group Interviews.....	177
5.2 Stage 2: Establishing Ethical Guidelines	177
5.3 Creating the Interview Protocol	179
5.3.1 Ensuring Interview Questions Align with Research Questions.....	179
5.3.2 Constructing an Inquiry-Based Conversation.....	180
5.3.3 Receiving feedback on interview protocols.....	182
5.3.4 Piloting the Interview Protocol.....	183
5.4 Conducting and Recording the Interview and Focus Group	183
5.5 Analysing and Summarising the Interview	184
5.6 International Expert Review.....	186
5.6.1 International Expert Biography	186
5.6.2 Findings	187
5.7 Final Focus Group.....	200
5.7.2 Focus Group Findings	203

Table of Contents

5.8	STATSports Implementation of the Framework	223
5.9	Summary	228
Part 4 Summary and Conclusions		232
6	Summary and Conclusion	233
6.1	Summary	233
6.2	Revisiting the Research Objectives	235
6.2.1	Research Objective 1	236
6.2.2	Research Objective 2	238
6.2.3	Research Objective 3	239
6.2.4	Research Objective 4	240
6.2.5	Research Objective 5	241
6.2.6	Research Objective 6	241
6.3	Revisiting the Research Questions	242
6.3.1	Research Sub-Question 1	243
6.3.2	Research Sub-Question 2	244
6.3.3	Research Sub-Question 3	247
6.3.4	Research Sub-Question 4	248
6.3.5	Overall Research Question	249
6.4	Research Contributions	250
6.4.1	Literature and Research Community	251
6.4.2	To the Knowledge of the Application of Security and Privacy Risk Assessment in Software Development	253
6.4.3	To the Knowledge of Demonstrating Compliance to the GDPR Data Protection Principles to the SME Software Development Community	256
6.5	Impact on the Field	257
6.6	Research Limitations	258
6.7	Research Validity	260
6.7.1	Reliability	260
6.7.2	Internal Validity	261
6.7.3	External Validity and Generalisability	261
6.7.4	Construct Validity	262
6.8	Further Research	263

Table of Contents

6.9 Conclusion.....	264
References.....	267
Acronyms.....	283
Glossary of Terms.....	286
Appendix A Framework Review Information Leaflet and Questionnaire	289
Appendix B Questionnaire Questions Matrix Mapped to RSQs.....	302
Appendix C Presentation to Experts	306
Appendix D Key Word Search and Validation of Nist SP-800-53 R5, ISO/IEC 15408-2 and IEC 62443-3.....	307
Appendix E Interview Protocol Matrix - Focus Group Questions	308
Appendix F Expert Review SSI Transcript – Dr. Kim Wuyts.....	317
Appendix G STATSports Final Focus Group Transcript	340
Appendix H Framework	368
Appendix I Implemented Framework – STATSports.....	369

Table of Figures

Figure 0.1 Map of the Thesis	xviii
Figure 0.2 Map of the Thesis - Part 1	1
Figure 1.1 Overview of the framework steps	8
Figure 1.2 Research questions and objectives	17
Figure 1.3 Research Approach Overview	18
Figure 1.4 Publishing, workshop, and presentations from research	22
Figure 2.1 Research sub-questions and objectives addressed in literature review	24
Figure 2.2 High level potential data in flow in the IoMT	31
Figure 2.3 ‘Spheres’ of protection of healthcare data	49
Figure 2.4 Representation comparison of the security risk and safety risk management processes	57
Figure 2.5 Seven stages of PASTA	69
Figure 2.6 How the literature review sections correlate to the RSQs and ROs	82
Figure 2.7 Elements of the framework	84
Figure 0.3 Map of the Thesis - Part 2	85
Figure 3.1 Summary of research question, sub-questions, and objectives	86
Figure 3.2 Overview of research methods used from the layers of the research onion for this research project	87
Figure 3.3 Action design research cyclical process (Sein et al. 2011)	92
Figure 3.4 Canonical action research process (Davison et al. 2004; Smith et al. 2010)	93
Figure 3.5 Adaption of the CAR approach for this research project	94
Figure 3.6 Diagnosing stage of study	95
Figure 3.7 Action planning stage of study	96
Figure 3.8 Action taking stage of study	97
Figure 3.9 Evaluating stage of study	98
Figure 3.10 Typology of interviews (Cohen et al. 2005; Saunders et al. 2009)	103
Figure 3.11 Summary of the research methodology	106
Figure 3.12 Canonical action research strategy applied to this research	107
Figure 0.4 Map of the Thesis - Part 3	113
Figure 4.1 Outline of the cycles used to develop the framework	115
Figure 4.2 Evolution of the framework	116
Figure 4.3 Background section and framework six steps that make up the DPIA	117

Table of Figures

Figure 4.4 Cycle 1 summary	120
Figure 4.5 Cycle 1 appreciate the problem outline	121
Figure 4.6 Cycle 1 literature studied and expert advice	123
Figure 4.7 Cycle 1 outline on development of the framework aspect	127
Figure 4.8 Cycle 1 evolve the framework outline	129
Figure 4.9 Cycle 1 action outline.....	130
Figure 4.10 Cycle 1 evaluate experience summary outline	131
Figure 4.11 Cycle 1 summary usefulness assessment	132
Figure 4.12 Cycle 1 report research results summary	133
Figure 4.13 Cycle 2 summary	134
Figure 4.14 Cycle 2 appreciate the problem outline	135
Figure 4.15 Cycle 2 literature study and expert advice outline	136
Figure 4.16 Outline on aspect of the framework development in cycle 2	136
Figure 4.17 Cycle 2 progress in the framework development outline.....	138
Figure 4.18 Cycle 2 action outline.....	140
Figure 4.19 Evaluation of the DPIA draft implemented in cycle 2	140
Figure 4.20 Assessed usefulness of the DPIA and accompanying excel document from cycle 2.....	142
Figure 4.21 Cycle 2 research results report summary	143
Figure 4.22 Steps 1-4 of the framework	144
Figure 4.23 Cycle 3 summary	145
Figure 4.24 Cycle 3 appreciate the problem outline	145
Figure 4.25 Cycle 3 literature studied and expert advice outline	146
Figure 4.26 Outline on aspect of the framework development in cycle 3	147
Figure 4.27 Framework properties sources.....	148
Figure 4.28 Cycle 3 progress in the framework development outline.....	153
Figure 4.29 Framework adaption of TM process to the risk assessment part of ISO 14971 and AAMI TIR57 recommended security risk process	154
Figure 4.30 Cycle 3 action summary	157
Figure 4.31 Evaluation of the framework implemented in cycle 3	158
Figure 4.32 Assessed usefulness of framework from cycle 3.....	159
Figure 4.33 Cycle 3 research results report summary	160
Figure 4.34 Steps 5 and 6 of the framework.....	161
Figure 4.35 Cycle 4 summary	162

Table of Figures

Figure 4.36 Cycle 4 appreciate the problem summary	162
Figure 4.37 Cycle 4 literature studied and expert advice	163
Figure 4.38 Cycle 4 framework aspect developed.....	164
Figure 4.39 Potential data flow in the IoMT	166
Figure 4.40 DFSPCs progression in cycle 4	167
Figure 4.41 Application of the DFSPCs in cycle 4.....	169
Figure 4.42 Evaluation supplied in cycle 4.....	169
Figure 4.43 Mapping from attack to DFSCs.....	170
Figure 4.44 Cycle 4 assessed usefulness and exit.....	170
Figure 4.45 Reported results from cycle 4.....	171
Figure 5.1 Steps of validation	174
Figure 5.2 RSQ. 4 and RO. 5 and RO. 6 validated in chapter 6.....	175
Figure 5.3 Validation as part of action taking and evaluating stages of this action research	186
Figure 5.4 RSQs and ROs mapped to questionnaire questions 1.1 – 1.3 analysed in value	187
Figure 5.5 RSQs and ROs mapped to questionnaire questions 1.4 - 1.8 analysed in value	188
Figure 5.6 RSQs and ROs mapped to questionnaire questions analysed in composition	192
Figure 5.7 RSQs and ROs mapped to questionnaire questions analysed in usability ..	197
Figure 5.8 Validation as part of action taking and evaluating stages of this action research	201
Figure 5.9 RSQs and ROs mapped to questionnaire and focus group analysed in value	204
Figure 5.10 RSQs and ROs mapped to questionnaire and focus group analysed in value	205
Figure 5.11 RSQs and ROs mapped to questionnaire and focus group analysed in composition.....	210
Figure 5.12 RSQs and ROs mapped to questionnaire and focus group analysed in usability.....	216
Figure 5.13 Validation as part of action research project.....	229
Figure 0.5 Map of the Thesis - Part 4	232
Figure 6.1 Relationship between Research Questions and Objectives.....	236

Table of Figures

Figure 6.2 RSQ. 1 addressed by RO. 1 and 3	243
Figure 6.3 RSQ. 2 addressed by RO. 2 and 3	244
Figure 6.4 Framework steps mapped to the AAMI TIR 57 recommended security risk management framework with privacy integrated	246
Figure 6.5 RSQ. 3 addressed by RO. 4 and 5	247
Figure 6.6 RSQ. 4 addressed by RO. 5 and 6	248
Figure 6.7 Publishing of research results	252

Table of Tables

Table 2.1 Literature review key areas, keywords, and search strings	26
Table 2.2 Comparison of Privacy Principles	45
Table 2.3 Standards and domains investigated.....	55
Table 2.4 Seven parts of ISO/IEC 27034	62
Table 2.5 STRIDE security threat categories, property violated, definition (Swiderski and Synder 2004; Shostack 2014b)	66
Table 2.6 Privacy property violated against LINDDUN threat category and definition (Deng et al. 2010)	68
Table 2.7 PASTA stages adapted from.....	70
Table 2.8 ISO/IEC 80001-2-2 19 Security capabilities (IEC 2012).....	72
Table 2.9 Standards used in IEC/TR 80001-2-8 mappings for the 19 security capabilities in IEC/TR 80001-2-2	74
Table 2.10 Standards investigated for security and privacy controls	76
Table 2.11 NIST SP 800-53r5 control identifiers and family names	77
Table 2.12 ISO/IEC 15408 terms (ISO/IEC 2014a, pp.2–18).....	78
Table 2.13 ISO/IEC 15408-3 terms (ISO/IEC 2008b)	80
Table 4.1 STATSports’ customer and GDPR requirements triggered policies.....	122
Table 4.2 Framework Properties and Threat Types with Definitions and Descriptions	149
Table 4.3 LINDDUN classification of hard and soft privacy with properties and corresponding threats.....	153
Table 4.4 Options for risk mitigation (NIST 2012).....	156
Table 4.5 Risk mitigation and prioritisation	157
Table 4.6 List of keywords for search of three technical standards	166
Table 5.1 Sample matrix for mapping the steps and components of the framework to the research questions	180
Table 5.2 Questionnaire categories developed to themes for developing interview protocol.....	181
Table 5.3 Software team recommendations for filter level categories for threat elicitation	212
Table 5.4 Example GDPR lawful processing requirements	225
Table 5.5 Example threat elicitation	227

Table of Tables

Table 5.6 Example risk analysis results228

Abstract

The Internet of Medical Things (IoMT) is a fast-growing domain as healthcare moves out of structured health services into care in the community. As a result, the personal and sensitive health data associated with the IoMT can potentially flow through a diversity of apps, systems, devices and technologies, public and open networks. This exposes data in the IoMT to additional attack surfaces, which requires the hardening of the security and privacy of the data. Consequently, the data is bound by regulatory security and privacy requirements enforced by the General Data Protection Regulation (GDPR). A key GDPR requirement for any project processing personal data and data concerning health, is security and privacy by design and a data protection impact assessment. Applying regulatory compliant requirements is a struggle for developers in small to medium enterprises due to lack of knowledge, experience and understanding. The PhD research developed a framework for developers in small to medium enterprises, to assist in demonstrating meeting regulatory compliance for security and privacy of data in flow in the IoMT. The framework is founded in the data protection principles of the GDPR and in security and privacy by design. The framework expands on the established threat modeling steps to apply both security and privacy properties to protect data in flow in the IoMT. To mitigate the identified security and privacy threats, the framework includes a set of categorised technical security and privacy controls developed through medical device security and privacy standards. The originality of this framework is the inclusion of security and privacy requirements in the extension of the traditional threat modeling process, the security and privacy controls embedded in the medical security standards and the documentation of this systematic process in an innovative data protection impact assessment.

Related Peer Reviewed Publications

- Treacy, C., McCaffery, F. and Finnegan, A. (2015). Mobile Health & Medical Apps: Possible Impediments to Healthcare Adoption. In: eTELEMED, The Seventh International Conference on eHealth, Telemedicine, and Social Medicine. Lisbon, Portugal: IARIA, 2015, pp.8–11.
- Treacy, C. and McCaffery, F. (2016a). Data Security Overview for Medical Mobile Apps Assuring. *International Journal on Advances in Security*, 9(3 & 4), pp.146–157.
- Treacy, C. and McCaffery, F. (2016b). Medical Mobile Apps Data Security Overview. In: SOFTENG: The Second International Conference on Advances and Trends in Software Engineering. Lisbon, Portugal, pp.123–128.
- McCaffery, F., Özcan-Top, Ö., Treacy, C., Paul, P., Loane, J., Crilly, J. and Mahon, A.M. (2018). A Process Framework Combining Safety and Security in Practice. In: *Communications in Computer and Information Science*. pp.173–180.
- Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: *26th EuroSPI Conference*. Edinburgh: Springer Links. Available from: <https://2020.eurospi.net/index.php/workshop#>.
- Treacy, C., Loane, J. and McCaffery, F. (2020a). A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In: Messnarz, R. et al., eds. *Systems, Software and Services Process Improvement: 27th European Conference, EuroSPI 2020*. Springer Nature, pp.107–119.
- Treacy, C., Loane, J. and McCaffery, F. (2020b). Developer driven framework for security and privacy in the IoMT. In: *ICSOFT 2020 - Proceedings of the 15th International Conference on Software Technologies*. Springer, pp.443–451.
- Shahid, A., Bazargani, M., Banahan, P., Mac Namee, B., Kechadi, T., Treacy, C., Regan, G. and MacMahon, P. (2022). In: *Healthcare* Vol. 10, No. 5, p. 755. Multidisciplinary Digital Publishing Institute.
- Treacy, C., Regan, G., Shahid, A. and Maguire, B. (2022) (Submitted) Legal, Privacy, Social and Ethical Requirements and Impact Assessment for an Artificial Intelligence based Medical Imaging Project. In: *European Systems Software and Service Process Improvement and Innovation (EuroSPI²) 2022*. <https://conference.eurospi.net/index.php/en/>

Document Map

Figure 0.1 provides a map of the sections of the thesis and the chapters contained within each section. At the beginning of each part of the thesis, the relevant section of the document map is highlighted.

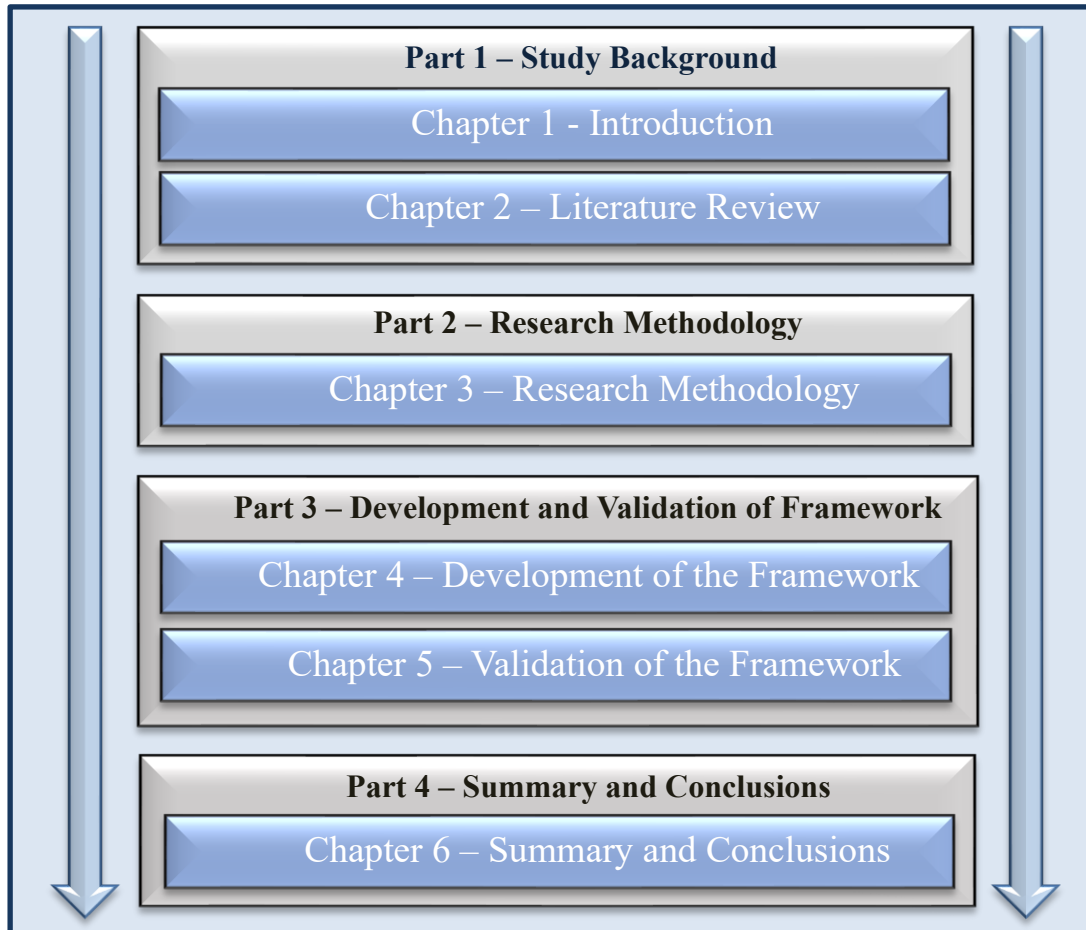


Figure 0.1 Map of the Thesis

Part 1 Study Background

The first part of this thesis contains two chapters as illustrated in Figure 0.2. Chapter 1 presents an introduction to this research and outlines the research questions and objectives. Chapter 2 presents the findings of the literature review that was performed as part of this study.

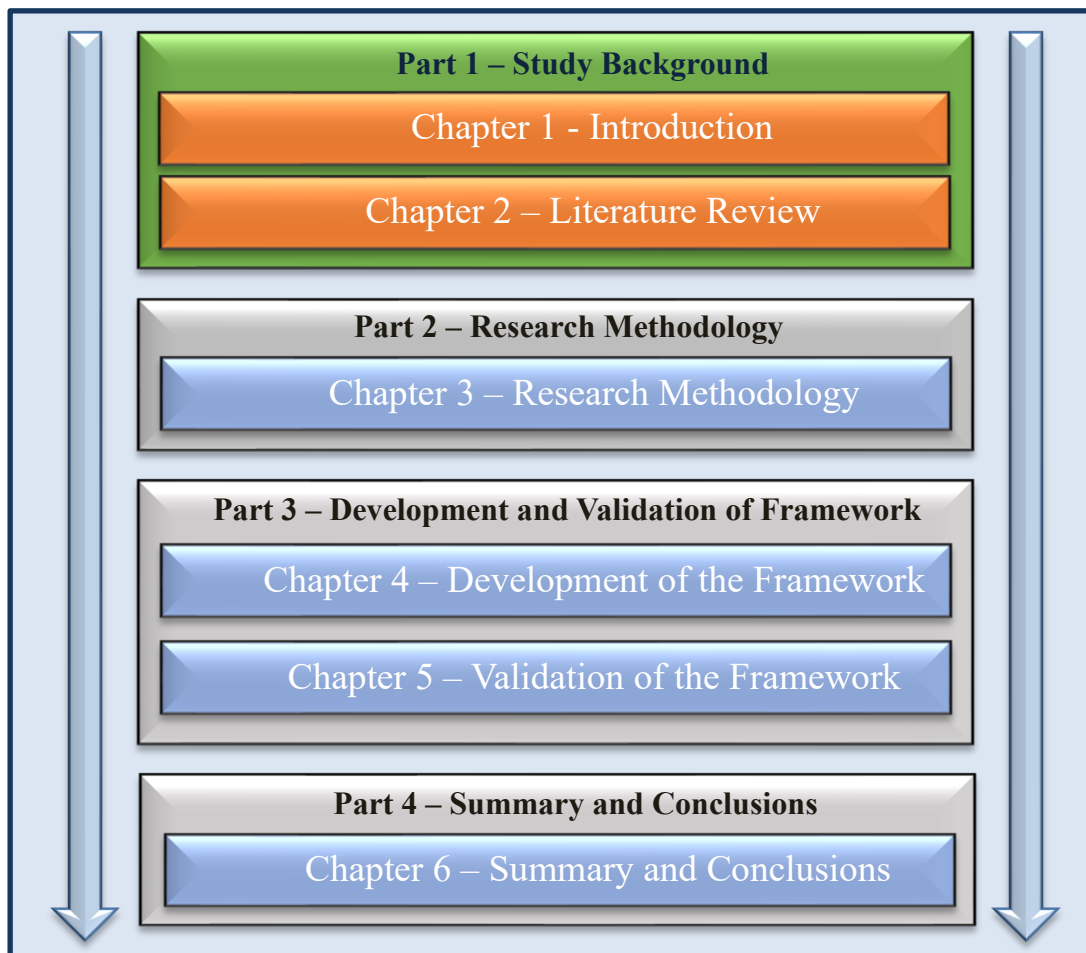


Figure 0.2 Map of the Thesis - Part 1

1 Introduction

This chapter introduces this thesis and presents the motivation and background to the research. Section 1.1 provides a brief overview of the Internet of Medical Things (IoMT), the regulatory and best practice requirements for the security and privacy of personal and sensitive data in the IoMT. The research problem is outlined in section 1.2 and the research context is discussed in section 1.3. The proposed solution to the research problem is presented in section 1.4. Section 1.5 presents the research questions and objectives that are addressed as part of this study. Section 1.6 details the approach taken to perform this research and section 1.7 provides a description of the research contribution. Finally, section 1.8 provides and an outline of the structure of the thesis.

1.1 Overview

The Internet of Medical Things (IoMT) is medical care delivered through an increasingly complex network of information technology systems, medical devices, and applications (Alsubaei et al. 2019). The IoMT is interconnected through the internet and wireless technologies such as Wi-Fi, Ultra-Wideband, Bluetooth, 4G/5G, and so on (Alsubaei et al. 2017; Srivastava et al. 2020; Al Shorman et al. 2020). The IoMT connects patients, doctors, nurses, pharmacists, and other services that link into healthcare (Gatouillat et al. 2018). It is fundamentally “*changing healthcare delivery, affordability, and reliability*” (Shelke and Sharma 2018, p.4). The IoMT is being used to increase patient engagement and experience, manage diseases and drugs, improve treatments, reduce errors, and lower costs (Balandina et al. 2015; Alsubaei et al. 2017; Rubí and Gondim 2019).

The information transmitted through the IoMT includes personal health information (PHI) and sensitive health data. It is essential that this data is kept secure and private. Cybersecurity threats in the IoMT could directly affect clinical care and patient safety (Thomasian and Adashi 2021). Breaches of PHI can have serious consequences for both providers and patients. The impact of data breaches in the medical domain are broad and can lead to financial losses, losses in reputation, legal action, and life impacting conditions (Senseon 2019; Ponemon Institute/IBM 2021; Tarikere et al. 2021). A data breach that maliciously change a medical diagnosis or prescribed medication has serious physical harm consequences (Seh et al. 2020).

However, because of the open nature and complex communications protocols in the IoMT, the PHI is exposed to broader cybersecurity risks. This is a realism that

cybercriminals have identified and are actively exploiting (Filkins 2014; Anandarajan and Malik 2018). There are a number of issues that contribute to this exploitation in the IoMT. Cybersecurity in healthcare in general is not as mature as other domains (Tarikere et al. 2021). Reports (Ponemon Institute 2018; Cisco 2019) determined that in terms of security and privacy maturity, the medical healthcare domain is behind other domains and vulnerable to connectivity cybersecurity. Software developers in healthcare do not have the extensive experience with the types of threats other consumer app industries are familiar with (e.g., finance). This is of further significance when considering that many services in the IoT are designated by small to medium enterprises (SMEs) (Balandina et al. 2015). This is driven partly by the demand of the healthcare industry to embrace IoT without a profound understanding of the security and privacy risks and the rush into the lucrative healthcare domain by organisations not familiar with the regulatory requirements of this field (Sun et al. 2018; Hatzivasilis et al. 2019). A lack of experience can lead to an incomplete or missing security and privacy risk assessment, which leads to insufficient security and privacy controls, leaving an IoMT system exposed to cybersecurity vulnerabilities.

SMEs specifically struggle due to the lack of strong in-house expertise and knowledge of the regulatory, security, and privacy requirements for PHI. SMEs also struggle with the application of information security and privacy standards due to their limited resources and knowledge (Wagner et al. 2020). The standards are disseminated through various domains, and are difficult to understand and implement (Wagner et al. 2020). There is also limited European or international standards designed to assist SMEs towards ensuring appropriate protection of data (Manso et al. 2015). Difficulties in budget constraints, deficiencies in understanding and lack of trained personnel (Dhillon 2011; Cisco 2018; Ponemon Institute/IBM 2021), technologies in use (Alsubaei et al. 2019) and understanding regulatory requirements (Parker et al. 2017), are some of the issues that contribute to inadequate cybersecurity and privacy strategies within this domain (Treacy & McCaffery, 2016). Recommendations are that security and privacy are designed at the beginning of a development project, into the devices, the communication protocols, and the services (McManus, 2018).

Added to these issues, are the complexities for SMEs and developers in understanding the security and privacy regulatory requirements (Parker et al. 2017). The General Data Protection Regulation (GDPR) is the regulatory requirement for any organisation processing any PHI of any European Union (EU) citizen or within the EU.

The GDPR has a regulatory requirement of *data protection by design and by default* (EU General Data Protection Regulation (GDPR) 2016, p.25). This position is also supported by expert recommendations who direct that security and privacy are designed into a project from the beginning (Schneier and Shostack 1999; Tondel et al. 2008; Danezis et al. 2014; Shostack 2014b; De Francesco 2019). For the IoMT this includes considering security and privacy not only for the devices and apps but also for the communication protocols and services (McManus 2018). However, many SME software development teams are not aware of security and privacy by design or how to implement these models. In addition, the GDPR requirement of Article 24(1) states an organisation is to *implement appropriate technical and organizational measures* to ensure and demonstrate compliance with the regulation and document a Data Protection Impact Assessment (DPIA) (EU General Data Protection Regulation (GDPR) 2016, p.22). However, SMEs struggle with understanding the GDPR data protection principles and meeting compliance (Jasmontaitė-Zaniewicz et al. 2021). This is a noteworthy issue for SMEs as data protection authorities apply the GDPR regardless of the size of an organisation, which can lead to substantial fines for non-compliance (Jasmontaitė-Zaniewicz et al. 2021).

Given the importance of data security and privacy in IoMT systems, meeting and demonstrating the GDPR data protection principles, this research aims to find a way to assist developers in SMEs to demonstrate data security and privacy in their IoMT products to meet GDPR regulatory compliance.

1.2 Research Problem Defined

To understand the challenges for SME software developers in implementing security and privacy during development and in demonstrating compliance with the GDPR data protection principles, this research conducted an extensive literature review, which revealed many difficulties for applications. The research was conducted within an Irish software development SME organisation. This SME also shared the difficulties they encountered in implementing data security and privacy for their software products and systems and demonstrating compliance with the GDPR data protection principles. As a result, the focus of this research is on the following difficulties:

- The lack of knowledge in SME software development teams on how to demonstrate compliance with the GDPR data protection principles. The GDPR does not provide clear guidelines for designers and developers on how to build

GDPR compliant products (Hatzivasilis et al. 2019; Sun et al. 2018; Ataei et al. 2020; Jasmontaité-Zaniewicz et al. 2021);

- Issues around understanding the appropriate standards and guidance to implement and meet the requirements for data security and privacy risk management in software development and in the IoMT. The standards are disseminated and are difficult to locate for those with little or no experience of standards. Many of the standards reference other standards because of the complexity of the security and privacy requirements and they are difficult to implement. They are not widely known and therefore there is poor uptake in implementation in software development Roth 2014 Barlette and Fomin (Wagner et al. 2020; ENISA 2021);
- The lack of a systematic approach for SME software developers to apply both security and privacy simultaneously in software development (ENISA 2021; Jasmontaité-Zaniewicz et al. 2021);
- The lack of expertise, time and understanding of data security and privacy application in SME software development teams (Cisco 2017; Ponemon Institute 2018; ENISA 2021).

The reasons for the difficulties in understanding and demonstrating data security and privacy for IoMT products in compliance with the GDPR data protection requirements are twofold. The first reason is that there is no one standard or guidance document for software developers to adhere to. The second reason is that the GDPR is complicated and details on the different aspects of the data protection requirements are disseminated throughout the regulation. This complexity can lead to uncertainty and misunderstanding for SMEs. SMEs in general do not have personnel experienced in deciphering and implementing standards and regulations. To add to these difficulties, while the standards specify what to do, they do not tell you how to implement risk management or security and privacy in software development. This lack of guidance in how to implement security and privacy requirements in software development is a particular problem for SMEs.

1.3 Research Context

This study is based in the SME software development domain. The Irish Small and Medium Enterprise Association (ISME) defines a small enterprise as one that has fewer than 50 employees and a medium enterprise has fewer than 250 employees (ISME 2021). The research was completed in an Irish SME STATSports, which presented with many

Chapter 1 Introduction

of the challenges outlined in sections 1.1 and 1.2. The particular focus of the research is to provide a DPIA to support STATSports' software developers with data security and privacy in the IoMT to meet the GDPR data protection principles. Collaborative research with an SME encountering the challenges provided an opportunity to observe and collaborate with SME software developers to develop an approach to meet the requirements to demonstrate compliancy with the GDPR data protection principles.

STATSports was founded in 2008 and at the time of this research had 132 employees. STATSports is a sports technology company that provides performance monitoring and analysis solutions for professional sports teams and athletes. The company developed a range of Global Positioning System (GPS) tracking devices and software platforms that analyse an athlete's performance in real-time. This allows coaches and trainers to monitor and provide accurate and reliable feedback on live data in any arena infrastructure. The technology is used by some of the world's leading sports teams and organisations, including the English Premier League, the NBA, and the Irish Rugby Football Union. The organisation developed the Apex Athlete Series GPS performance tracker in 2019 for the consumer market and the individual player. In 2021, STATSports and Arsenal partnered to create the STATSports Arsenal FC Edition GPS tracker. This bespoke product allows Arsenal fans to compare their performances against the Arsenal men's, women's, and academy teams. In 2022, STATSports will be using their proprietary technology to move into the medical device domain. All STATSports software systems process PHI.

STATSports need to meet; the GDPR data protection principles, data security and privacy requirements from their elite clients, and their move into the medical domain, provoked the organisation to request assistance to implement and demonstrate data security and privacy in their software systems and products in the IoMT.

The reasons for the focus on SME software development teams in the IoMT domain are:

- The researcher was embedded in the STATSports organisation and their software development team. In addition, the researcher has contact, and access to other SME software development organisations in the IoMT domain;
- The desire to assist SME software developers demonstrate security and privacy of the data in their IoMT software products and systems with the GDPR data

protection principles and thus their overall competitiveness (Horgan et al. 2018; Jasmontaitė-Zaniewicz et al. 2021);

- It is acknowledged that SME's do not have the resources or expertise of larger organisations. Furthermore, existing information security standards such as ISO 27001 and NIST Cybersecurity framework are perceived as being too big or complex for small organisations and are not suitable for software development risk management (Horgan et al. 2018);
- The importance of the medical technology (MedTech) sector in Ireland. Ireland is established as a globally recognised centre of excellence for MedTech, home to 300+ companies (indigenous and SME), 60% of which are Irish owned, employing over 40,000 people (Department of Business Enterprise and Innovation 2020b; IDA 2021). SME software development organisations play a significant role in the growth and success of the Irish MedTech industry (Enterprise Ireland 2021).

1.4 Towards A Data Protection Impact Assessment Framework for Medical Device Software Developers for Meeting GDPR Security and Privacy Requirements in the Internet of Medical Things – MDev DPIA

The MDev DPIA (henceforth known as the framework) addresses the identified difficulties and challenges that a SME software development team may face in demonstrating data security and privacy of their software systems or products to the GDPR data protection principles. The aim of the framework is to provide a systematic approach for SME software developers to apply data security and privacy in software development to demonstrate compliance with the GDPR data protection principles. The framework was designed to assemble the appropriate components and processes that software developers could implement to meet the GDPR data protection principles. These components and processes were compiled from disseminated standards, guidance, and best practice documents from the medical, network security, data security and privacy domains. The results of the components and processes completed through the implementation of the framework are documented. The documentation of the components and processes is founded in the GDPR requirements for a DPIA.

The framework currently focuses on the legal requirements for personal data protection in the EU, which is regulated by the GDPR (General Data Protection Regulation (GDPR), 2016). The focus on the EU GDPR is due to the fact that the majority

of STATSports' elite clients and customers are EU data subjects. Also, STATSports receive data protection requirements from their clients based in the EU. In addition, the GDPR is recognised as one of the most progressive and comprehensive regulations for data protection in the world (Data Protection Commission Ireland 2020).

The framework has six steps: Step 1: Contextual knowledge. Step 2: System decomposition. Step 3: Threat identification. Step 4: Threat analysis. Step 5: Identify security and privacy properties against threats. Step 6: Selection of controls to mitigate threats. Figure 1.1 presents the steps and gives a high-level overview of the details of each step of the framework.

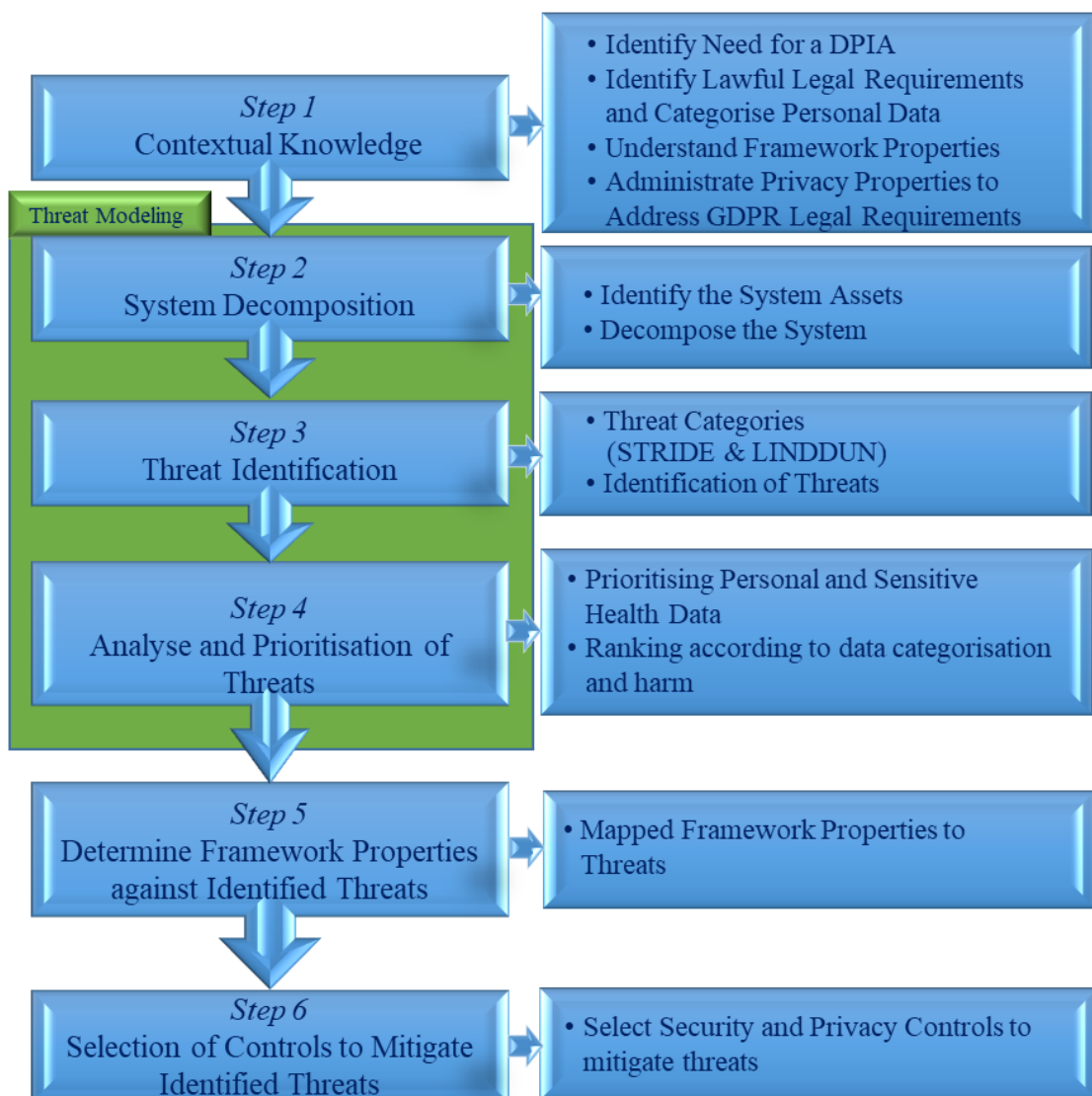


Figure 1.1 Overview of the framework steps

The framework is presented in one document with an accompanying Excel document. This Excel document is populated as the organisation completes the framework. The framework document provides the information to complete the Excel document. The preliminary section of the framework document establishes the scope of the DPIA, a brief description of the system, the stakeholders and their contact details, recording of any consultation that could influence the DPIA and a record of disclosure to third parties (if any). This section also provides a division to list any relevant documents to the DPIA, for example organisational policy documents, data processing agreements or finance costing documentation. The objective is to collect all of the information pertinent to the software system development in one document. At the beginning of every step of the framework there is a table that provides the components, outcomes, and referenced links. The components list the parts of the step. The outcomes list what should be delivered from each part of the step.

1.4.1 Step 1

This step provides the contextual knowledge to assist SMEs and new or inexperienced developers to understand the security and privacy context in order to be able to use the framework. This step establishes the Framework Principles, outlined in Annex A of the framework, which are founded in the GDPR data protection principles. This includes establishing the GDPR requirements to identify the need for a DPIA and identifying and categorising the data the product will use. The GDPR data protection principles are grounded in the framework properties, which are the common goals that the framework wants to protect for data in flow in the IoMT. The framework properties are outlined in Table 5 in this step. The framework properties reflect both security and privacy properties to meet the GDPR data protection principles. Also included in this step is the documentation of any potential regional regulatory requirements that should be considered when developing the system and notice to link to the relevant documentation within the organisation in relation to these.

Section three of this step requires the organisation to complete the rationale as to why a DPIA is required via a screening statement. This enables the software development team and organisation to come to the same understanding in relation to the need for a DPIA. The questions to assist in developing the screening statement are founded in the ISO/IEC 29134 (ISO/IEC 2017c) standard that provides guidelines for a privacy impact assessment. In this step the organisation document and categorise the personal

Chapter 1 Introduction

identifiable information (PII) and special categories of such as Personal Health Information (PHI) that will be processed in the system/product. Annex B of the framework provides the definitions for PII and PHI in relation to the GDPR. The definition for PII relates to personal data as defined by Article 4 of the GDPR.

“Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”(EU General Data Protection Regulation (GDPR) 2016 Art. 4(1))

PHI includes the definitions provided by Article 4 of the GDPR on data concerning health.

“Means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.”(EU General Data Protection Regulation (GDPR) 2016 Art.4(15))

This step also includes details on the requirements in relation to consent compliance and content awareness. This part of the framework involves the administration of two soft privacy properties, *Content Awareness* and *Policy and Consent Compliance*, and management of their LINDDUN threat categories *Unawareness* and *Non-compliance* respectively. Both of these soft privacy properties are significant for GDPR regulatory requirements and the requirements of the privacy standard ISO/IEC 27701 (ISO/IEC 2019). The *non-compliance* threat category means not following the data protection legislation, the advertised policies or the existing user consents of the regulatory jurisdiction (Wuyts and Wouter 2015). The step includes details on the requirements of a privacy policy and provides a draft policy in Annex C of the framework. This step establishes appropriate knowledge for the developers to address the initial legal requirements of the GDPR in the development of a software product handling personal and health data. One of the key components of this step is Table 7 in the framework. This table supports the requirement of lawful processing. It outlines what data the system will collect and process. It provides how organisation will meet the GDPR data protection principles in relation to lawful processing and how it will be transparent and consensual with the user.

1.4.2 Step 2

Steps 2 - 4 are founded in the established risk-based approach to designing software systems, threat modeling (TM). The threat models applied in the framework are STRIDE and LINDDUN. Step 2 includes the identification of the assets in your system and are recorded in this step. Assets are resources or components of a system that are valuable and need to be protected in the context of system decomposition and threat modeling. Decomposition of the system accomplished with Data Flow Diagrams (DFDs). At each level of decomposition, the details are carried through with the DFD and added to. This is to prevent duplication of work. Each decomposition level will continually refer to the higher-level composition through version control referencing. The decomposition approach applied, is founded in the developer driven threat model introduced by Dhillon (2011). This was developed to provide a process that incorporates guidelines on creating DFDs for developers with or without security expertise.

DFDs were used because they are an established tool used for TM (Osterman 2007; Shostack 2014b) and both STRIDE and LINDDUN use DFDs for decomposition and use (Sion, Wuyts, et al. 2018). DFDs support following the data flow through a system and problems tend to follow the data flow (Shostack 2014b). Likewise, ISO/IEC 27701, advises the use of DFDs as helpful tools to inform a protection impact assessment and risk assessment transfer, which assists with regulatory requirements. Additionally, STRIDE and LINDDUN provide a set of threat types in relation to the elements of DFDs. Annex D of the framework provides an adapted set of DFD elements and symbols for inexperienced developers. Three key features for creating DFDs to assist inexperienced developers and SMEs are outlined in the framework, which are: DFDs Elements and Symbols, Decomposition Levels and Annotations. As key part of the DFD elements provided by the framework is the documentation of trust boundaries, entry and exit points, which are colour coded to aid in visualisation.

1.4.3 Step 3

This step includes identifying potential threats to the system that could violate the framework properties. This step is completed using the framework threat taxonomy to elicit threats of the software system by assessing the data security and privacy through per-interaction. Categorising threats makes it easier to understand what the threat allows an attacker to do and supports in assigning priority and mitigation (Hussain et al. 2014). Threat identification is central to the TM process but, is also one of the most difficult

aspects of the process to complete, for developers with little or no experience (Dhillon 2011).

The framework uses the threat categories from two different TMs used in software development, STRIDE and LINDDUN, for identifying and assessing security and privacy threats and vulnerabilities. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Shostack 2014b). These six categories represent different types of security threats that can be used to attack a software system. LINDDUN stands for Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance (Deng et al. 2010). It is a TM used to evaluate privacy risks associated with the collection, use, and disclosure of personal information (Wuyts and Joosen 2015). Anne F of the framework provides the threat taxonomy and the corresponding framework properties they violate. Threat identification is completed through per interaction-based methods used by both LINDDUN and STRIDE and is centred upon the building blocks of DFDs (Sion et al., 2018).

Threat identification is a challenge within the software TM field, particularly for inexperienced software developers (Dhillon 2011). The framework provides a threat to attack starter kit library resource in Annex G. This library is not an inclusive list of common attacks for each of the threat types and many of the attack types overlap throughout the threat taxonomy. The objective of the table is to provide a groundwork threat to attack library to bridge the gap in lack of knowledge for inexperienced developers and SMEs. The library also provides extra context and knowledge in relation to attack types and resources to provide a foundation to build an organisational threat library. The provision of these resources is to promote further development of knowledge, interest and build confidence in this element of threat modeling.

The threat to attack type starter kit library provides a short outline of each of the framework threats and provides a list of common attacks within the threat type. The attack types are mapped to the most critical risks listed in the Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors 2019 (CWE 2019), the OWASP Top 10 2017 (OWASP 2017) and the OWASP API Security Top 10 2019 (OWASP 2020b). This mapping aims to provide a foundation for understanding and build knowledge on resources available in this domain.

1.4.4 Step 4

Step 4 is threat analysis the risk assessment of the threats identified through step 3. This step is completed through prioritisation of the risks to determine which threats should be addressed first. The risk assessment will consider data security and privacy and the controls to mitigate these threats and how they could affect safety, and how each might impact the other. Threat analysis is also a challenging piece of TM (Dhillon 2011). Both the STRIDE and LINDDUN categories are abstract enough, which means that attacks could apply to one or more of the threat categories. There is a degree of required understanding and knowledge to map to tangible attacks and without security knowledge, STRIDE can't be used effectively (Dhillon 2011).

To support SMEs and developer's lack of knowledge and understanding required to complete threat analysis, the framework provides a threat to attack starter kit library. The framework threat prioritisation is guided by the NIST SP 800-30 guide for conducting risk assessments (NIST 2012). Threat prioritisation is guided by the qualitative outcomes of the assessment scales provided by NIST SP 800-30. NIST SP 800-30, provides standardised guidance on applying risk assessment for SMEs and developers with little or no knowledge and experience. The framework assessment scale uses the five-point rating system – Very Low, Low, Moderate, High, and Very High, from NIST SP 800-30. The framework includes a NIST SP 800-30 risk matrix founded on the overall likelihood in contrast to level of impact. The assessment is additionally measured by the sensitivity of the personal data and safety of the patient associated with the threat and vulnerabilities. The risk assessment considers not only the individual aspects of security and privacy but how they impact each other, comparable to the consideration applied in TIR 57 of security and safety. Threats and vulnerabilities can involve either or both security and privacy. When applying controls for either security and privacy it is important to examine how they impact the other.

1.4.5 Step 5

Step 5 of the framework provides a connection between the prioritised elicited threats and the security and privacy properties the framework intends to protect. The threat categories of STRIDE and LINDDUN map to the security and privacy property it violates. The security and privacy properties are affiliated to the standards and regulatory requirements and step 5 maps the threats identified in step 4 to the framework's security and privacy properties. The purpose of this mapping is to simplify identification of

appropriate security and privacy controls to mitigate the identified threats. This is a straightforward step in the framework necessary to complete step 6. Similar to the threat elicitation and analysis stages, there will be commonalities and an overlapping of properties and categories.

1.4.6 Step 6

This step is the identification of the countermeasures needed to defend the security and privacy properties breached by the identified and prioritised threats. The framework provides a set of technical security and privacy controls to maintain the security and privacy of data in flow. These controls have been classified with respect to the security and privacy properties. These are called the Data Flow Security and Privacy Controls (DFSPCs). The aim of the DFSPCs is to provide a set of technical controls to assist developers comply with security and privacy requirements of regulation and close the gap in knowledge in this area. The DFSPCs fill the vacuum of specific technical controls for the security and privacy of data in flow to assist developers to comply with the regulatory requirements. The DFSPCs are provided as an individual resource within the accompanying framework Excel document.

1.5 Research Questions and Objectives

The central focus of this research is the development of a security and privacy risk assessment framework which will assist SME software developers demonstrate compliance with the GDPR data protection principles in their IoMT software systems or products. The development of framework is required to answer the overall Research Question which is:

“How can the development of a security and privacy risk assessment framework for data in flow in the IoMT assist software developers in SMEs to demonstrate compliance with the GDPR data protection requirements in their software products?”

This overall Research Question has been further divided into four lower-level Research Sub-Questions (RSQ):

***RSQ. 1** - What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?*

***RSQ. 2** - What are the methods and/or standards for security and privacy risk assessment for software development?*

***RSQ. 3** - What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?*

***RSQ. 4** - To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?*

The development of the framework has been subdivided into six Research Objectives (RO) for the purpose of this study:

***RO. 1** - Investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs when implementing the requirements.*

The first objective aims to gain a greater understanding of the GDPR data protection principles and consequently the data security and privacy requirements. This objective also aims to understand the challenges faced by SME software developers in meeting the GDPR data protection requirements in research and in practice.

***RO. 2** - Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.*

Research objective two aims to gain an understanding of what standards and/or best practice methods may be applied for security and privacy risk assessment in software development to help determine compliance with the GDPR data protection requirements.

***RO. 3** - Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.*

The third objective aims to understand what activities are required for software developers to demonstrate compliance with the GDPR data protection principles and how these activities and results should be documented.

***RO. 4** - Development of a security and privacy risk assessment framework to assist software developers to demonstrate compliance with the GDPR data protection requirements in the IoMT.*

The fourth objective aims to develop a framework which may be used to assist SME software developers demonstrate compliance with GDPR data protection requirements in their IoMT software systems or products.

RO. 5 - Validate the framework with industry and research domain experts.

Research objective five aims to validate all elements of the framework through review by experts, in the areas of security and privacy in software development and an expert in the privacy threat model domain.

RO. 6 Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.

The final research objective aims to validate the value, composition, and usability of the framework. This will be addressed by a pilot implementation in a SME software development team focusing on the implementation of a DPIA for a new cloud product feature for an existing product. The framework is used as the focus for the process, providing the activities and outcomes required to fulfil the GDPR data protection principles. The implementation engages the entire software development team and other stakeholders within the SME. Figure 1.2 overleaf, provides a diagrammatic outline of the research questions and objectives.

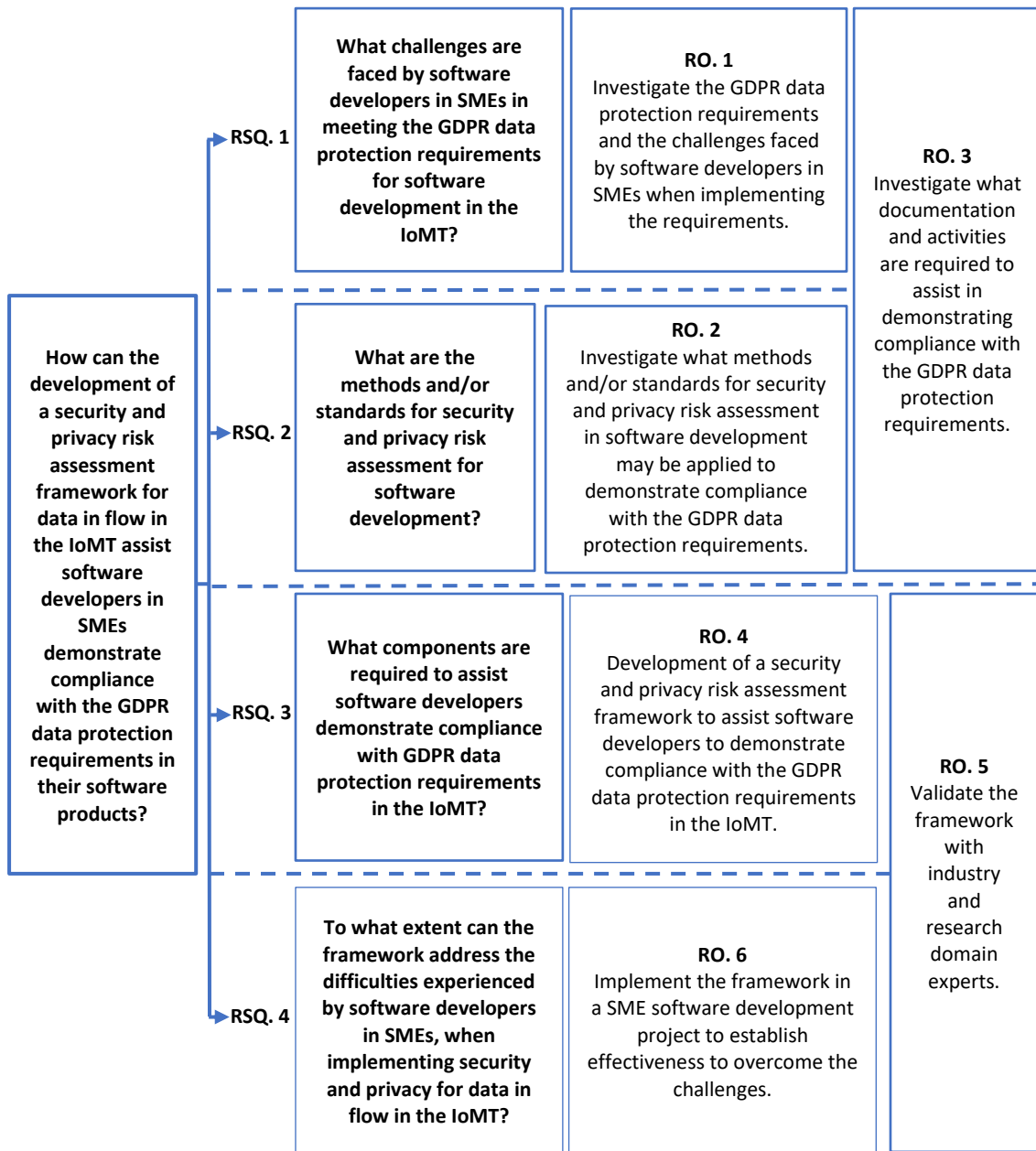


Figure 1.2 Research questions and objectives

1.6 Research Approach

A visual overview of the approach to the research is presented in Figure 1.3 overleaf. The overview displays the chronological sequence of how the research sub-questions and research objectives were addressed during the research. The research approach addressed each research sub-question and research objective. To address research sub-questions one and two an extensive literature review based on research objectives one, two and three was conducted. The breadth of the disseminated information involved with this study, resulted in two overlapping research objectives. Research objective three spanned

research sub-question one and two. Research objective five spanned research sub-question three and four.

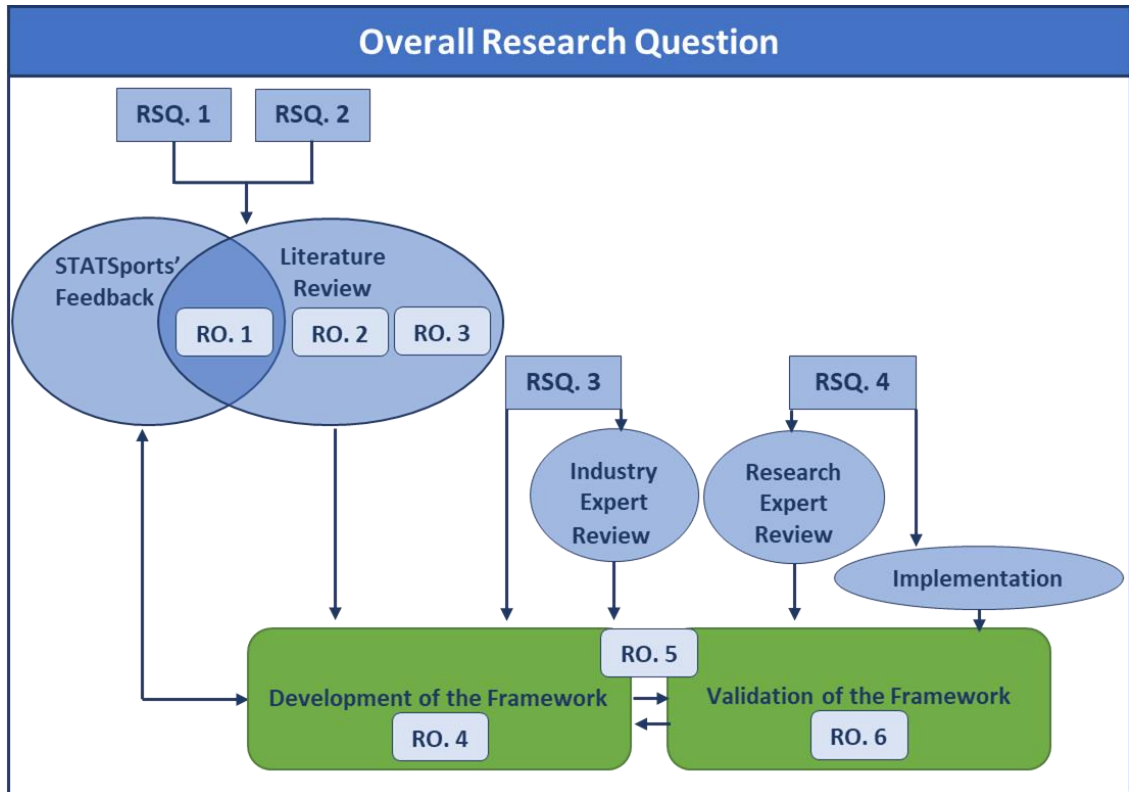


Figure 1.3 Research Approach Overview

The aim of the literature review was to develop a greater understanding of the challenges faced by SME software developers in meeting the GDPR data protection requirements and data security and privacy implementation in software development. The literature review was conducted to gain insight into how these challenges are currently addressed in software development. The literature review also conducted a review on what processes and documentation would be required in order to demonstrate conformity to the GDPR data protection principles. The literature review was supplemented with the feedback provided by the software development team in STATSports. The aim of this phase of research was to confirm that the challenges revealed in the literature review were experienced in a specific SME software development team context.

To address research sub-question three, the results of the literature review informed the development of the framework. This research sub-question was addressed by fulfilling research object four and five. The development of the framework was completed in a collaborative iterative approach between the researcher, the STATSports software team and two experts in software security development. The research in this project sought to link theory with practice, and thinking with doing, within solving a

specific problem. Canonical Action Research (CAR) is a research strategy suited to researching and supporting change. CAR is a type of action research that focuses on developing and refining a theoretical framework or model to guide future practice through iterative cycles of planning, action, observation, and reflection (Davison et al. 2004). The two experts supported the development and validation of the components of the framework. The development of the technical security and privacy controls were completed with validation feedback from another Irish SME that have an IoMT application. Improvements and modifications suggested as a result of the various stages of validation were included in the next version of the relevant component of the framework. Validation of the developed framework was completed by a world expert in privacy research Dr. Kim Wuyts. Dr. Wuyts is one of the key researchers behind the development and extension of the LINDDUN privacy threat model. During the early development of the framework and the security and privacy controls the researcher recognised the lack of privacy controls. This resulted in searching the literature to understand how privacy was being addressed in software development and adaption of the LINDDUN threat model. When investigating an appropriate expert to validate the developed framework, experience and understanding in privacy for software development was significant criteria. Other criteria included experience in security risk assessment, security software development and threat modeling. The researcher contacted several experts. One expert the researcher communicated with was Tony UcedaVélez. He is one of the creators of Process for Attack Simulation and Threat Analysis (PASTA) framework (UcedaVélez et al. 2015). After an initial discussion with Tony UcedaVélez we came to the conclusion that PASTA was not appropriate for my framework. It was too complicated and not appropriate for applying to a framework specifically for a software development team. Tony UcedaVélez acknowledged that he would not have the privacy knowledge to validate the framework adequately. Another expert the researcher communicated via email with was Danny Dhillon. Danny was the author of the developer driven threat modeling process. His expertise was in threat modeling for analysing a system's architecture to find security flaws and reduce architectural risk (Dhillon 2011). Danny also acknowledged that he would not have the privacy knowledge to validate the framework. The researcher also communicated with Adam Shostack, the leading expert in threat modeling and STRIDE. Adam was writing a book and did not have time to provide validation for the framework. Adam did recommend Dr. Wuyts and noted that her research background was in privacy in software

development and her experience included security software engineering with experience using STRIDE. These attributes meet the criteria for the expert validator. The decision to involve only one expert, Dr. Wuyts, was based on the outlined specific circumstances and the objectives of the research. Dr. Wuyts' extensive experience in meeting the criteria for the validation expert and her recognised international expertise in privacy threat modeling deemed her suitable as the validation expert.

Research sub-question four addressed the validation of the framework. This validation was conducted to establish to what extent the framework can address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT. This research sub-question was addressed by research objectives five and six. Research objective five involved the validation of the framework by an academic expert. The academic expert has extensive experience in security in software development in industry and developed the privacy threat model component, LINDDUN, incorporated into the framework. The focus of this validation was to ensure the value, composition, and usability of the framework. This validation also appraised if the privacy requirements of the GDPR data protection principles were met by the framework. A further validation of the framework was completed through a pilot implementation in a software development project with the SME organisation, STATSports. The focus of this part of the validation was to ensure the usability of the framework by SME software developers with little experience, to establish the framework's effectiveness to overcome the challenges communicated from the organisation and established through the literature review.

1.7 Research Contributions

Data security and privacy is a key requirement for compliance with the GDPR data protection principles for any organisation or system processing PHI. The interaction with STATSports presenting their challenges in meeting the GDPR data protection principles in their software systems and products, along with an extensive literature review presented a need to develop a systematic approach to assist SME software developers demonstrate compliance with the GDPR data protection principles. A number of contributions have been made through this research which are:

1. A comprehensive literature review supplemented with feedback from STATSports has provided new understandings on the challenges faced by SME software developers in implementing data security and privacy in their IoMT

software systems and products when seeking to demonstrate compliance to the GDPR data protection principles;

2. The key original contribution of this research is the development and validation of a Developer Driven Framework for Data Security and Privacy in the IoMT to meet the GDPR Data Protection Principles. The framework provides the following contributions:
 - i. The expansion of the outdated confidentiality, integrity, and availability security properties to include the added complexity of the IoMT and incorporate privacy;
 - ii. A collection of processes-based on security, privacy, network and medical device standards and best practice mapped to the AAMI TIR 57 security risk management standard for medical devices to conduct a data security and privacy risk assessment for data in flow in the IoMT for software developers. This collects the disseminated security and privacy risk assessment processes and requirements into a single framework.
 - iii. A systematic approach for SME software development teams to implement a risk assessment for both data security and privacy simultaneously in software development;
 - iv. An ability for a software team to demonstrate what measures they have taken to meet the GDPR data protection principles through the documentation of the framework's components in a DPIA;
 - v. A Threat to Attack Starter Kit Library mapping threat types to attacks to assist inexperienced developers in the domain to implement threat modeling;
 - vi. The framework applies technical security and privacy controls (appropriate for software development), from the standards used for the development of IEC/TR 80001-2-8 (IEC/TR 2016) application of risk management for IT-networks incorporating medical devices to the IoMT domain;
 - vii. A draft privacy policy-based on the GDPR to assist SMEs meet this legal requirement;
 - viii. The implementation of the framework resulted in a DPIA that included a data security and privacy risk assessment of the PHI processed by the STATSports new product to meet the GDPR data protection principles;
 - ix. The research has resulted in several publications. These are mapped to the RSQs and are presented in Figure 1.4 overleaf.

<p>RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?</p>	<p>Treacy, C., McCaffery, F. and Finnegan, A. (2015). Mobile Health & Medical Apps: Possible Impediments to Healthcare Adoption. In: eTELEMED, The Seventh International Conference on eHealth, Telemedicine, and Social Medicine. Lisbon, Portugal: IARIA, 2015, pp.8–11.</p> <p>Treacy, C. and McCaffery, F. (2016b). Medical Mobile Apps Data Security Overview. In: SOFTENG: The Second International Conference on Advances and Trends in Software Engineering. Lisbon, Portugal, pp.123–128.</p> <p>Treacy, C. and McCaffery, F. (2016a). Data Security Overview for Medical Mobile Apps Assuring. <i>International Journal on Advances in Security</i>, 9(3 & 4), pp.146–157.</p>
<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>McCaffery, F., Özcan-Top, Ö., Treacy, C., Paul, P., Loane, J., Crilly, J. and Mahon, A.M. (2018). A Process Framework Combining Safety and Security in Practice. In: <i>Communications in Computer and Information Science</i>. pp.173–180.</p>
<p>RSQ. 3 What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?</p>	<p>Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: <i>26th EuroSPI Conference</i>. Edinburgh: Springer Links. Available from: https://2020.eurospi.net/index.php/workshop#.</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2020a). A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In: Messnarz, R. et al., eds. <i>Systems, Software and Services Process Improvement: 27th European Conference, EuroSPI 2020</i>. Springer Nature, pp.107–119.</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2020b). Developer driven framework for security and privacy in the IoMT. In: <i>ICSOFT 2020 - Proceedings of the 15th International Conference on Software Technologies</i>. Springer, pp.443–451.</p>
<p>RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?</p>	<p>PhD Thesis</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2021). Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things. In: <i>4TH International Clinical Engineering and Health Technology Management Congress (ICEHTMC)</i>. Lake Buena Vista, FL: AAMI.</p> <p>Treacy, C. and McCaffery, F. (2021). Assisting Software Developers to Meet GDPR Data Protection and Privacy Requirements for their IoMT Products. In: <i>2021 European Medical Device Cybersecurity Virtual Conference</i>. Virtual: TT Group. Available from: http://www.emergogroup.com/services/europe/european-medical-device-classification.</p>

Figure 1.4 Publishing, workshop, and presentations from research

1.8 Document Structure

The thesis is separated into four parts. Part 1 contains Chapter 1, the *introduction* and Chapter 2, the *literature review*. Chapter 2, presents a literature review of material related to data security and privacy in the IoMT, the GDPR data protection principles and data protection impact assessment requirements, standards, guidance and best practice on security and privacy risk management and mitigation. Part 2 contains one part, Chapter 3, which outlines the research methodology used in this research. The selected methods and the reasons for their application are also examined. Part 3 contains Chapter 4, the *development of the framework* and Chapter 5, *validation of the framework*. Chapter 4 presents the development of the research framework, which was conducted in an Irish SME software development team with industry experts. Chapter 5, discusses the validation of the overall framework. The framework is subject to an expert review by the developer of LINDDUN, a privacy threat model applied in the framework and a focus group session with the STATSports software development team. The thesis concludes with Part 4 and Chapter 6, *summary and conclusions*. Chapter 6, presents a summary of the thesis and the conclusions drawn from the research. This chapter also presents the contributions of this research, the impact on the field of study, the research limitations, research validity and areas of potential future research.

2 Literature Review

2.1 Introduction

This chapter presents a review of literature related to the security and privacy of data in the Internet of Medical Things (IoMT). To align with the context of this research the literature review, where available, will focus in the Small/Medium Enterprises (SMEs) domain. The literature review was conducted to provide answers for RSQ. 1 and RSQ. 2 and RO. 1, RO. 2, and RO. 3 of this project, which are presented in Figure 2.1.

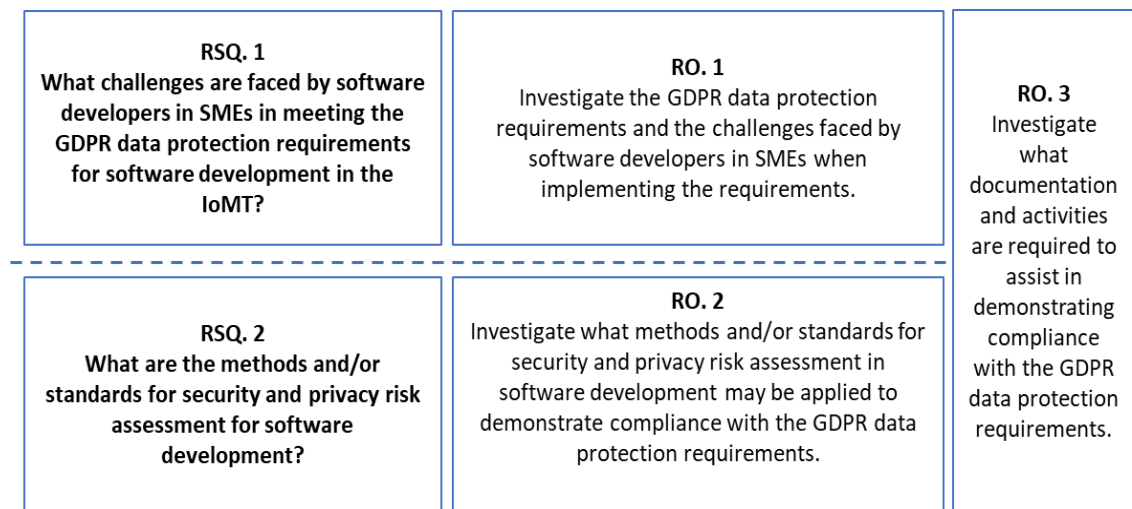


Figure 2.1 Research sub-questions and objectives addressed in literature review

The chapter begins with a review of what the IoMT is. It continues by presenting what data in flow in the IoMT looks like. The chapter continues with a review of data security and privacy in the IoMT. This section then outlines the requirements for security and privacy in the IoMT. The section continues by outlining the challenges faced by software developers in meeting security and privacy regulatory requirements and best practice. The chapter then examines the data protection requirements of the EU, the GDPR. The GDPR is the regulatory emphasis as the research is completed in an Irish SME. This section will focus on data security and privacy in the context of the GDPR data protection principles. It also reviews the factors that need to be considered to meet the requirements of a DPIA. The next section of the chapter examines the existing standards and guidelines for data security and privacy of data in flow in the IoMT. The next section describes the area of data security and privacy risk assessment and corresponding standards and models. The chapter continues with a section outlining

Chapter 2 Literature Review

existing frameworks in this domain. The final section discusses security and privacy controls.

The literature review presented in this chapter acts as a foundation on which the research is built. This research incorporates many aspects. This is due to the complexities of ensuring the security and privacy of health data in the IoMT within regulatory and best practice requirements. The research aims to bring together many facets with the aim to assist SMEs and developers inexperienced in this domain. The objective is to provide a systematic process for the aforementioned groups to provide evidence, of data security and privacy implementation within their IoMT products. Understanding the research previously published will ensure the research presented in this thesis will be distinct and up to date. The literature review performed was a traditional or narrative review. The traditional or narrative review approach was taken because it can be helpful in developing conceptual or theoretical frameworks (Coughlan et al. 2007). This supported the objective of the research. A traditional or narrative review:

- Summarises, synthesises, and discusses literature on chosen topic; selective with regard to sources included
- Purpose: to give a comprehensive overview of the literature in a chosen area; to identify gaps in existing research; to develop conceptual framework; to refine research topic/question (Cronin et al. 2008, p.38).

This review approach was completed to help focus the broad research question and topic selection and help the refinement of the topic (Coughlan et al. 2007). The approach helped to establish the theoretical framework and focus or context for this research. It supported establishing the factors required to address the RQs and RSQs 1-3 presented in Figure 2.1 above and bringing these together to provide a systematic framework. The research is based in a theoretical framework applied and validated in practice. This was facilitated by the fact the researcher was embedded within the organisation and the software development team.

The review began with identification of the key areas, keywords and search strings developed from the research questions, presented in Table 2.1. Papers were identified using Google Scholar, IEEE Xplore, Elsevier, and ACM Digital Library. The returned papers from this search were considerable and the following screening criteria were applied:

Chapter 2 Literature Review

- A date limit was applied to each key area that aligned with its significant entrance in the field in the literature, see Table 2.1;
- The researcher read the title, abstract and conclusion;
- Any research published in a language other than English was discarded.

Table 2.1 Literature review key areas, keywords, and search strings

Key Areas	Keywords	Search Strings	Date Limit
IoT IoMT Mobile Medical Apps (MMA)	Data in Flow Security Privacy Cybersecurity Health data	<ul style="list-style-type: none"> • Security AND in the IoT or IoMT AND (implementation OR difficulties OR challenges OR issues OR problems OR practices OR methods OR assessment OR measurement OR techniques OR tools OR procedure OR best practice) • Privacy AND the IoT IoMT (implementation OR difficulties OR challenges OR issues OR problems OR practices OR methods OR techniques OR tools OR procedure OR best practice) • Cybersecurity AND IoT OR IoMT AND (implementation OR difficulties OR challenges OR issues OR problems OR practices OR methods OR assessment OR measurement OR techniques OR tools OR procedure OR best practice) • Security AND Privacy in the IoT OR IoMT • Health data security OR privacy AND IoT OR IoMT • MMA data (security OR privacy) 	IoT 2005 IoMT 2015 Privacy IoT AND IoMT 2015 2015 2010 2010 2010
GDPR	Data Protection	<ul style="list-style-type: none"> • GDPR AND (application OR data protection OR SMEs OR developers OR implementation in products OR SMEs) • DPIA AND (developers OR SMEs OR implementation OR practice OR procedure OR best practice) • Data protection AND (data security OR data privacy) 	2015
Standards Best Practice	Security Privacy Network security Cybersecurity App development Software development Risk assessment IoT IoMT	Standards AND OR Best practice (security OR privacy OR network security OR cybersecurity OR app development OR app development security OR app development privacy OR software development OR risk assessment OR risk management OR IoT OR IoMT OR IoT security OR IoMT security OR IoT privacy OR IoMT privacy)	No limit
Threat modeling	Security Privacy Software development	Threat modeling AND IoT OR IoMT AND (frameworks OR risk assessment OR best practice OR development OR	2004
Security and Privacy Controls	Security Privacy Health data Medical devices	Security OR Privacy controls AND (medical data OR medical devices OR health data)	2008

The papers from this search were then uploaded into reference manager Mendeley. Mendeley was used to manage the research papers to ensure they covered a number of different publishers, years, and authors and to eliminate any repetition. The research papers were sorted and tagged according to keywords and corresponding search strings and to support cross-referencing of key areas. The researcher also used the backward and forward snowballing search strategy when the full paper was read. Greenhalgh and Peacock (2005), reported that up to 51% of references in a review are identified by snowballing. Snowballing is seen by some authors as a complementary search strategy (Kitchenham et al. 2010). The researcher reviewed the references in a start set of papers in the key areas. The start set of papers were established by the researcher using the key areas and keywords. At the point of reviewing and uploading to Mendeley, the researcher checked if the paper had already been examined and found earlier through the initial search or either previous backward or forward snowballing. Papers that fulfil the basic criteria listed above from the snowballing strategy were uploaded into the appropriate Mendeley folder and tagged.

2.1.1 The Internet of Medical Things (IoMT)

The term Internet of Things (IoT), was first used in a presentation given by Kevin Ashton at Proctor and Gamble in 1999 (Ashton 2009). The presentation described an emerging global internet-based information service architecture. This information service architecture was described in an ITU Internet Report in 2005: The Internet of Things as a new dimension having been added to information and communications technologies (ICTs) “*from **anytime, any place** connectivity for **anyone**, we will now have connectivity for **anything***” (ITU 2005, p.2). Today the definition of IoT still remains ambiguous (Minerva et al. 2015) with no universal definition (Whitmore et al. 2015; Lynn et al. 2020). Minerva et al. (2015, p.73) suggest that this lack of a specified definition is because the scope of an IoT system changes, from “*a small system which contains uniquely identifiable things and small sensors to a system that interconnects millions of things with a capacity to deliver complex services.*” Essentially, the IoT is a wide range of entities, including people, machines, and things that are interconnected into information space anywhere at any time (Minerva et al. 2015). The things in the IoT, can comprise a multitude of diverse devices from consumer devices, such as phones, tablets and wearables, to industrial sensors, actuators and monitors (Lynn et al. 2020).

The development and growth of the IoT has transformed the healthcare industry (Papaioannou et al. 2020). The integration of medical devices within the IoT has led to the emergence of the Internet of Medical Things (IoMT) (Balandina et al. 2015; Yaacoub et al. 2020). The IoMT is essentially an IoT-based solution that enables the development of IoT enabled healthcare systems for monitoring, diagnosis and a variety of different kinds of healthcare uses (Joyia et al. 2017). It is a connected system, consisting of a variety of networks, medical devices and applications that collect data that are then provided to medical healthcare IT systems (Joyia et al. 2017; Alsubaei et al. 2018; Marr 2018). The IoMT is a rapidly growing domain (Yaacoub et al. 2020). A report from the Deloitte Centre for Health Solutions proposes the IoMT market worth, will be \$158.1 billion in 2022 (Taylor et al. 2018). The report states that the IoMT and its relationship to medical technologies (MedTech) *“is instrumental in helping healthcare achieve better patient outcomes, lower climbing health care costs, improve efficiency and activate new ways of engaging and empowering patients”* (Taylor et al. 2018). The importance of this domain in the Irish context is demonstrated by the fact that it is one of the key research priority areas for Ireland from 2018 to 2023 (Department of Enterprise Trade and Employment 2018). The area of focus combines the IoT and devices, wearables, routers, sensors, actuators, and associated IT services and platforms in healthcare. The focus on these areas is due to the recognition in Ireland that the pace and scale of healthcare transformation will be exponential if MedTech can harness the IoMT (Taylor et al. 2018). Ireland’s MedTech sector *“has become one of the leading producers of medical device products globally and is the second largest exporter of medical technologies products in Europe”* (Department of Business Enterprise and Innovation 2020a). In fact, the MedTech sector in Ireland is now recognised as one of the top five emerging global hubs (Irish Medtech Association 2019; Department of Business Enterprise and Innovation 2020a).

2.1.2 Data Flow

The term data flow was published in ISO/IEC 2382-7:2000 Information technology – Vocabulary - Part 7: Computer programming (ISO/IEC 2000). The term remains unchanged in the revised standard 2015 published standard and is defined as the *“movement of data through the active parts of a data processing system in the course of the performance of specific work”* (ISO/IEC 2015a). This term is also used in ISO/IEC TR 20748-1 Information technology for learning, education and training (ISO/IEC

2016b). Data flow in the IoMT is determined by many factors, which includes but is not exclusive to:

- The size of the system being developed;
- The intended use of the data;
- How the system is to be developed;
- What networks are available at the time;
- What the data will be used for;
- Where the data will be stored and processed; and
- What type of processing will happen to the data.

Other factors that determine the data flow in the IoMT is the size of the organisation completing the development, which will have a bearing on the level of developer's experience and the technology and services available.

Figure 2.2 on pg. 31, presents a high-level potential data flow in the IoMT using examples of smart wearables such as watches and smart things such as monitors and medical devices. This diagram presents that data in the IoMT could flow everywhere (Piccarreta and Hogan 2018). An example of this potential flow of data in the IoMT is presented in Figure 2.2 on pg. 31. A particular example taken from this diagram would be a continuous glucose monitoring (CGM) device that wirelessly connects to a mobile app. The CGM device is attached to the individual's body, presented by a picture on the left of Figure 2.2 on pg. 31 in user grouping. The CGM device collects glucose level readings continuously. For instance, a simple communication task could be in monitoring the users' sugar level for reporting. The device transmits the glucose level readings wirelessly to a mobile app on the individual's smartphone. The CGM could send this data to the app using various wireless technologies. The mobile app processes the glucose level data and displays it in real-time to the individual. This information could then be sent across networks and through network infrastructure devices to arrive at a doctor's surgery system or cloud system, where it could be stored, monitored and further processed. The cloud-based platform could potentially use machine learning algorithms to analyse the data and identify patterns and trends in the individual's glucose levels. This information could then provide insights and recommendations to the individual or their healthcare provider to help manage their diabetes more effectively. The healthcare provider can also access the individual's glucose level data through the cloud platform and use it to make treatment decisions and adjustments as needed. Overall, this data flow

Chapter 2 Literature Review

allows for continuous monitoring and analysis of glucose levels, which can lead to improved diabetes management and better health outcomes for individuals with diabetes. The information could potentially pass between multiple applications, various technologies, or other devices to get stored and further processed on the cloud or in a local database.

Other examples presented in Figure 2.2 overleaf, include in smart things for remote patient monitoring of vital signs, EKG or blood pressure. Wearable devices such as smart watches and clothing. They are designed to monitor various health metrics such as heart rate, breathing rate, and posture. They contain embedded sensors that transmit data wirelessly to a mobile app for analysis and tracking.

For this research, data flow is the path data takes through a system comprised of software, hardware, or a combination of both, that includes all nodes through which the data travels, from its original source to its end users. It is the movement of data as it passes from one component to the next across networks, network infrastructure devices, between apps, individual systems, and devices, taking into consideration how it changes form during the process. In short, data flow in the IoMT can be through various apps, individual systems, devices, technologies, and public and open networks. During this movement the data can change form from data to information and contrariwise.

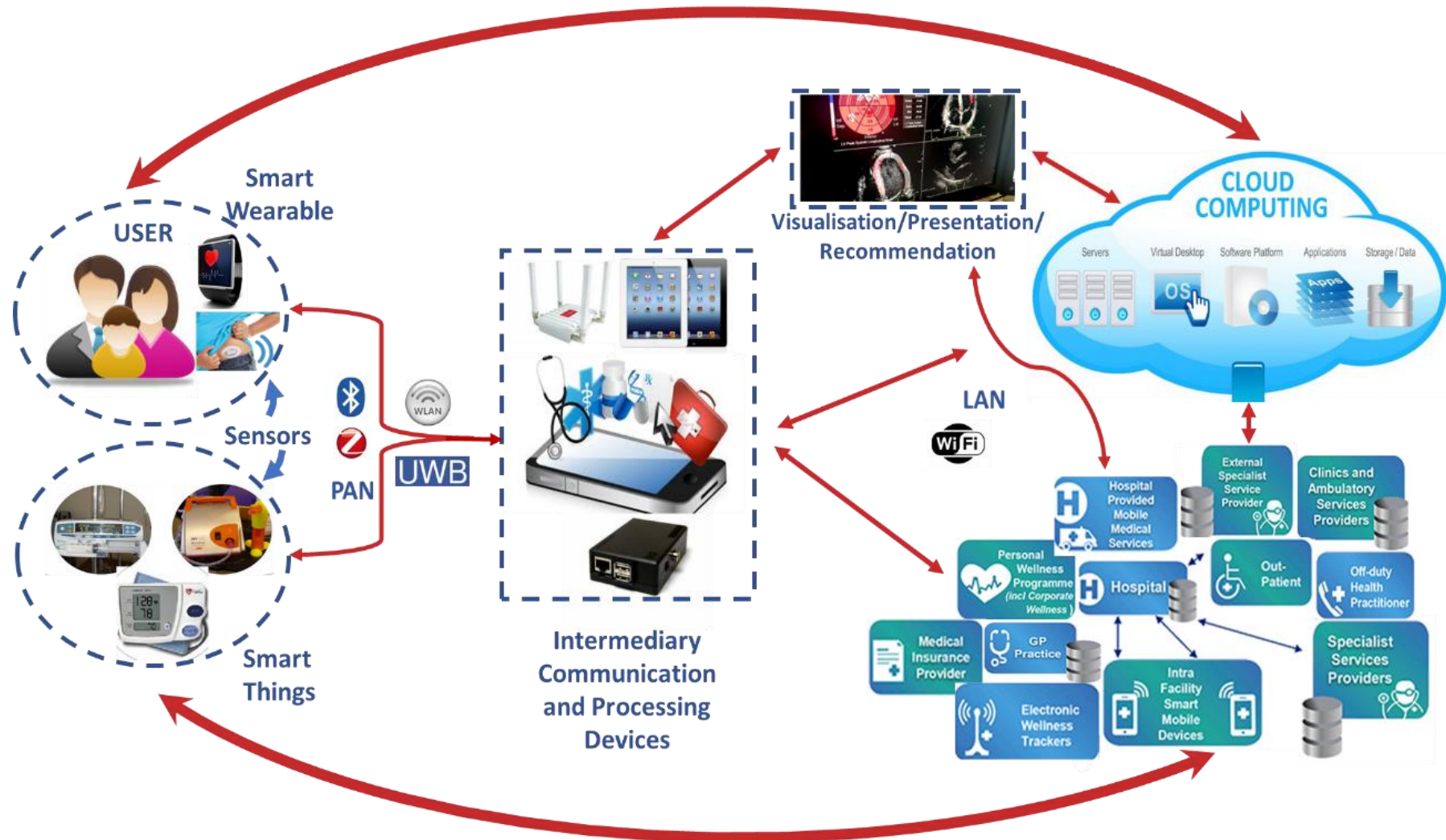


Figure 2.2 High level potential data in flow in the IoMT

2.1.3 Data Security and Privacy in the IoMT

The IoMT is a growing domain and as it grows, cybersecurity risks have risen (Brien et al. 2018; Papageorgiou et al. 2018). The increasing digitisation of health data across many platforms combined with valid concerns about health data privacy, has created a situation in which healthcare organisations and systems are vulnerable to cyberattack. In recent years, the IoMT has been at the forefront of cyberattacks (Alsubaei et al. 2019). The Verizon 2018 Data breach investigations report (2018), outlined the number of data breaches reported was 2216 from 65 countries and of which the healthcare industry faced 536 breaches and this increased in 2020 (Bitglass 2021). This implies that the healthcare industry has faced the highest number of breaches among all industries (Seh et al. 2020). The Ponemon Institute/IBM Security *2019 Cost of a Data Breach Report* (2021), revealed that the healthcare industry has the highest breach costs with an average mitigation cost of \$6.45 million. The report also stated that healthcare data breaches typically cost 65% more than data breaches experienced in other industry sectors. The demand for end-to-end communication in the IoMT requires comprehensive data privacy as well as security (Basir et al. 2019). The sensitivity of data in the IoMT means that detailed consideration of data security and privacy is required. Security and privacy of patient health data are two essential concepts because of the increase of cybersecurity risks in the IoMT (Sun et al. 2018).

One of the main aspects in the IoMT that leaves health data vulnerable to cybersecurity and privacy breaches is interconnectivity (Anandarajan and Malik 2018). As stated by Liaqat et al. (2020, p.698), "*IoMT infrastructure comes at the cost of severe cyber threats and attack countermeasures.*" A range of serious consequences can result from attacks on patient information, medical devices or a hospital's systems and operations (Ponemon Institute 2018). The degree of severity when an attack is successful in the IoMT could cause a serious failure. Concerns relating to disruptions or data breaches in the IoMT could directly affect delivery of services, clinical care, patient privacy, and patient safety (Williams and Woodward 2015; Williams and McCauley 2017; Papaioannou et al. 2020). As seen in Figure 2.2 on pg. 31, there are numerous IoMT deployment scenarios. The data flow through the IoMT navigates a myriad of systems and networks and at every point requires ensuring the security and privacy of data.

As seen in Figure 2.2 the inherent mobility capabilities of wireless communication systems make them instrumental in the adoption of IoMT services and applications. They enable highly scalable and flexible deployments. The communication can be over varied frequencies short or long range. Short range communication protocols typically used with sensors include Bluetooth, ZigBee, Wi-Fi, and mobile communications (Gardašević et al. 2020). These sensors require connectivity to an established gateway for communicating and storing information via networks (Dwivedi et al. 2022). There are many forms of wireless networks. Examples of wireless networks currently used in the IoMT include:

- Local Area Network (LAN) is used to connect medical devices and systems, such as patient monitors, infusion pumps, ventilators, and other medical equipment, within a healthcare facility or a specific location, for example a hospital. LAN can be wired, wireless, or a combination of both, depending on the specific requirements of the healthcare facility. Wireless Local Area Network (WLANs) are usually implemented as extensions of existing wired LANs to provide enhanced user mobility. WLANs are groups of wireless networking nodes within a restricted geographic area (Zamani and Ahmad 2014), such as a hospital building, that are capable of radio communications. WLANs provide a wireless network infrastructure which enable the connectivity of IoMT devices that allow medical devices to communicate with each other and with healthcare providers. LAN and WLANs can facilitate real-time monitoring and diagnosis of patients. An example would be remote patient monitoring, where medical data is transmitted wirelessly from wearable devices to healthcare providers. This facilitates the continuous monitoring of patients outside of traditional healthcare settings. However, it's important to note that the security and privacy of patient data in IoMT both LANs and WLANs are critical concerns. It is crucial to ensure the confidentiality and integrity of patient data. And therefore, appropriate security measures, such as encryption, access control, and data backup, must be implemented. It is essential that developers not only consider the security of the WLAN, but also how it may affect other networks that are accessible through it, such as internal wired networks or LANs (Souppaya and Scarfone 2012);
- Wireless Sensor Networks (WSNs) are networks consisting of numerous small, low-power devices called sensors that are equipped with sensing, processing, and communication capabilities (Al-Karaki and Kamal 2004). They are typically

designed to be low-cost, energy-efficient, and highly scalable, allowing them to be deployed in large numbers and in diverse environments. In the IoMT, WSNs are typically deployed in hospitals, clinics, and other healthcare settings to monitor patients' vital signs, track medication usage, and provide real-time alerts to healthcare providers. As presented Figure 2.2, WSNs can be used in home healthcare settings to monitor patients' health remotely, allowing healthcare providers to detect and respond to health issues before they become more serious. WSNs in the IoMT typically consist of a network of sensors that are placed on or inside the patient's body, such as wearable sensors, implantable sensors, and smart medical devices (Al Shorman et al. 2020). These sensors collect data on various physiological factors, such as heart rate, blood pressure and glucose levels, and transmit this data wirelessly to a central monitoring system (Anandarajan and Malik 2018). The central monitoring system can then analyse the data and provide real-time alerts to healthcare providers if any anomalies are detected (Anandarajan and Malik 2018). The use of WSNs in the IoMT can help improve patient outcomes, reduce healthcare costs, and enhance the quality of care provided to patients (Joyia et al. 2017);

- Body Sensor Networks (BSNs) are a type of WSN that are specifically designed to collect and transmit physiological data from the human body, consisting of numerous biosensor nodes or a network of wearable or implantable sensors that are attached to different parts of the body, such as the chest, wrist, and ankle (Kompara and Hölbl 2018). They can be used to measure various physiological parameters, such as heart rate, blood pressure, body temperature, respiratory rate, and oxygen saturation. The data gathered can be used to monitor patients with chronic conditions, such as diabetes, heart disease, and respiratory disorders. Like WNSs, BSNs are typically focused on the collection and transmission of data from the body to a central monitoring system (Al Ameen et al. 2012). This data can be analysed and used for purposes such as health monitoring, disease management, and performance optimisation. BSNs can also be integrated with other medical devices and systems, such as electronic health records (EHRs) and telemedicine platforms, to enable remote monitoring and healthcare delivery. They can also be used to detect motion, posture, and activity levels. This use can be used to monitor athletes' performance, prevent injuries, and improve training programs;

- Wireless Body Area Network (WBANs) are a type of wireless network that connects multiple medical devices and sensors placed on or around the body (Khan and Yuce 2010; IEEE Standards 2012). Saleem et al. (2011, p.1384) defines an “*in-body area network allows communication between invasive/implanted devices and a base station. An on-body area network, on the other hand, allows communication between non-invasive/wearable devices and a base station*”. WBANs typically focus more on the integration of multiple devices and the coordination of data exchange among them, while BSNs are more focused on collecting and transmitting data from the body to a central monitoring system.;
- Personal Area Networks (PANs) and Wireless Personal Area Networks (WPANs). A PAN is a network that connects devices within an individual's personal space, typically within a range of about 10 meters and can be created using various technologies like Bluetooth and ZigBee. It can include wired and wireless devices. A WPAN is a type of PAN that uses wireless technologies to connect devices. WPANs are commonly used for a range of IoMT applications, wireless medical sensors, and other medical devices (IEEE Standards 2012). The most common technology used in WPANs is Bluetooth.

With the evolution of the IoMT and wireless healthcare technology, the boundaries between these concepts are becoming increasingly indistinct. However, there are considerations for data security and privacy in these networks. These include; secure management of decryption and encryption operations; ensuring the availability of patient information at all times; ensuring the data authentication and integrity and protecting the confidentiality of the data from disclosure (Movassaghi et al. 2014).

As outlined above, these networks of sensors are attached to or implanted inside the body of a patient and to transmit the information gathered to a gateway, short-range communication technologies are typically used. Some of the short-range communication technologies used in the IoMT and presented in Figure 2.2 are now outlined. Yaqoob et al. (2020) noted that the majority of medical devices use Bluetooth/Bluetooth Low Energy (BLE), ZigBee, Wi-Fi and radio frequency channels to communicate.

Bluetooth wireless technology is an open standard for short-range radio frequency (RF) communication used primarily to establish WPANs (Padgette and Padgette 2017). BLE is a low power subset of the Bluetooth protocol that is commonly used in the IoMT that require short distance communication, low latency and low bandwidth such as

applications like sports and fitness monitors and portable medical devices (Koutras et al. 2020). Both Bluetooth and BLE are widely used in medical devices and the IoMT (Zubair et al. 2022). They are used in medical devices, such as blood glucose monitors, heart rate monitors, blood pressure monitors, and wearable devices for remote patient monitoring. They are used due to their low power consumption, low cost, support for multimedia, such as data and audio streaming and the ability to transmit data over short distances wirelessly (Al Ameen et al. 2012; Zubair et al. 2022). Their use in the IoMT can provide a range of benefits, including real-time monitoring of patient health, remote diagnosis and treatment, and improved patient outcomes. However, the use of Bluetooth and BLE in the IoMT also presents security risks, such as unauthorised access to patient data, interference with medical devices, and attacks on the network (Zubair et al. 2022). It is important for software developers to mitigate these risks and implement robust security measures, such as encryption, authentication, and access control. It is important to ensure that the devices and networks in the IoMT are secure to protect patient privacy and prevent security breaches.

Ultra-Wide Band (UWB) has gained attention for use in medical networks, particularly for WBANs and wearable devices (Garcia-Pardo et al. 2018). UWB offers several advantages over other wireless technologies, including high data rates, low power consumption, the ability to penetrate through obstacles and the ability to accurately locate and track medical devices (ISO/IEC 2016a). A key benefit of UWB for medical networks is its ability to provide precise and accurate location and tracking information, which is critical for monitoring patients in real-time (Jiang et al. 2011). It is used in the IoMT as it is suitable for real-time applications in radio frequency sensitive settings such as hospitals (Koutras et al. 2020). UWB can also be used for non-invasive high-resolution imaging and sensing, which can aid in the diagnosis and treatment of medical conditions (Jiang et al. 2011). Potential security issues with UWB in the IoT and IoMT is the risk of unauthorised access to patient data. Like other short-range communication technologies UWB technology allows for the transmission of large amounts of data over short distances. With this, there is a possibility that sensitive patient data could be intercepted by unauthorised individuals or entities (Chanal and Kakkasageri 2020). Software developers should implement strong encryption protocols to protect the data in transit and at rest to mitigate this risk. Another concern is the potential for UWB devices to be hacked or manipulated. UWB devices rely on wireless communication protocols, which are vulnerable to attacks such as man-in-the-middle attacks, denial of service attacks, and

spoofing attacks (Koutras et al. 2020). An additional consideration with UWB technology, is the potential to compromise patient privacy. As UWB devices are capable of precise location tracking, there is a risk that sensitive information about a patient's location and movements could be inadvertently shared or accessed by unauthorised parties (Yaghoubi et al. 2022). To address this, strict privacy policies and procedures to ensure that patient data is only accessible to authorised individuals and is not shared without patient consent should be applied.

ZigBee is another wireless communication protocol that is widely used for IoMT devices. It uses low-power digital radio signals to enable devices to communicate with each other (Ngoc 2008). ZigBee was designed to provide low-cost, low-power, wireless mesh networking capabilities for a variety of applications (Omojokun 2015). This means it is used in a wide range of applications in WPANs. The benefit for WPANs is ZigBee mesh networking capabilities allow devices to communicate with each other and relay data through the network, ensuring reliable connectivity even in challenging environments such as hospitals. This means it can be easily deployed in hospital environments, where there may be a large number of devices in close proximity (Omojokun 2015). These are important factors in medical applications, where devices may need to operate for long periods of time on battery power and transmit critical data reliably and securely. ZigBee's security features, including encryption and authentication (Michaels et al. 2017), which are essential for data security and privacy in the IoMT. Correct implementation of these features is necessary to help to protect sensitive medical data from unauthorised access or tampering. This is especially important in IoMT applications, where patient data privacy and security are critical.

The dominant family of WLAN standards is IEEE 802.11, also known as Wireless Fidelity (Wi-Fi)[®] (Zamani and Ahmad 2014). Wi-Fi can play an important role in connecting medical devices, sensors, and other healthcare equipment to the internet and to each other. Wi-Fi is a common gateway facility, however, a relatively higher power usage and inconsistency of the network are the main limiting factors when used in hospitals (Dwivedi et al. 2022). Additionally, due to data security and privacy concerns in healthcare, any Wi-Fi in the IoMT must be carefully planned to prevent unauthorised access to patient data, signal disruption by physical barriers or other sources of electromagnetic interference and must be implemented with care and attention (La Polla et al. 2013).

Long-range wireless technologies such as cellular networks 4G LTE and 5G are used by the IoMT to provide wireless connectivity between medical devices, healthcare providers, and other connected devices. These networks are used by the IoMT because they provide high-speed data rates and low latency rates. This supports transferring large amounts of medical data, such as medical images, videos, and other diagnostic data essential for real-time applications, such as remote surgery and telemedicine, where delays in data transmission could have serious consequences (Li 2019). Also, these networks offer reliable and stable connectivity and wide coverage, even in areas where other communication technologies may not be available or may experience interference, making them suitable for IoMT applications in both urban and rural areas (Mishra et al. 2021).

Ensuring data security and privacy has been addressed both 4G LTE and 5G. The networks have implemented several measures to address these concerns including. 4GLTE uses AES (Advanced Encryption Standard) encryption algorithm for data transmission and mutual authentication. 5G have further improved this measure by implementing network slicing to create virtual networks that are customized for specific applications, such as healthcare. This helps to prevent unauthorised access to data by isolating it from other parts of the network. It also uses stronger encryption algorithms and more advanced authentication protocols, such as the 5G-AKA (Authentication and Key Agreement) protocol, which provides better protection against hacking and unauthorised access (Mishra et al. 2021). However, privacy concerns could arise from data, location and identity exposure. In addition, when including 5G in an IoMT system the manufacturer needs to consider there are no physical boundaries of 5G network as they use cloud based data storage (Ahmad et al. 2017). This will directly impact decisions in the IoMT system, as privacy laws and subsequent requirements for storage of user data differ country by country.

Data security and privacy protection in wireless and sensor technologies such as Bluetooth, UWB, ZigBee, Wi-Fi, etc., against potential attacks is a must in the IoMT. IoMT devices that rely on wireless communication protocols, are vulnerable to attacks such as man-in-the-middle attacks, denial of service attacks, and spoofing attacks (RM et al. 2020). To ensure data flow through communication technologies does not compromise data security and privacy, robust measures must be considered and enforced before deploying in the IoMT (Yaacoub et al. 2020). Wireless networks and communications technologies typically need to support several data security and privacy objectives

including; confidentiality, integrity, availability and access control (Zamani and Ahmad 2014).

Other considerations for security and privacy in the IoMT include the interoperability and interconnectivity of the domain. The security and privacy of data is more exposed due to the complexity of transferring data through many potential platforms, systems, devices, and networks domains. There are *“a wide range of communication protocols, across multiple protocol stack layers, need to be supported to ensure interoperability between nodes and endpoints”* (Gebremichael et al. 2020, p.152354). The lack of global standards and agreement on technologies in the IoT/IoMT makes interoperability a problem (Tan and Wang 2010; Cavalcante et al. 2015). As noted by Seliem et al. (2018), although existing network protocols implement highly secured measures they struggle with the communications in resource-constrained environments. The resource constraints of the IoT/IoMT makes it difficult to apply security and privacy preserving techniques. They comment that this may *“lead to creating barriers rather than connections between different machines”* (Seliem et al. 2018, p.10), which can lead to security and privacy vulnerabilities. An additional complication for security and privacy in the IoMT is due to the fact that data storage and processing is typically assigned to third-party cloud services, opening another attack dimension (Gebremichael et al. 2020).

2.1.4 Summary

This section presented an introduction to the IoMT, data flow and data security and privacy in the IoMT. Section 2.1.1 outlined how the integration of medical devices within the IoT has led to the emergence of IoMT. It presented that the IoMT is a rapidly growing domain that is instrumental in helping healthcare achieve better patient outcomes, lower climbing health care costs, improve efficiency and activate new ways of engaging and empowering patients. An overview of data flow was provided, as the movement of data through the active parts of a data processing system during the performance. The description of data flow through the IoMT described various nodes through which the data travels, from its original source to its end-users. Examples of potential data flow paths in the IoMT were provided. The final section 2.1.3 outlined that with the growth of the IoMT and increase in cybersecurity risks in the healthcare industry has also grown. The interconnectivity of health data across many platforms combined with valid concerns about health data privacy has created a situation in which healthcare organisations and

systems are vulnerable to cyberattacks. Due to the sensitivity of data in the IoMT, detailed consideration of data security and privacy is required. The interconnectivity in the IoMT leaves health data vulnerable to cybersecurity and privacy breaches. A range of networks and technologies that support IoMT were discussed. Within this discussion the security and privacy concerns in relation to using these elements to support data flows in a system was provided.

2.2 Requirements for Security and Privacy in the IoMT

The findings of this section are used to address research sub-question 1.

RSQ. 1: What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?

Data protection is upheld by different legal instruments, depending on the jurisdiction (De Francesco 2019). The data protection regulatory obligations that include security and privacy requirements, in the EU are determined by the GDPR.

The GDPR states:

1. *Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*
2. *This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (EU General Data Protection Regulation (GDPR) 2016, sec.Art. 1).*

However, it is recognised in this domain that safety and security can be in conflict (Katzis et al. 2016), along with other attributes such as privacy. The safety obligations are determined by the health data that is involved in this domain that directly impact the physical safety of a patient (Koutras et al. 2020). Given this research is in the IoMT domain, it is crucial that safety from harm is the key priority for the patient. This is enforced in the requirements for any standalone medical device. The regulation requires medical device software must be analysed to consider any risks associated with the use of the device that may lead to direct or indirect harm to the patient (HPRA 2020). A manufacturer must apply a risk management system for identifying risks associated with their medical device software (IMDRF Software as a Medical Device (SaMD) Working Group 2014). The process must include estimating and evaluating the risks, controlling

these risks, and monitoring the effectiveness of that control. The recognised standard to implement the risk management system is ISO 14971:2019 Medical devices - Application of risk management to medical devices (ISO 2019). It is important in this domain to ensure that any controls implemented for security and privacy do not diminish either security, privacy, or safety of the user. This means for standalone software in the IoMT security, privacy and safety are required and linked through regulation and standards.

Security and privacy principles are led by regional regulatory requirements and can be embedded as a part of international certification such as ISO 27001. Security principles are guided in an organisation through the 'information security policy' and the associated policies developed for an organisation (ISO/IEC 2017b). The security principles are guided by standards and the desired security properties the organisation wants to preserve. ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013) is the most widely used standard guiding the development of the security principles for an organisation (ISO/IEC 2017a). ISO 27001 is an international standard which is recognised globally for managing risks to the security of information an organisation holds. ISO/IEC 27701 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (ISO/IEC 2019) is the standard guiding the development of privacy principles for an organisation. ISO 27701 is an extension of ISO 27001 that provides assurance that your organisation complies with GDPR and other applicable personal identifiable information (PII) regulations. ISO/IEC 27701 also links with the eleven privacy principles of ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework (ISO/IEC 2018b). These standards are discussed further in section 2.5. It is recommended that any security and privacy principles should map to those of the organisation and balance the regulatory data privacy and security obligations (ISO/IEC 2017a).

Privacy is a fundamental human right (Danezis et al. 2014) and includes the rights of data subjects to have their information protected to uphold their privacy. Privacy is a multi-faceted concept and therefore it is difficult to find a global, consistent and overarching definition of privacy (Solove 2002; Alshammari 2019). Data privacy means the data can only be accessed by the people who have authorisation to view and use it (Sun et al. 2018). Alshammari, propose an operational definition of data privacy for privacy engineering:

“Data privacy can be defined as the collection, processing and dissemination of personal data in a manner that prevents the occurrence of adverse privacy events and their negative impacts on data subjects.”
(2019, p.16)

The concept of Privacy by Design (PbD) was introduced and defined by Ann Cavoukian *to capture the notion of embedding privacy into technology itself – making it the default, delivered through various PETs* (Cavoukian 2009, p.iv). Privacy-Enhancing Technologies (PETs) are technologies that prevent unnecessary or unlawful collection, use and disclosure of personal data and provide ways for the data subjects to exercise control over their personal data (Cavoukian 2009; Danezis et al. 2014; Alshammari 2019). Cavoukian developed the approach *“by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems”* (2009, p.3). This fundamental PbD research provided *The 7 Foundational Principles* (Cavoukian 2010). These principles became the foundational concepts for much PbD research (Elshekeil and Laoyookhong 2017). Privacy principles within software development are an emerging field. Privacy principles are *“a set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems”* (ISO/IEC 2018b, p.3).

Article 25 of the GDPR regulation requires *“data protection by design and by default”* (EU General Data Protection Regulation (GDPR) 2016, p.23). This is imposed through the regulation’s data protection principles, that require developers to employ security and privacy from the beginning of system development (EU General Data Protection Regulation (GDPR) 2016; Galvez and Gurses 2018; Stalla-Bourdillon et al. 2020). Stalla-Bourdillon et al. (2020), maintains that data protection by design plays a key role in enabling and demonstrating compliance with the GDPR.

The principles of Security by Design (SbD) and PbD, within the context of software engineering, means security and privacy are designed into a development project from initiation, into the devices, the communication protocols and the services (Mouratidis and Kang 2013; McManus 2018; De Francesco 2019). Since IoMT systems produce and deal with sensitive health data, it is critical that data security and privacy is highlighted from the very beginning of development (Minerva et al. 2015). This means that at the core of development in the IoMT, it is essential that both security and privacy of data is prioritised (Sun et al. 2018).

The disadvantages of not implementing data security from a project outset, is referred to as far back as Schneier and Shostack in 1999. Schneier and Shostack state that when there are attempts with the ‘bolt security on’ approach, to bolt security on at a later phase or after a system is designed, *“has been shown to be difficult, expensive, and failure prone”* (1999, p.9). The PbD approach is characterised by anticipating and preventing privacy-invasive events before they happen (De Francesco 2019).

Additionally, financial loss is an important consideration for organisations and compliance with the GDPR is necessary to avoid fines (Ataei et al. 2020). It is also important that the developers and designers understand the negative impacts that a data breach can have on an organisation’s reputation and also on an individual’s life. SbD and PbD are built on the preservation of security and privacy properties. Security and privacy properties are created to protect the principles the organisation is required to adhere to through regulation. Security and privacy properties are adopted in development to reduce the exposure of systems and services from attackers who could gain access and compromise sensitive data.

Traditional data security means that data is stored and transferred securely (Li and Lou 2010). Security properties are high-level security goals to protect information from violation in storage and transfer (Yskout et al. 2006). The model of security properties was based on a way to guarantee that a security policy, protocol or mechanism are met (Focardi and Gorrieri 2000). The ISO/IEC 27000 series standard, asserts that the preservation of properties such as confidentiality, integrity and availability (CIA) of information is fundamental (ISO/IEC 2010). The traditional data cybersecurity properties ensure the confidentiality, integrity and availability of information, also known as the CIA triangle model or triad (Hatzivasilis et al. 2019). However, Whitman and Mattord note that, *“The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triad model no longer adequately addresses the constantly changing environment”* (2011, p.8). Therefore, the review examined network security and discovered Part 3 of the ISO/IEC 27033 standard for network security (ISO/IEC 2010). The security properties in this standard include authenticity, non-repudiation, authentication, non-repudiation, access control, opacity, communication or transport security and reliability. Other researchers include some of these and other security properties for the IoT and IoMT. Papaioannou et al. (2020), include authentication as one of the essential security requirements of an IoMT based healthcare system. Gebremichael et al. (2020) argue that; Authentication, Access Control, and

Authorization (AAA) are three factors required for security in the IoT and accordingly the IoMT.

Privacy principles and properties are interchangeable. Privacy principles are high-level privacy goals to ensure regulatory compliance and the rights of the user and the privacy of their data. Privacy properties allow people to act without their identity or their actions being identifiable (Fremantle 2017). As stated above, the foundational privacy principles provided by Ann Cavoukian, assisted in providing the basis for research in the development of privacy principles or properties. The review considered the privacy principles from ISO/IEC 29100, Cavoukian's 7 privacy principles, the GDPR and the privacy properties from LINDDUN TM. The review established for the research:

- The GDPR as the key data protection principles because the organisation and their clients requesting the data security and privacy requirements are based in the EU.
- The ISO/IEC 29100 eleven principles as guidelines for developers as part of the research. This standard was selected as it provides references to known privacy principles for information technology and specifies a common privacy terminology.
- LINDDUN groups as the privacy properties. LINDDUN was selected as it established the privacy properties to comply with established privacy terminology and regulatory influence (Deng et al. 2010). Additionally, LINDDUN is a privacy threat modeling methodology that supports a systematic analysis of systems to extract privacy threats in software designs (Wuyts et al. 2014).

Table 2.2 overleaf, presents the categories of principles and properties examined to support data privacy in the research. It provides the eleven privacy principles from ISO/IEC 29100 standard designed to provide organisations with a comprehensive approach to managing personal information protection. The 7 Foundational Principles of PbD developed by Ann Cavoukian to proactively address privacy risks and protect personal information throughout its entire lifecycle, from collection to disposal (Cavoukian 2010). Table 2.2 presents the seven principles to support the GDPR data protection principles. Finally, Table 2.2 lists the LINDDUN seven privacy properties designed to provide a comprehensive approach to privacy protection (Deng et al. 2010). The research also accepted the assertion by Yaacoub et al. (2020), that for the IoMT appropriate security and privacy solutions should include minimum computations and require minimal resources.

Table 2.2 Comparison of Privacy Principles

ISO/IEC 29100	Ann Cavoukian (Privacy by design)	GDPR	LINDDUN
Consent and Choice	Proactive not Reactive; Preventative not Remedial	Lawfulness consent, fairness, and Transparency	Linkability
Purpose legitimacy and specification	Privacy as default setting	Processing Legitimacy	Identifiability
Collection limitation	Privacy embedded into design	Data Minimisation (Limited to the purpose)	Non- repudiation
Data minimisation	Full functionality – Positive-sum, not Zero-sum	Storage limitation (No longer than necessary)	Detectability
User, retention and disclosure limitation	End-to-End Security – Full Lifecycle Protection	Integrity and confidentiality (unauthorised, unlawful, accidental loss, destruction, damage, technical or organisational measures)	Information Disclosure
Accuracy and quality	Visibility and Transparency – Keep it Open	Accuracy (Accurate, up to date, erased or rectified)	Content Unawareness
Openness, transparency and notice	Respect for User Privacy – Keep it User-Centric	Accountability (Responsibility + Findability Demonstrate compliance)	Non- compliance Unlinkability
Individual participation and access			
Accountability			
Information security			
Privacy compliance			

2.3 Challenges for Developers Implementing Security and Privacy in the IoMT

The findings of this section are used to address research sub-question 1.

RSQ. 1: What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?

Reports (Cisco 2017; Ponemon Institute 2018), determined that in terms of security maturity and privacy, the medical healthcare domain is behind other domains and vulnerable to cybersecurity attacks with SMEs particularly vulnerable. SMEs nowadays face significant information security risks due to the constant and evolving threat landscape (Manso et al. 2015). This is a concern particularly in Ireland, as according to Irish MedTech Association Ibec, four out of five MedTech companies are SMEs or start-ups (Irish Medtech Association 2019). SMEs make up approximately 99 percent of

businesses in the EU and contribute considerably to economic growth and a large share of employment (Jasmontaitė-Zaniewicz et al. 2021). The European Commission's *Green Paper on mHealth* findings are that this market is dominated by individuals or small companies, with 30% being individuals and 34.3% are small companies (defined as having 2-9 employees) (European Commission 2014). Research completed by the European Union Agency for Cybersecurity (ENISA) shows that SMEs within the EU seem to understand that cybersecurity is an important issue (ENISA 2021). However, the research also identified that some of the greatest challenges for SMEs are *“low awareness of the threats posed to their business by poor cybersecurity, the costs of implementing cybersecurity measures often combined with a lack of dedicated budget, the availability of ICT cybersecurity specialists, a lack of suitable guidelines aimed at the SME sector, and low management support”* (ENISA 2021, p.3).

It is acknowledged that the IoMT *“suffers from challenges such as the lack of security and privacy measures”* (Yaacoub et al. 2020, p.581). Reports from Araxan (2014; 2016) outlined that up to 22% of the hacked apps examined were listed on the US Food and Drug administration (FDA) approved list. Some of the reasons for this lack of measures have been listed above in the ENISA research. Other researchers and reports have also referenced some of the difficulties such as: budget constraints, deficiency in knowledge and lack of trained personnel (Dhillon, 2011; Cisco, 2017; Ponemon Institute, 2018); challenges due to the lack of security and privacy training and awareness (Yaacoub et al. 2020). Moreover, security and privacy issues have arisen due to the rush into the lucrative healthcare domain and the speed the healthcare domain is embracing IoT without a profound understanding of the security and privacy risks (Hatzivasilis et al. 2019; Sun et al. 2018).

Many SMEs are not as well equipped as large companies when it comes to dealing with the GDPR. In SMEs, developers and designers are the key groups responsible for bringing functional activities for compliance with GDPR in systems and products (Wagner et al. 2020). However, these groups lack the knowledge of secure coding practice (Weir et al. 2016). One of the main problems is that the GDPR does not provide clear guidelines for designers and developers on how to build GDPR compliant products (Ataei et al. 2020). Security and privacy risk management at development level is highly specialised. One of the main challenges in the IoMT is maintaining the patient's privacy without reducing the security level (Yaacoub et al. 2020). The growing skills gap and scarcity of digital talent means there is increasing concern among key stakeholders that

this will delay the deployment of IoMT solutions and constrain market growth (Taylor et al. 2018). It is a domain that is predominately approached after college or training and because of interest or pressure from an organisation. There is also the inability for SMEs in building digital capability and experience due to the lack of talent in the security and privacy development domain and problems in recruiting qualified personnel (Barlette and Fomin 2008). In addition, developers and designers have difficulty understanding the security and privacy regulatory requirements (Parker et al. 2017). This means that compliance with the GDPR can be problematic for SMEs (Jasmontaitè-Zaniewicz et al. 2021). Commonly, SMEs seek the support of security and privacy experts, many of whom often struggle with a lack of experience in operational technology (Wagner et al. 2020). This in turn impacts their ability to comply with regulations due to budget constraints (Ponemon Institute 2018). SMEs have limited time, effort, and money, in comparison to large enterprises (Barlette and Fomin 2008).

The ENISA research (ENISA 2021), outlined that the lack of suitable guidelines aimed at the SME sector creates a significant challenge, given that the current regulatory process entails many overlapping analyses (Roth 2014). Managing the raft of regulatory change that occurs in the changing landscape of the IoMT, is imperative for both developing connected medical devices and the success of the IoMT. Standards are high level and do not provide a systematic approach for developers. Barlette and Fomin (2008), found in their research that standards provide limited advice on how cybersecurity processes can be implemented in practice and aligned with system and business objectives. They determine that there is no standard capable of improving the cybersecurity of SMEs and suggest the creation of a framework specifically designed for SMEs (Wagner et al. 2020).

Additionally, complexity and compatibility issues in terms of the variety of IoMT technologies in use (Alsubaei et al., 2019) can cause difficulties. As outlined in section 2.1.2, data in flow in the IoMT can be through various apps, systems, devices, technologies, public and open networks, which are inherently insecure such as wireless sensor networks and the cloud, has led to many security issues (Ponemon Institute 2018). The interconnectivity complexities of the data in flow in the IoMT and their impact on data security and privacy is also a challenge in this domain. *“However, integration of different technologies induces vulnerability issues that can be typically found in mobile telecommunications, sensor networks, and Internet-based communications”* (Srivastava et al. 2020, p.2).

For SMEs noncompliance can have important repercussions in terms of fines or loss of trust (Jasmontaité-Zaniewicz et al. 2021, p.13). Due to the transmission of patient data in the IoMT, it is important that organisations can demonstrate clearly to patients, the public and health care professionals how their data is being used to reduce the risk of undermining the benefits that access to the data can bring (Mann et al. 2016). An expected constraint for SMEs in delivering a DPIA is limited resources. SMEs development teams tend to be smaller, which narrows knowledge and experience in development practices (Sion, Yskout, et al. 2018). The authors also note the adoption and integration of third-party solutions, such as platforms, libraries, middleware, and services as already known constrictions to a project. SMEs largely rely on third party platforms, libraries, middleware, and services to develop and support their products. Establishing the already known security and privacy constraints at the beginning of the project could control duplicated or unnecessary effort and the potential for an explosion in the number of threats. Furthermore, it could also decrease the possibility that threats are overlooked meaning the security or privacy threats are not actually mitigated as highlighted by both Berger et al. (2016) and Sion et al.(2018).

2.4 General Data Protection Regulation (GDPR)

The findings of this section are used to address research objectives 1 and 3.

RO. 1: Investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs when implementing the requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

Data protection is upheld by different legal instruments, depending on the jurisdiction (De Francesco 2019). The General Data Protection Regulation (GDPR) (2016), is a European regulation that applies to all public and private sectors who process personal data. It also applies to organisations outside the EU that offer goods or services to individuals in the EU. The GDPR applies to ‘controllers’ and ‘processors’ of personal data and introduced constraints on both. A controller determines the purposes and means of processing personal data. The GDPR obligates a controller to ensure their contracts with processors comply with the GDPR. A processor is responsible for processing personal data on behalf of a controller. If you are a processor, you are legally obliged to

maintain records of personal data and processing activities and will have legal liability if you are responsible for a breach.

In 2003-2006 the EuroSOCAP Project introduced the concept ‘spheres’ of protection of healthcare data that represents the different aspects that must be considered in this sector (McClelland 2010). When protecting healthcare data each of these spheres are significant and intertwined. These are presented in Figure 2.3 below.

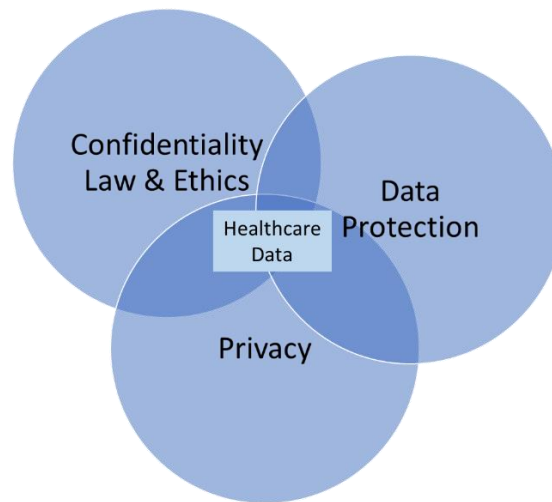


Figure 2.3 ‘Spheres’ of protection of healthcare data

The GDPR incorporates these concept spheres under the data protection principles of the regulation. Research done by Elshekeil and Laoyookhong (2017) completed a comparison of ten data protection and privacy principles. They found that there was no consensus on data protection or privacy principles or goals. However, two of their comparisons relate to this research. They compared the seven data protection principles of the GDPR, outlined below, and the eleven privacy principles of the international standard ISO/IEC 29100:2011+A1:2018 (ISO/IEC 2018b), discussed in section 2.5.3.

The data protection directives of the GDPR regulation are provided in Article 25. Article 25 relates to establishing all necessary measures to protect personal data (De Francesco 2019). This is one of the most critical pieces mandated by the GDPR. The regulation requires *data protection by design and by default* (EU General Data Protection Regulation (GDPR) 2016, p.23 Art. 25). This requires that data protection (privacy and security), are built into the core of technical products and implemented into the design of any system processing personal data (Galvez and Gurses 2018).

Article 25 asserts that the controller shall:

“...both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects...measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (EU General Data Protection Regulation (GDPR) 2016, p.23).”

The measures to protect personal data, are to apply the fundamental principles of data protection. Compliance with these fundamental principles is a key step for controllers in ensuring that they fulfil their obligations under the GDPR (Data Protection Commission Ireland 2019b). There are seven fundamental principles, and these are established in the two parts of Article 5 of the GDPR. The first part, Article 5(1), outlines six principles in relation to the processing of personal data:

- *“Lawfulness, fairness, and transparency;*
- *Purpose limitation;*
- *Data minimisation;*
- *Accuracy;*
- *Storage limitation; and*
- *Integrity and confidentiality (security);”* (EU General Data Protection Regulation (GDPR) 2016, p.6).

The second part, Article 5(2) Accountability; defines it is the controller’s responsibility for complying with the GDPR principles. The controller must demonstrate that there are appropriate processes and records in place to demonstrate that there is compliance with the data protection principles. *“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”* (EU General Data Protection Regulation (GDPR) 2016, p.7). The GDPR intends that these principles are the basis of any organisation’s approach to processing personal data (Information Commissioner’s Office 2018).

This GDPR requirement of *“data protection by design and by default”* means that security and privacy are employed from the beginning of system development (Galvez and Gurses 2018). Consequently, the data protection principles of the GDPR incorporates PbD and Security by Design (SbD), for any system or service that involves processing

personal data (Sion, Yskout, et al. 2018). SbD and PbD requires developers to employ security and privacy from the beginning of system development (EU General Data Protection Regulation (GDPR) 2016; Galvez and Gurses 2018). The regulation has provided a way in which an organisation can show that both SbD and PbD have been implemented in the development of their system or product, by generating a DPIA. Using a DPIA can provide evidence for an organisation that the development project has implemented appropriate technical measures to ensure a level of security and privacy appropriate to the risk (EU General Data Protection Regulation (GDPR) 2016; Data Protection Commission Ireland 2018; ICO 2020). The next section will define a DPIA and what it should contain. One of the suggested advantages of showing compliance with the GDPR was that it *“can act as a competitive advantage, fostering consumer trust and providing new business opportunities”* (Jasmontaitè-Zaniewicz et al. 2021, p.17). However, SMEs struggle with realising such competitive advantages due to lack of understanding and expertise. This is because demonstrating compliance requires a sound understanding of personal data protection principles and other legal concepts of the GDPR (Jasmontaitè-Zaniewicz et al. 2021).

2.4.1 Data Protection Impact Assessment (DPIA)

A data protection impact assessment (DPIA) is an effective way to assess and demonstrate a project’s compliance with the GDPR data protection principles and obligations (ICO 2020). The European Commissioner’s Article 29 Data Protection Working Party guidance describes a DPIA as *“a process for building and demonstrating compliance”* (2017, p.4). This guidance defines a DPIA as a procedure designed to describe the processing and assess the necessity and proportionality of the processing. It is to help manage the risks to the rights and freedoms of natural persons resulting from the processing of their personal data, by assessing them and determining the measures to address them (Article 29 Data Protection Working Party 2017). The Irish Data Protection Commission guide to DPIAs states: *“The primary aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project”* (2019a, p.22). The instrument for a privacy impact assessment (PIA) or DPIA was introduced with Article 35 of the GDPR. This refers to the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing (Data Protection Commission Ireland 2019a).

Article 35 (1), of the GDPR states, a DPIA is required in cases:

“...where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.” (2016 Art. 35(1))

The minimum features of a DPIA are set out in Article 35(7) of the GDPR and are:

“The assessment shall contain at least:

- (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller*
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes*
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 and*
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.”* (2016 Art. 35(7)(a)-(d))

In addition to the GDPR, there are a number of international guidance documents and standards that address the creation and the elements of a DPIA. Two international standards that address the elements and creation of a DPIA are:

- ISO/IEC 29134:2017 Information technology - Security techniques - Guidelines for privacy impact assessment (ISO/IEC 2017c);
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 2019).

ISO/IEC 29134:2017 provides detailed guidance for conducting a PIA and advises on the structure and content of a PIA report. However, in the privacy risk analysis phase of this standard, it only describes the fundamental considerations for the impact analysis, which does not provide sufficient information for the risk assessor (Wei et al. 2020). This standard incorporates guidelines for structure: Objective, Input, Expected Output, Actions, and Implementation Guidance. These sections align with recital 90 of the GDPR that outlines elements that overlap with elements of risk management, required for a

DPIA (Article 29 Data Protection Working Party 2017). The risk management elements in recital 90 is to use processes by:

- Establishing the context: considering the nature, scope, context and purposes of the processing and the sources of the risk
- Assessing the risks: assess the particular likelihood and severity of the risk
- Treating the risks: *“mitigating that risk and ensuring the protection of personal data, and demonstrating compliance with this Regulation”* (EU General Data Protection Regulation (GDPR) 2016 Recital 90)

The ISO/IEC 27701:2019 standard establishes *“a management system that aims to manage the processes for protecting the capture, accountability, availability, integrity, and confidentiality of personal data”* (Lachaud 2020, p.194). The standard states that the organisation *“should determine the elements necessary for the completion of a privacy impact assessment”* (ISO/IEC 2019, p.31). The standard provides limited guidance on the elements the organisation should include. However, it does directly reference ISO/IEC 29134:2017 for guidance on PIAs related to the processing of PII.

The Data Protection Commission of Ireland recommends that a DPIA should bring together, in summary form:

- The record keeping from each stage of the DPIA process.
- Note the conclusions from each step of the process.
- It should also include an overview of the project, explaining why it was undertaken and how it will impact on data protection.
- It should describe the process adopted in conducting the DPIA.
- It should set out the data protection risks and solutions which were identified as part of the process.
- A DPIA does not necessarily require a formal signing-off process, but your organisation may require it, particularly if it recommends significant changes to the nature of a project, or if it recommends accepting significant risks. (Data Protection Commission Ireland 2020)

The British Information Commissioner’s Office (ICO), stress throughout their guide, to keep a record of all steps taken as part of the DPIA (ICO 2020). The guidance asserts doing this will help support that the process is completed thoroughly. In addition, keeping a record will help to reassure stakeholders that all data protection risks have been considered (ICO 2020). This written record should also form the basis of putting into

effect the data protection solutions which have been identified and can be used to check off the implementation of each solution.

The European Union Agency for Network and Information Security (ENISA) encourage policy makers and regulators to promote the use of DPIAs as a means for TM and building data protection by design and by default (ENISA 2017). ENSIA go as far to state that DPIAs “*can be essential to app developers to assess the risks of their tools and embed privacy and data protection requirements by design and by default*” (ENISA 2017). However, the formal aspects of the regulation, such as DPIA requirements, can constitute an additional burden for SMEs, due to high levels of bureaucracy associated with these obligations (Jasmontaitè-Zaniewicz et al. 2021). There is no requirement to produce a final DPIA report but the Data Protection Commission of Ireland recommend it as good practice to do so (Data Protection Commission Ireland 2020).

2.5 Standards for Data Security and Privacy

The findings of this section are used to address research sub-question 2 and research objectives 2 and 3.

RSQ. 2: What are the methods and/or standards for security and privacy risk assessment for software development?

RO. 2: Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

This section provides a review of risk assessment standards from the medical, security and privacy domains that are used in software development.

The standards investigated and their domains in this section are presented in Table 2.3.

Table 2.3 Standards and domains investigated

Standard	Domain
AAMI TIR57:2016 Principles for medical device security - Risk Management	Medical Device Security Risk Management
ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management	Risk Management
ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework (ISO/IEC 2018b)	Privacy
ISO/IEC 27701:2019 Privacy Information Management System (PIMS)	Privacy
ISO/IEC 27033 Information technology - Security techniques - Network security <ul style="list-style-type: none"> • ISO/IEC 27033-1:2015 Part 1: Overview and concepts • ISO/IEC 27033-2:2012 Part 2: Guidelines for the design and implementation of network security • ISO/IEC 27033-3:2010 Part 3: Reference networking scenarios -- Threats, design techniques and control issues • ISO/IEC 27033-4:2014 Part 4: Securing communications between networks using security gateways • ISO/IEC 27033-5:2013 Part 5: Securing communications across networks using Virtual Private Networks (VPNs) • ISO/IEC 27033-6:2016 Part 6: Securing wireless IP network access 	Network Security for all types of organisations
ITU-T X.805 Security architecture for systems providing end-to-end communications (ITU-T 2003)	Network Security
ISO/IEC 27034-1:2011 Information technology - Security techniques - Application security <ul style="list-style-type: none"> • ISO/IEC 27034-1:2011 Overview and concepts • ISO/IEC 27034-2:2015 Organization Normative • ISO/IEC 27034-3:2018 Application security management process • ISO/IEC 27034-4 (Deleted) Application security validation • ISO/IEC 27034-5:2017 Protocols and application security control data structure • ISO/IEC 27034-6:2016 Case studies • ISO/IEC 27034-7:2018 Assurance prediction framework 	Application Development

There are different frameworks for assessing security and privacy risks within an organisation. The most popular are the ones from NIST and ISO. However, these risk assessment methodologies may have limitations when using them to analyse compliance with GDPR privacy requirements (Duricu 2019). The limitations can include not being able to identify some aspects or risks that personal data is subject to and what and how the rights and freedoms of the individuals are being affected (Duricu 2019). Unlike regulations which are typically restricted to specific geographic regions, standards are internationally recognised and as such transcend borders.

The findings of this section and section 2.6 are used to address research objects 2 and 3.

RO. 2: Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

2.5.1 AAMI TIR57:2016 Principles for Medical Device Security - Risk Management

AAMI/TIR57 (AAMI 2016), is the only document available in the medical device-related standards and guidance, dealing with the application of cybersecurity principles. It was created to address risk assessment and development lifecycle processes for the management of cybersecurity in medical devices (AAMI 2016). AAMI TIR57 builds off the principles presented in the ISO 14971 Medical Devices—Application of Risk Management to Medical Devices (ISO 2012). ISO 14971 is a required standard already implemented by medical device manufacturers. AAMI TIR57 directs cyber risk management by applying the principles presented in ISO 14971 to security threats that could impact data security of a medical device or information processed by the device.

Figure 2.4 overleaf, presents the AAMI TIR57 security risk and ISO 14971 safety risk management processes. The security risk process provided by AAMI TIR57 mirrors the ISO 14971 safety risk management processes. Figure 2.4 is adapted from the AAMI TIR 57 standard Figure 1 (2016, p.ix) and Figure 3 (2016, p.6). AAMI TIR 57 recommends that medical device manufacturers establish a “*companion security risk management process to their existing ISO 14971 based safety risk management process*” (2016, p.6). The standard’s recommendation is that security and safety staff should work jointly to ensure that any security risks do not impact safety and vice versa that a safety related hazards do not impact security risks, with the application of controls that mitigate safety or security risks. The object for the paralleled risk management processes is to manage all risks in collaborative engagement.

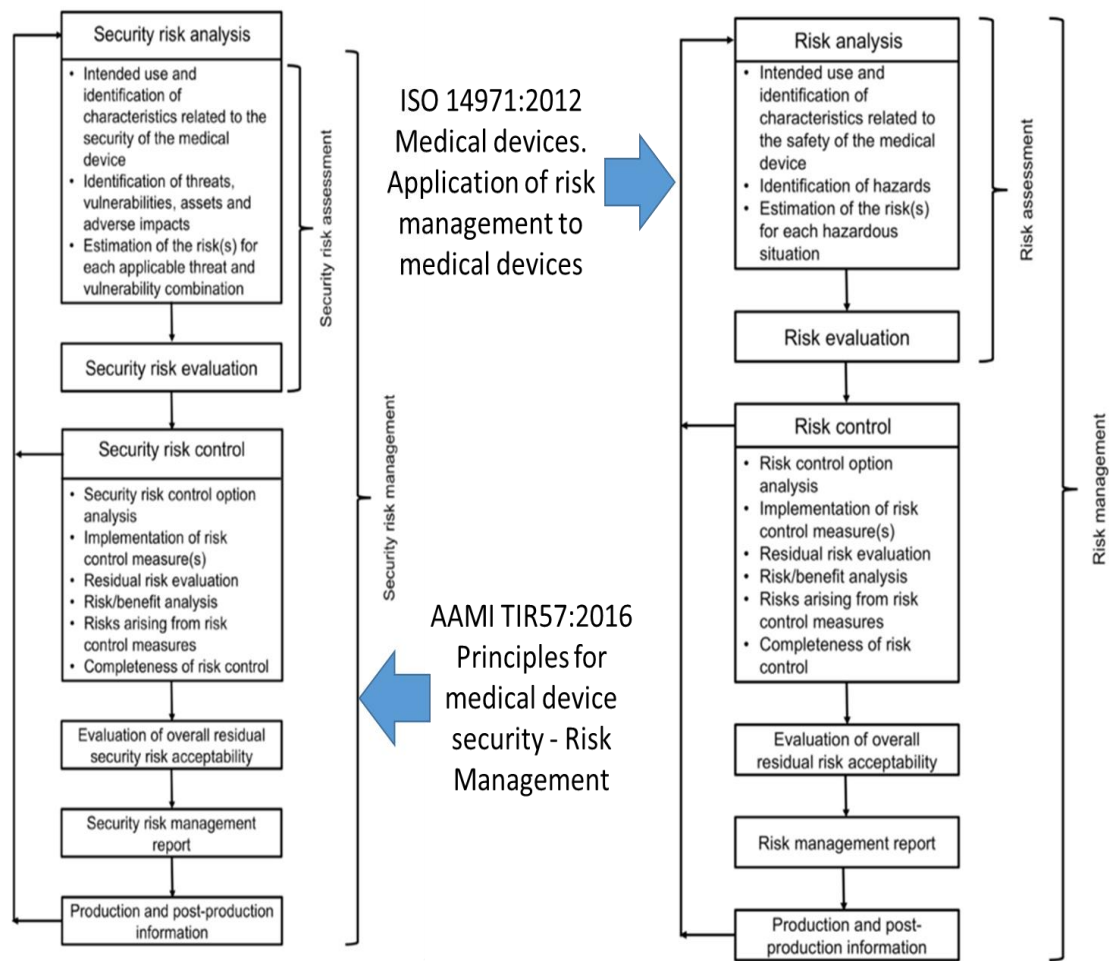


Figure 2.4 Representation comparison of the security risk and safety risk management processes

AAMI TIR57 includes steps on how to identify and evaluate threats and vulnerabilities, control security risks, and monitor the effectiveness of the controls (Yuan et al. 2018). The standard provides guidance to help developers to proactively detect and prevent potential threats before the device goes to market (Yuan et al. 2018). The FDA added TIR57 to its list of accepted standards within a month of its release, which indicated the need for protection of medical devices in an increasingly connected world (Yuan et al. 2018). The research framework adopts all phases of AAMI TIR57 and expands the scope to include both security and privacy. It focuses the risk assessment on the identification, analysis, and evaluation of all potential security and privacy aspects. Annex B of AMMI TIR57 suggests the use of TM as a means to analyse a systems architecture to identify assets requiring protection. Implementing TM for risk analysis allows the SMEs and developers in the IoMT domain, apply appropriate strategic

decisions on security and privacy risks that require mitigating controls for data in flow (Treacy et al. 2020)

2.5.2 ISO/IEC 27005:2018 Information technology - Security Techniques - Information Security Risk Management

The ISO/IEC 27005:2018 (ISO/IEC 2018a) standard provides guidelines to identify organisational needs regarding information security requirements and to create an effective information security management system. This standard supports the general concepts specified in ISO/IEC 27001:2013 Information technology - Security techniques management systems - Requirements (ISO/IEC 2013a). It is designed *to assist the implementation of information security based on a risk management approach* (Tofan 2010, p.130). ISO/IEC 27005 is applicable to all organisations, regardless of size or sector. ISO 27005 does not specify any specific risk management methodology, but it does include a process based on six key clauses:

1. Context establishment;
2. Risk assessment;
3. Risk treatment;
4. Risk acceptance;
5. Risk communication and consultation;
6. Risk monitoring and review (ISO/IEC 2018a).

The standard outlines each of the clauses into a repeatable structure of the following:

1. Input: the information necessary to perform an action;
2. Action: the activity itself;
3. Implementation guidance: any additional detail;
4. Output: the information that should have been generated by the activity (ISO/IEC 2018a).

The aim of the approach is to ensure that organisations have all the information required before beginning any risk management activity. The standard is flexible and recommends an organisation selects their own approach to risk assessment based on their specific business objectives.

This standard is closely aligned with the ISO/IEC 27034 set of standards for application security, discussed in section 2.5.7. It is particularly aligned with Part 3, which describes the Application Security Management Process (ASMP) for the organisation. The ASMP is performed in five steps all of which correspond to steps in

the risk management process established by ISO/IEC 27005 risk management process (ISO/IEC 2018a). However, this standard is particular to organisational level adaption intended to manage risks that could compromise the organisation's information security. ISO/IEC 27005 refers to risk characterised in terms of organisational conditions. Additionally, the standard does not specify, recommend or name any specific risk analysis method (Ghazouani et al. 2014). This does not provide the degree of guidance required for this research. This standard is also not largely meant for technical risk assessment such as the NIST SP 800-30 standard.

2.5.3 ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework

The international standard, ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework (2018b), provides a high-level framework for the protection of PII within ICT systems. The standard defines the organisational, technical, and procedural aspects associated with safeguarding the privacy of PII. ISO/IEC 29100 specifies common privacy terminology, defines actors and their roles in processing PII, describes privacy safeguarding requirements and references known as privacy principles (Cho et al. 2016). The standard is provided as a basis for additional privacy standardisation initiatives for such matters as: a technical reference architecture; the implementation and use of specific privacy technologies and overall privacy management; privacy controls for outsourced data processes; privacy risk assessments; or specific engineering specifications (ISO/IEC 2018b).

This research studied ISO/IEC 29100 for common privacy terminology along with the GDPR terminology. The research considered the eleven privacy principles for data protection presented in this standard, which are:

- Purpose Legitimacy and Specification;
- Collection Limitation;
- Accountability;
- Data Minimization;
- Accuracy and Quality;
- Consent and Choice;
- User, Retention and Disclosure Limitation;
- Openness, Transparency and Notice;
- Individual Participation and Access;
- Information Security;
- Privacy Compliance;

The emphasis being to assist developers recognise and understand the privacy requirements in relation to PII. The research employed the standard's substance around the eleven privacy principles, to provide a set of questions for SMEs and developers inexperienced in this domain to address privacy requirements. The questions are directly related to the individual GDPR data protection principles.

2.5.4 ISO/IEC 27701:2019 Privacy Information Management System (PIMS) Standard

ISO/IEC 27701 (ISO/IEC 2019) specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation (ISO/IEC 2019). The standard is intended to address the need for companies to meet their privacy regulatory obligations and the need for a clear and shared regulatory framework. This standard specifies related requirements for a PIMS and provides guidance for PII controllers and processors responsible for PII processing and their accountability. ISO/IEC 27701 is applicable to all types and sizes of organisations, which are PII controllers and/or PII processors processing PII within an Information Security Management System (ISMS). An ISMS is a set of policies and procedures for managing the sensitive data of an organisation (ISO/IEC 2019). It pertains to public and private companies, government entities and not-for-profit organisations.

The research supports an organisation using the ISO/IEC 27701 standard for developing a classification scheme for PII. The research also employed the standard's recommendations for the elements to include in a PIA. These recommendations are incorporated into the DPIA template developed for the research and for documentation of the processes.

2.5.5 ISO/IEC 27033-3:2010 Information technology - Security Techniques - Network Security Part 3: Reference networking scenarios - Threats, Design Techniques and Control Issues

ISO/IEC 27033-3 (ISO/IEC 2010), is number three in a set of six ISO/IEC 27033 standards for network security. ISO/IEC 27033-3 describes the threats, design techniques and control issues associated with referenced network scenarios (ISO/IEC 2010). For each scenario, the standard provides detailed guidance on the security threats, the security

design techniques and controls required to mitigate the associated risks. The standard references other parts of the set, ISO/IEC 27033-4 to ISO/IEC 27033-6, to prevent duplicating the content of these parts.

The information in ISO/IEC 27033-3:2010 is used in the research framework for the expansion of the traditional CIA triad security properties. The research adopted the security properties in ISO/IEC 27033-3 as these were developed for end-to-end security for networks. The objective of this research is end-to-end security for data in flow in the IoMT and the adoption of the properties were incorporated into the research to assist this objective. The properties are used throughout the research.

2.5.6 ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications

ITU-T X.805 (ITU-T 2003), is a security architecture framework for providing end-to-end network security. This framework was heavily influenced by the set of network security standards ISO/IEC 27033. The architecture outlined by ITU-T X.805, *logically divides a complex set of end-to-end network security-related features into separate architectural components* (ITU-T 2003, p.2). The separate architectural components in ITU-T X.805 are security dimensions, security layers and security planes. ITU-T X.805 defines a security dimension as, *a set of security measures designed to address a particular aspect of the network security* (ITU-T 2003, p.3). ITU-T X.805 identifies eight security dimensions to protect against all major security threats. It maintains the dimensions are not limited to the network, but extend to apps, end user information and apply to service providers or enterprises offering security services to their customers. The security dimensions are referenced in ISO/IEC 27033-3 as security properties.

ITU-T X.805 provides a dimension privacy, which is excluded in ISO/IEC 27033-3 security properties. The growing importance of privacy, due to regulatory requirements, requires the inclusion of privacy in properties for systems processing PII.

2.5.7 ISO/IEC 27034:2011+ - Information technology - Security techniques - Application Security

The ISO/IEC 27034 set of standards are internationally recognised for guidance on InfoSec to those specifying, designing and programming or procuring, implementing and using application systems (ISO/IEC 2014b). The set of standards provides components, processes and frameworks to help organisations acquire, implement and use trustworthy

applications, at an acceptable security cost (ISO/IEC 2014b). This standard is closely aligned with ISO 27005 (ISO/IEC 2018a) for information security risk management. ISO/IEC 27034 contains seven parts under the general title Information Technology - Security Techniques - Application Security and three parts are in different versions of draft, as listed in Table 2.4. The researcher investigated the different parts of this standard to determine if they were relevant to the research.

Table 2.4 Seven parts of ISO/IEC 27034

ISO/IEC 27034 - Parts of Standard
ISO/IEC 27034-1:2011 Information technology - Security techniques - Application security Overview and concepts
ISO/IEC 27034-2:2015 Organization Normative Framework
ISO/IEC 27034-3:2018 Application Security Management Process
ISO/IEC 27034-4 (Deleted) Application Security Validation
ISO/IEC 27034-5:2017 Protocols and Application Security Control Data Structure
ISO/IEC 27034-6:2016 Case Studies
ISO/IEC 27034-7:2018 Assurance Prediction Framework

The standard introduces the concepts of an Organisation Normative Framework (ONF) and application security controls (ASC). An ONF, as defined in Part 2 of the standard, is a suite of app security-related policies, procedures, roles and tools (ISO/IEC 2015c). An ASC, as defined in Part 1, is a *“data structure containing a precise enumeration and description of a security activity and its associated verification measurement to be performed at a specific point in an application's life cycle”* (ISO/IEC 2014b, p.2).

The standard promotes the development of a security controls library for reference when implementing the ONF to support the organisations ISMS. It states its purpose is to provide general guidance that will be supported, in turn, by more detailed methods and standards. It does not offer or recommend a set of security controls for app development. It directs the user to widely accepted libraries to develop a security controls library for the organisation.

Chapter 2 Literature Review

The standards referenced for the proposed ASCs library include:

- ISO/IEC 27002, Code of practice for information security management;
- NIST SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations;
- ISO/IEC 21827, Systems Security Engineering - Capability Maturity Model® (SSE-CMM®);
- ISO/IEC 15408-3, Evaluation criteria for IT security - Part 3: Security assurance components;
- ISO/IEC 15026-2, Systems, and software engineering - Systems and software assurance - Part 2: Assurance case;
- ISO/IEC 15288, Systems, and software engineering - System life cycle processes; and
- ISO/IEC 12207, Systems, and software engineering - Software life cycle processes.

Three of these standards are mapped in ISO/IEC 80001-2-8 for the security controls development, ISO/IEC 27002, ISO/IEC 15408-3 and NIST SP 800-53r4. Annex B of Part 1 provides an example case study demonstrating mapping ASC with security controls from NIST SP 800-53 Rev.3. The case study illustrates how security controls from NIST SP 800-53 Rev. 3 and their classification (classes, families and identifiers) can be integrated as ASCs for use in accordance with ISO/IEC 27034 (ISO/IEC 2014b). This mapping is out of date as NIST SP 800-53 is now in revision five.

A report by ENISA, *Cybersecurity Challenges and Recommendations for SMEs. Challenges and Recommendations* (ENISA 2021), presents an analyse on the ability of SMEs within the EU to cope with the cybersecurity challenges. The report and its recommendations were developed based on a two-month-long survey with 249 European SMEs and targeted interviews with selected participants followed. The report found that there is a lack of availability of guidelines in the form of standards, whitepapers or guidelines suitable for SMEs. As a result SMEs would require a specialised dedicated staff member to implement current standards and guidelines (ENISA 2021). The report notes this could be a challenge for a SME health development organisations, and simple to follow standards and guidelines specifically for SMEs should be developed (ENISA 2021). The most broadly applicable and useful part of this standard, is Part 3, which was published in May 2018. This part describes the Application Security Management

Process (ASMP) for the organisation. The ASMP is performed in five steps all of which correspond to steps in the risk management process established by ISO/IEC 27005 (ISO/IEC 2018a) risk management process. This could be beneficial for an organisation that has no risk management experience as it focuses explicitly on app security risk management.

Examination of these standards provided limited benefit for the research. The complicated structure of the standard and lack of fixed ASCs did not lend itself to additional use for the research. The investigation focused back to the standards ISO/IEC 27002, NIST SP-800-53r4, ISO/IEC 15408-2 and ISO/IEC 15408-3, mapped in IEC/TR 80001-2-8, for security and privacy controls.

2.5.8 Summary

This section provides an examination of risk assessment standards from the medical, security and privacy domains used in software development. The examination of the standards provided a risk management process to build the framework around AAMI/TIR 57. AAMI/TIR 57 is the only medical device related standards dealing with the application of cybersecurity principles. The research framework adopted this standard as it supports assessment with the medical devices risk management standard ISO 14971 and TM. The ISO/IEC 27005 risk management process was presented as particular to organisational level adaption for information security. The standard does not specify, recommend or name any specific risk analysis method and is not largely meant for technical risk assessment such. As such it was considered not to provide the degree of guidance required for this research. The standard ISO/IEC 29100 was outlined as it provides a framework for PII in ICT systems. The research used the standard's eleven privacy principles to develop a set of questions to help developers understand and comply with GDPR data protection principles. The questions are directly related to the individual GDPR data protection principles. ISO/IEC 27701 standard specifies related requirements for a PIMS and provides guidance for PII controllers and processors responsible for PII processing and their accountability. The research incorporated the recommendations for the elements to include in a PIA into the DPIA. The research used the properties from ISO/IEC 27033-3 to expand the traditional CIA triad security properties for the framework properties. The properties adopted were developed for end-to-end security for networks and the objective of this research is end-to-end security for data in flow in the IoMT. The ITU-T X.805 standard included the privacy property as an inclusion of

privacy in the framework. Examination of the ISO/IEC 27034 set of standards did not present any application for the development of the risk management process for the framework.

2.6 Introduction

This section of the literature review will discuss Threat modeling (TM), an important process in the field of cybersecurity and privacy in software development. It involves identifying and evaluating potential threats to a system or application in order to develop effective security and privacy measures. Sections 2.7.1 and 2.7.2 will provide an overview of two widely used threat models, STRIDE and LINDDUN, respectively. Section 2.7.3 discusses NIST SP 800-30 Revision 1, a standard used for risk assessment in information security.

2.7 Threat Modeling for Software Development

The findings of this section are used to address and research objectives 2 and 3.

RO. 2: Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

Threat modeling has long been acknowledged as one of the most important activities in software security (McGraw 2006; Howard and Lipner 2006). The term TM was created by Microsoft to describe “*an attack-focused analysis activity used to find software security flaws*” (Dhillon 2011, p.42). The TM process is the use of abstractions to aid in thinking about risks (Shostack 2014b), where there is a systematic examination of a system’s architecture or design to find security flaws and reduce risk (Dhillon 2011). In brief, TM is about identifying potential threats to the system being modeled and by understanding the threats it is possible to determine its vulnerabilities.

A DPIA is recommended at the planning stage of a project to capture knowledge on data protection requirements or existing measures. This is underlined through research by Berger et al. (2016) and Sion et al. (2018). Berger et al. (2016) maintain that TM DFDs do not support being able to explicitly model already known security measures or requirements. The authors claim not documenting the already known security measures or requirements in TM DFDs, excludes reasoning about it during the TM process. This

leads to duplicated or unnecessary effort, or worse, threats that are overlooked. This is supported in reasons by Sion et al. (2018), that a key problem related to using DFDs as the main input for security TM is that the already known security constraints are not communicated in a structured way. Sion, Yskout, et al. (2018), maintain their research to structure known security constraints into the TM process has shown positive improvements to limit and scope the threat elicitation space by leveraging knowledge about existing security solutions in the system under design.

2.7.1 STRIDE

STRIDE is an acronym for the security threat categories; **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege (Swiderski and Synder 2004). The STRIDE model threat categories with their definition and the security properties they violate are shown in Table 2.5.

Table 2.5 STRIDE security threat categories, property violated, definition (Swiderski and Synder 2004; Shostack 2014b)

Security Property Violated	Security Threat	Definition
Authentication	Spoofing	Allows an adversary to pose as another user, component, or other system that has an identity in the system being modeled (Swiderski and Synder 2004) Pretending to be something or someone other than yourself (Shostack 2014b)
Integrity	Tampering	The modification of data within the system to achieve a malicious goal (Swiderski and Synder 2004) Modifying something on disk, on a network, or in memory (Shostack 2014b)
Non-repudiation	Repudiation	The ability of an adversary to deny performing some malicious activity because the system does not have sufficient evidence to prove otherwise (Swiderski and Synder 2004) Claiming that you didn't do something or were not responsible. Repudiation can be honest or false, and the key question for system designers is, what evidence do you have? (Shostack 2014b)
Confidentiality	Information disclosure	The exposure of protected data to a user that is not otherwise allowed access to that data (Swiderski and Synder 2004) The exposure of protected data to a user that is not otherwise allowed access to that data (Shostack 2014b)
Availability	Denial of Service	Occurs when an adversary can prevent legitimate users from using the normal functionality of the system (Swiderski and Synder 2004) Absorbing resources needed to provide service (Shostack 2014b)
Authorisation	Elevation of Privilege	Occurs when an adversary uses legitimate means to assume a trust level with different privileges than he currently has (Swiderski and Synder 2004) Allowing someone to do something they're not authorised to do (Shostack 2014b)

STRIDE uncovers security design flaws using the STRIDE threat categorisation approach (Hernan et al. 2006). STRIDE focuses on identification of potential threats in each element of the system and their interactions (Shostack 2014b). The STRIDE model deals with six basic concepts of security (Falah et al. 2015). The six security properties violated by the STRIDE threats are; Authentication, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization (Shostack 2014). As outlined previously, the research recognised the limitations to protecting data in flow in IoMT using the CIA triad. In addition, there are limitations using the STRIDE threat categorisation in identifying threats. Marback et al. (2009) asserted that only a subset of all possible threats that a system could possibly be vulnerable to are covered with the STRIDE threat categories. Also, after the security properties used for the framework were expanded, they did not line up exactly with the STRIDE threat categories. This required a reconfiguration of the framework properties to the STRIDE threat categories; this is further discussed in chapter 4.

STRIDE is the mostly widely used TM tool for security threats (Hussain et al. 2014). However, it is important to recognize that it does not consider privacy threats (Deng et al. 2010). A TM tool that addresses privacy threats is LINDDUN (Deng et al. 2010), which is a systemic approach to assist with the elicitation and mitigation of privacy threats in software systems. Both STRIDE and LINDDUN utilise a similar systematic TM approach.

2.7.2 LINDDUN

Deng et al. (2011) recognised that the STRIDE model does not cover privacy threats and that a systematic and effective methodology did not exist for privacy threats and so developed LINDDUN. LINDDUN is based on the TM approach of STRIDE and follows the same steps (Sion, Wuyts, et al. 2018). LINDDUN is an acronym for the privacy threat categories; **L**inkability, **I**dentifiability, **N**on-repudiation, **D**etectability, **D**isclosure of Information, **U**nawareness and **N**on-compliance (Deng et al. 2010).

The privacy property and its violating LINDDUN threat category and definition are presented in Table 2.6.

Table 2.6 Privacy property violated against LINDDUN threat category and definition (Deng et al. 2010)

Privacy Property Violated	Privacy Threat	Definition
Unlinkability	<i>Linkability</i>	Being able to sufficiently distinguish whether 2 Items of Interest (IOI) are linked or not, even without knowing the actual identity of the subject of the linkable IOI. Not being able to hide the link between two or more actions/identities/pieces of information.
Anonymity & Pseudonymity	<i>Identifiability</i>	Being able to sufficiently identify the subject within a set of subjects (i.e., the anonymity set). Not being able to hide the link between the identity and the IOI (an action or piece of information).
Plausible deniability	<i>Non-repudiation</i>	Having irrefutable evidence concerning the occurrence or non-occurrence of an event or action.
Undetectability & Unobservability	<i>Detectability</i>	An attacker can sufficiently distinguish whether an item of interest (IOI) exists or not.
Confidentiality	<i>Disclosure of Information</i>	Exposing information to someone not authorized to see it.
Content Awareness	<i>Unawareness</i>	Not understanding the consequences of sharing personal information in the past, present, or future.
Policy and Consent Compliance	<i>Non-compliance</i>	Not following the (data protection) legislation, the advertised policies, or the existing user consents

2.7.3 NIST SP 800-30 Revision 1

NIST SP 800-30 Revision 1's (NIST 2012), purpose is to provide guidance for conducting risk assessments of federal information systems and organisations. It provides guidance for completing each of the three steps in the risk assessment process: prepare for the assessment; conduct the assessment; and maintain the assessment (NIST 2012). The publication also outlines how risk assessments and other organisational risk management processes complement and inform each other. AAMI TIR57, incorporates several principles from NIST SP 800-30. This standard is referenced by AAMI TIR57 for terms and definitions and as a security risk management process, with a particular emphasis on risk assessment methods (AAMI 2016). Annex B of AAMI TIR57 apply the

process for performing security risk assessment for a medical device based on the principles described in NIST SP 800-30.

2.8 Existing Frameworks

The findings of this section are used to address and research objectives 2 and 3.

RO. 2: Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

2.8.1 Process for Attack Simulation and Threat Analysis (PASTA)

Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat modeling framework developed in 2012 by Tony UcedaVélez (UcedaVélez et al. 2015). The purpose of PASTA is to provide a dynamic threat identification, enumeration, and scoring process (UcedaVélez et al. 2015). It is a seven-stage framework that is based on TM for assessing an organisations cybersecurity position. The framework works through each of the seven stages, building on the previous stage to provide a list of priorities to fix an organisations cybersecurity vulnerabilities. It has an attacker-centric standpoint (Shevchenko et al. 2018). The seven stages are presented in Figure 2.5 below.



Figure 2.5 Seven stages of PASTA

Part of the risk-centric PASTA process is attack simulation and threat analysis, which is addressed by mapping the potential threats to a comprehensive list of current known attacks and weaknesses. Two endorsed resources for mapping the threats are the Common Attack Pattern Enumeration and Classification (CAPEC) and Common Weakness Enumeration (CWE). CAPEC is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defences. CWE is a community-developed formal list of common software weaknesses. It is a standard measuring stick for software security tools targeting these vulnerabilities, and a baseline standard for weakness identification, mitigation, and prevention efforts. PASTA does provide very rich documentation for the method however, it is a laborious and extensive process, as can be seen from a summary description of the stages in Table 2.7.

Table 2.7 PASTA stages adapted from

1. Define Objectives	<ul style="list-style-type: none"> • Identify Business Objectives • Identify Security & Compliance Requirements • Business Impact Analysis
2. Define Technical Scope	<ul style="list-style-type: none"> • Capture the boundaries of the technical environment • Capture Infrastructure Application Software Dependencies
3. Application Decomposition	<ul style="list-style-type: none"> • Identify Use Cases Define App Entry Points & Trust levels • Identify Actors Assets Services Roles Data Sources • Data Flow Diagrams (DFDs) Trust Boundaries
4. Threat Analysis	<ul style="list-style-type: none"> • Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation & Analytics
5. Vulnerability & Weakness Analysis	<ul style="list-style-type: none"> • Queries of Existing Vulnerability Reports & Issue Tracking • Threat to Existing Vulnerability Mapping Using Threat Trees • Design Flaw Analysis Using Use & Abuse Cases • Scouring (CVSS/CWSS) Enumerations (CWE/CVE)
6. Attack Modeling	<ul style="list-style-type: none"> • Attack Surface Analysis • Attack Tree Development Attack Library Mgt • Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis	<ul style="list-style-type: none"> • Qualify & Quantify Business Impact • Countermeasures Identification & Residual Risk Analysis • ID Risk Mitigation Strategies

As can be seen from Figure 2.5 on the previous page and Table 2.7, PASTA uses a colour coded system to categorise the various steps in the process. The use of color coding is to help to visually distinguish between different types of activities, such as attack tree builds, recommended by PASTA (UcedaVélez et al. 2015). The process suggests that the

use of color may be used to organise the layers of the attack tree by a criteria useful for the threat modeling team (UcedaVélez et al. 2015).

While PASTA can be effective for improving software security, there are several challenges that developers may face when implementing this process. To implement PASTA software developers require a good understanding of security concepts, threat modeling, and risk management (Wolf et al. 2020). Developers without adequate security expertise may find it challenging to apply PASTA effectively. The fact that implementing PASTA is a laborious (Shevchenko et al. 2018), can be seen as a challenge for SME software developers. PASTA has rich documentation however, integrating this type of process into an existing development process can be challenging for SME software developers. PASTA can be a time-consuming process that requires significant resources, including security experts and specialised experience (Shevchenko et al. 2018). Developers may face challenges in finding the time and resources required to conduct PASTA. There is a lack of tools available for PASTA implementation and maintenance which can increase the difficulty of following the methodology (UcedaVélez et al. 2015).

2.8.2 IEC 80001-2-2:2012 - Guidance for the Communication of Medical Device Security Needs, Risks and Controls

IEC/TR 80001-2-2 (IEC 2012) is the first published guidance report that provides information about recommended security features for medical devices. It is the only guidance available that specifically addresses security requirements for networked medical devices. This standard is specifically designed to assist Health Delivery Organisations (HDOs) in identifying and managing “new” risks associated with the increased deployment of medical devices onto medical IT networks (IEC 2012). It provides a basis for discussion and agreement for the security dialogue necessary between health delivery organisations (HDOs), medical device manufacturers (MDMs) and IT vendors to discuss risk and their respective roles and responsibilities towards the risk management (IEC 2012). It provides a classification of security capabilities, particularly suited to medical IT networks and the incorporated devices. There are 19 high-level security-related capabilities in IEC/TR 80001-2-2, for consideration when connecting medical devices to IT-networks. These are detailed in Table 2.8 overleaf. This capabilities classification is the foundation for this set of standards. The capabilities outlined in Table 2.8 are used to enhance the security of medical devices connected to healthcare IT networks. These capabilities help to mitigate potential security risks associated with the

use of interconnected medical devices in healthcare settings. The objective is collaboration of the medical device manufacturers and healthcare providers to implement these capabilities.

Table 2.8 ISO/IEC 80001-2-2 19 Security capabilities (IEC 2012)

Security Capability	Acronym
Automatic Logoff	ALOF
Audit Controls	AUDT
Authorization	AUTH
Configuration of Security Features	CNFS
Cyber Security Product Upgrades	CSUP
Health Data De-Identification	DIDT
Data Backup and Disaster Recovery	DTBK
Emergency Access	EMRG
Health Data Integrity and Authentication	IGAU
Malware Detection/Protection	MLDP
Node Authentication	NAUT
Person Authentication	PAUT
Physical Locks on Device	PLOK
Third-Party Components in Product Lifecycle Roadmaps	RDMP
System and Application Hardening	SAHD
Security Guides	SGUD
Health Data Storage Confidentiality	STCF
Transmission Confidentiality	TXCF
Transmission Integrity	TXIG

EC/TR 80001-2-2 was intended to be a communication framework between medical device manufacturers and health delivery organisations during procurement of a medical device. The 19 capabilities provide an understanding of the user needs, security controls and risks for consideration when connecting a procured medical device to an IT network. However, the security capabilities described in IEC/TR 80001-2-2 do not provide sufficient detail for the specification of requirements, they instead provide a classification and structure that can be used to organise such requirements (IEC 2012). This provides a challenge to software developers to fill the gap (Anderson 2016). Anderson and Williams (2018), concluded that effectiveness of the IEC/TR 80001-2-2 security capabilities to the technical controls in ISO/IEC 80001-2-8 in providing practical cyber security protection is minimal. Additionally, the risk analysis component of ISO 80001 is focused towards governance for an organisation, which can lead to the gaps

identified during the initial analysis (Anderson 2016). The capabilities are structured to provide references to source material that informs the capability, the fundamental security goal of the capability, and a statement of user (healthcare provider) need for the capability.

2.8.3 IEC/TR 80001-2-8:2016 Application of risk management for IT-networks Incorporating Medical Devices — Part 2-8: Application guidance — Guidance on Standards for Establishing the Security Capabilities Identified in IEC 80001-2-2

IEC/TR 80001-2-8 was developed to provide guidance for the application of the framework outlined in IEC/TR 80001-2-2 (Finnegan 2014). IEC/TR 80001-2-8 classifies security controls from six key security standards for each of the 19 capabilities from IEC/TR 80001-2-2. The report identified over 300 security controls in a set of tables evaluated for their relevance in establishing each of the 19 security capabilities (Jump and Finnegan 2017). The controls are to manage risks to confidentiality, integrity, availability and accountability of data and systems in the implementation of IEC/TR 80001-2-2. This technical report provides a complete set of security controls deemed appropriate to medical devices. Jump and Finnegan (2017), note that this should be considered an approach for a basic foundation in security. They stress that it does not replace a more technical review of the threats and assets through a good security risk management process.

Each of the 19 capabilities in the IEC/TR 80001-2-8 standard had a corresponding table presenting operational/administrative and technical security controls. The number of controls was different for each specific capability. The development of IEC/TR 80001-2-8 used six security standards to map security controls to the 19 security capabilities. The standards selected for the mapping were based on popularity of use and level of security rigour in terms of the range of security controls and associated requirements to apply a particular security control. These standards were selected based on expert opinion in the security domain (Finnegan and McCaffery 2014). Each mapped standard considered a different context to implement the capabilities from IEC/TR 80001-2-2. The standards were divided into two categories: those that provide technical controls and those that provide operational/administrative controls. Table 2.9 lists and summarises the standards used for the security controls mapped to each of the 19 capabilities.

Table 2.9 Standards used in IEC/TR 80001-2-8 mappings for the 19 security capabilities in IEC/TR 80001-2-2

Standard	Description
Technical Security Controls	
NIST SP 800-53 Rev. 4 and Rev. 5, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	This special publication provides a comprehensive set of security and privacy controls, three security control baselines and a process for selecting controls and baselines for an organisation to protect operations, assets, individuals and other organisations (Dempsey et al. 2014).
ISO/IEC 15408-2:2008, <i>Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components</i>	This standard defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will fulfil the most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. This standard also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist (ISO/IEC 2008a).
ISO/IEC 15408-3:2008 <i>Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components</i>	This part of the ISO/IEC 15408 standard defines the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST) divided into classes and families of products. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance (ISO/IEC 2008b).
IEC 62443-3-3:2013, <i>Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels</i>	This is one of a set of twelve comprehensive standards to address the entire security life cycle for Industrial Automation and Control Systems (IACS). The security controls described in the standard are specific to interconnected, safety critical systems, which many medical devices are. The standard defines system requirements based on a combination of system functional requirements and a risk assessment (IEC 2013).
Operational/Administrative Security Controls	
ISO/IEC 27002:2013, <i>Information technology -- Security techniques -- Code of practice for information security controls</i>	ISO/IEC 27002 is not a formal standard as such, but a collection of information security guidelines, a code of practice. It is intended to provide a guide for an organisation to implement, maintain, and improve its information security management (ISO/IEC 2013b). The document provides a list of potential controls and control mechanisms. It is intended to be implemented with guidance provided within ISO/IEC 27001.
ISO 27799:2008, <i>Health informatics -- Information security management in health using ISO/IEC 27002</i>	This standard addresses the unique area of security management needs in the health sector and PHI and is completely aligned with ISO/IEC 27002. The standard tailors the implementation of ISO/IEC 27002 for the health sector and PHI and how best to protect its confidentiality, integrity and availability (ISO/IEC 2008c). It is currently under revision.

The intended outcome of IEC/TR 80001-2-8 is to provide a minimum required level of security for health delivery organisations (Anderson and Williams 2018), when putting a medical device onto medical IT networks. According to the Finnegan (2014), IEC/TR 80001-2-8 considers each of the security capabilities and identifies security controls for consideration by all stakeholders during risk management activities, supplier selection, device selection etc. The research examined the controls in this standard for identification of security and privacy controls for data in flow in the IoMT. The examination found that the controls in IEC/TR 80001-2-8 impacted at a higher organisational level. The controls are embedded in the development and preservation of security on an organisational level. The controls functioned as an approach for recognition of a basic foundation in security between medical device manufacturers, vendors and healthcare delivery organisations (Finnegan and McCaffery 2014). The standard is relevant to create awareness for these groups in understanding the capabilities of the medical device that could potentially be acquired for use on their IT network. In addition, the standard does not place significant distinction or importance on privacy. There are limited controls that concentrate on the protection of privacy of data in the standard. The foremost focus of the standard is on security. The research did use this standard as a basis for the development of the technical security and privacy controls for implementation during software development. Anderson and Williams (2018), concluded that the effectiveness of the IEC/TR 80001-2-8 security controls provided minimal measure of cybersecurity. The research literature available on IEC/TR 80001-2-8 is based in the effectiveness of the controls to meet cybersecurity requirements and not in the application or implementation of the standard.

2.9 Security and Privacy Controls

The findings of this section are used to address research objectives 2 and 3.

RO. 2: Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3: Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

This section examines the standards investigated to provide the technical security and privacy controls. Technical controls in the context of this research are controls applicable

to mitigate identified threats to the system identified through a technical review of the threats and assets from a risk management process. The objective of the technical controls is to preserve the security and privacy properties at development of a product or system level. As stated in the above section, the IEC/TR 80001-2-8 standard is established for consideration of security controls at an organisational level. The research studied the standards used for the development of IEC/TR 80001-2-8, presented in Table 2.9 above, as they were already established for security controls. The objective was to determine what standards could provide technical security and privacy controls that could be implementation at development level. The standards that were considered appropriate for the technical controls are presented in Table 2.10. The investigation of these standards was triggered by the review of the international set of standards ISO/IEC 27034:2011, discussed in section 2.5 and IEC/TR 80001-2-8:2016 discussed in section 2.8.3. The operational/administrative standards applied for the development of the security controls in IEC/TR 80001-2-8:2016 were considered not suitable for the development of technical controls as they are applicable at organisational level. While it is important that the technical controls align to the high-level organisational policies and controls, the development of organisational polices and controls were out of scope for this research. The rest of this section will provide an overview of the standards from Table 2.10.

Table 2.10 Standards investigated for security and privacy controls

Standard	Description
NIST SP-800-53 Rev.5:2020 Security and Privacy Controls for Federal Information Systems and Organizations	Federal Information and Information Systems Security and Privacy Controls
ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components	IT Security
ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components	IT Security
IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	Security in Industrial Automation and Control System (IACS)

2.9.1 NIST SP-800-53 Rev.5:2020

NIST SP 800-53 (NIST 2020) is recommended in best practice by both the Open Web Application Security Project (OWASP) and the FDA for reference as sources of appropriate security controls in app security. The standard is in revision 5. Each security

Chapter 2 Literature Review

control in NIST SP 800-53 contains a baseline control and enhanced controls. The baseline controls are broken into minimum security controls impact baselines adapted from the Federal Information Processing Standards (FIPS) 200 which are Low-Impact, Moderate-Impact, High-Impact (NIST 2014a). IEC/TR 80001-2-8 mapped the baseline controls of NIST SP 800-53r4, this research considered the baseline controls plus all enhanced controls of NIST SP 800-53r5.

Control enhancements are included with many security controls and are added to increase the strength of the base control. The implementation of the control enhancements is intended only in conjunction with implementation of the base control. The baseline controls dominate in the management and organisational properties of security requirements. It was considered that the focus on management and organisational compliancy in the baseline controls of IEC/TR 80001-2-8 could cause a lack of attention on the implementation of security controls during the development process.

The NIST SP 800-53 controls are organised into 20 families presented in Table 2.11 below. These control families have various combinations of management, operational, and technical properties (NIST 2020). One of the key objectives of the research is to produce a set of technical controls for both security and privacy explicitly for developers to implement during the development process to secure data in flow in the IoMT. The intention of examining NIST SP 800-53 is to determine a set of technical controls to assist developers comply with regulatory requirements. The standard is substantial and complicated, and the objective is to close the gap in knowledge and understanding for developers. An additional intention is to fill the vacuum of specific technical controls for security and privacy to assist inexperienced developers in this domain.

Table 2.11 NIST SP 800-53r5 control identifiers and family names

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	Personally Identifiable Information Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

2.9.2 ISO/IEC 15408-2:2008

ISO/IEC 15408 (ISO/IEC 2008a), is an international standard for security evaluation and certification of IT systems. However, security evaluation with standards is not easy as there are many activities and documents for the evaluation process (Chen et al. 2015). There are some terms necessary to understand ISO/IEC 15408-2 which are presented in Table 2.12.

Table 2.12 ISO/IEC 15408 terms (ISO/IEC 2014a, pp.2–18)

Title	Description
Target of Evaluation (TOE)	- “A <i>ToE</i> is a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation (ISO/IEC 2008a, p.2). A TOE may be a monolithic product containing hardware, firmware, and software. It may contain resources such as electronic storage media (e.g., main memory) or say computing capacity (e.g., CPU time) that can be used for processing and storing information and is the subject of an evaluation.
Security Functional Requirements (SFRs)	Are a distinct set of rules levied over the TOE resources that define access to and use of these resources and therefore the information and services controlled by the TOE.
Security Function Policies (SFPs)	Are defined by the SFRs to represent the rules that the TOE must enforce. Each SFP must stipulate its scope of control, by defining the subjects, objects, resources or information, and operations to which it applies.
TOE Security Functionality (TSF)	The TSF implements the SFPs. They impose the rules defined in the SFRs and provide necessary capabilities. The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.
Internal TOE transfers	Where a TOE is an enormous, disseminated product of internal multiple separate parts where communication between these parts through an internal communication channel for example a processor bus.
Inter-TSF transfers	Where the TOE interfaces interact with trusted IT product over external communications channels. In these cases, the SFRs of the TOE have been administratively coordinated and the other trusted IT product is assumed to enforce its SFRs correctly.
Transfers outside of the TOE	Where the TOE interfaces interact with another IT product that may not be trusted. The SFRs are unknown or their implementation is not viewed as trustworthy. (ISO/IEC 2008a)

ISO/IEC 15408-2:2008 offers security functional components, which is the basis for a set of Security Functional Requirements (SFRs) that can be expressed in a Protection Profile (PP) or a Security Target (ST) used to create trusted products reflecting the needs of the market (Common Criteria for Information Technology Security Evaluation 2012). A PP is a document that defines a set of security requirements and objectives and describes the security features and functionality that the product or system should have in order to meet specific security needs (ISO/IEC 2008a). A ST is a document that

describes the security properties and functionality that an IT product or system is expected to provide, as well as the environment in which it is intended to operate (ISO/IEC 2008a). The SFRs are presented using a hierarchical structure of classes, families and components.

The requirements define the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as specified in a PP or an ST. A developer selects from the broad catalogue of generic predefined security functional components suitable for a TOE (ISO/IEC 2008a). ISO/IEC 15408-2:2008 is one of the most widely recognised security standards which address the security of a product. This part of the standard specifically addresses the functional security of a product or system, which is pertinent for the inclusion of security during design and development and therefore valuable for developers.

This standard was selected as part of the research as it specifically addresses the security of a product or system. It is also one of the standards mapped for technical security controls in IEC/TR 80001-2-8 and referenced for use for the development of security controls in the app security standards ISO/IEC 27034 and ISO/IEC 15408-3:2008.

2.9.3 ISO/IEC 15408-3:2008

ISO/IEC 15408-3 comprises a common set of security assurance requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The objective of security assurance is to provide confidence that a product or system will meet, has met, or is continuing to meet its specified security objective (Herrmann 2002). The security assurance requirements of ISO/IEC 15408-3 are concerned with the development environment, the TOE and defines the evaluation criteria for the evaluator (ISO/IEC 2008b). Thus, ISO/IEC 15408-3 is commonly used for the evaluation of the security of IT products and systems and can also be used for the evaluation of the security for procurement decisions with regard to such. Consequently, ISO/IEC 15408-3 can be used as a Risk Management/Risk Assessment tool to determine the security of an IT product or system during its design, manufacturing or marketing, or before procuring it.

ISO/IEC 15408-3 was examined as it was used for mapping the technical security controls for IEC/TR 80001-2-8 and was cited in ISO/IEC 27034, as one of the standards to look to when developing application security controls (ASCs). ISO/IEC 15408-3 target

audience include customers, developers, and evaluators of secure IT products. It is intended that this part is to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs (ISO/IEC 2008b). ISO/IEC 15408-3 is also presented in a hierarchical order and defines ten assurance classes, 42 assurance families and 93 assurance components with elements. A set of assurance elements is provided for each assurance component. An assurance element is a security requirement that cannot be further divided as it would not yield a meaningful evaluation result. It is the smallest security requirement recognised in ISO/IEC 15408 (ISO/IEC 2008b). Each assurance element belongs to one of the three sets of assurance elements which are developer action elements marked with a “D”, content and presentation of evidence elements marked with the letter “C” and evaluator elements marked with the letter “E”. As with part two the terms necessary to understand ISO/IEC 15408-3 are defined in Table 2.12 above in section 2.9.2, and further in Table 2.13 below.

Table 2.13 ISO/IEC 15408-3 terms (ISO/IEC 2008b)

Title	Description
Evaluation Assurance Levels (EALs)	Define a scale for measuring assurance for component TOEs
Composed Assurance Packages (CAPs)	Define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed
SAR	Security Assurance Requirement
PP	Protection Profile
Security Target (ST)	Security requirements contained in an implementation-dependent construct. An ST may be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.

One of the key objectives of this research is to establish standard based technical security and privacy controls most applicable for the security of data in flow in the IoMT for developers. There is no scope to apply security assurance levels to the controls for this research at this time. This means this part of the standard may not be suitable for this part of the research. Further, ISO/IEC 15408-3 provides the least number of controls to IEC/TR 80001-2-8. In IEC/TR 80001-2-8 only 23 ISO/IEC 15408-3 controls map across four of the nineteen capability tables, CSUP, MLDP, SAHD and SGUD.

2.9.4 IEC 62443-3-3:2013

IEC 62443-3-3 is one of a set of twelve comprehensive standards to address the entire security life cycle for Industrial Automation and Control Systems (IACS). The security controls described in the standard are specific to interconnected, safety critical systems, which many medical devices are. With this understanding both the FDA and IEC/TR 80001-2-8 standard has identified the IEC 62443 set of standards as primary standards to address cybersecurity in medical devices.

The IEC 62443-3-3 standard defines system requirements based on a combination of system functional requirements and a risk assessment (IEC 2013). This is done in the standard through seven Foundational Requirements (FRs), a similar concept to the families in the ISO/IEC 15408 standard. The seven FRs as defined in part 1 of the standard are:

- Identification and authentication control (IAC);
- Use control (UC);
- System integrity (SI);
- Data confidentiality (DC);
- Restricted data flow (RDF);
- Timely response to events (TRE); and
- Resource availability (RA) (IEC 2013).

This standard expands the seven FRs detailed in IEC 62443-1-1 into detailed technical System Requirements (SRs) that further extend to include a Requirement Enhancements (REs) like the components and functional elements of ISO/IEC 15408. Like NIST SP 800-53, each of the SRs have a baseline requirement.

This standard also defines the requirements for system capability Security Levels (SLs). The SLs are similar to the Evaluation Assurance Levels (EALs) in ISO/IEC 15408. This research considers only the FRs and SRs for the security and privacy technical controls.

2.10 Summary and Conclusion

This section presents a summary of the literature review and the conclusions drawn from it. Figure 2.6 overleaf, presents how the literature review sections relate to the research sub-questions and research objectives.

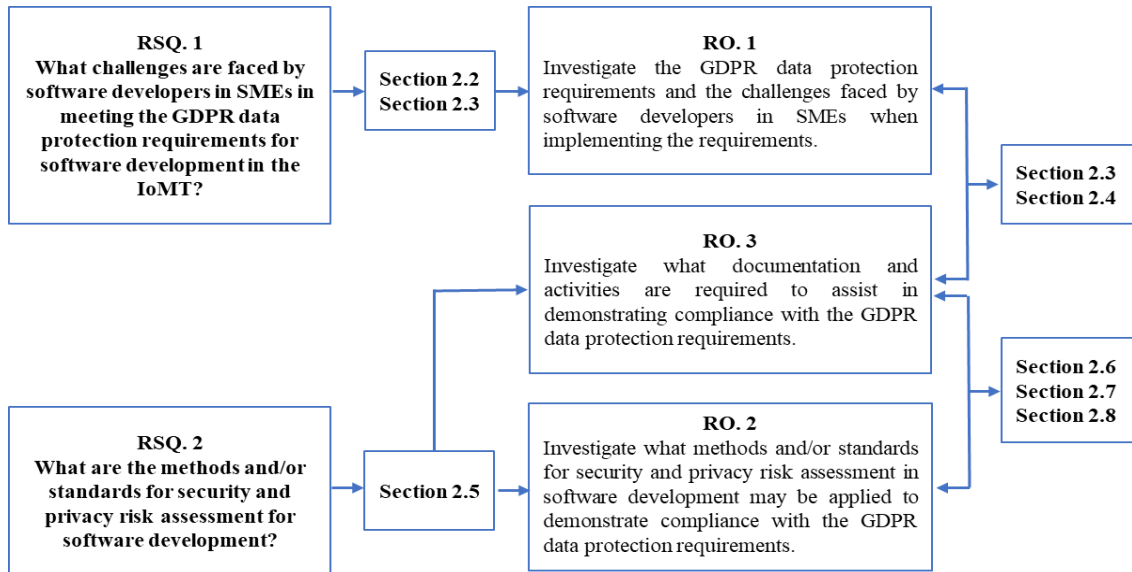


Figure 2.6 How the literature review sections correlate to the RSQs and ROs

This chapter began with an overview of the approach to complete the literature review in section 2.1. The approach taken was a traditional or narrative review approach that used backward and forward snowballing as a complementary search strategy.

The literature review began with a review of what is the IoMT in section 2.1.1, and outlined what data flow in the IoMT could potentially look like. This part of the review outlined the complexity of data in flow in the IoMT. It highlighted the intricacies to consider with the flow of data in the IoMT. Section 2.1.3, summarised the lack of adequate security and privacy in the healthcare domain. It discussed how this has a particular impact on SMEs and developers in experienced in security and privacy. The discussion developed on the need for concise and straightforward standards and guidelines in this domain.

The chapter then detailed the requirements for security and privacy of data in the IoMT. Section 2.2 stressed the many aspects that are required in relation to meeting the data protection requirements of the GDPR, SbD and PbD. The review considered the legal requirements in addition to the security and privacy requirements developers have to navigate in development to meet the GDPR data protection requirements. It revealed the lack of detailed guidance for the creation of a DPIA for developers and SMEs. A particular gap detected was around meeting the legal and risk assessment requirements.

Section 2.3 discussed the main challenges faced by software developers with employing security and privacy in their development projects. This section continued from the previous section by reviewing the industry reports and applying these findings

Chapter 2 Literature Review

to the literature. This section emphasised the lack of concise and straightforward standards and guidelines for developer inexperienced in this domain. The review also underscored the struggles SMEs encounter in meeting security and privacy requirements in their products.

Section 2.4 provided a detailed examination of the data protection requirements of the GDPR. The section examined the GDPR data protection requirements and how these requirements correlate to SbD and PbD. It also examined the factors that need to be considered to meet the requirements of a DPIA in section 2.4.1. It detailed the legal and risk assessment requirements of a DPIA. It introduced how threat modeling could meet the requirements for developers and SMEs. Based on these sections, the review then provided a summary of key existing standards for data security and privacy and risk assessment in the medical domain in section 2.5. The examined standards provided aspects such as security and privacy principles and properties that could provide support for inexperienced developers and SMEs to determine how to meet the GDPR regulatory requirements.

Section 2.6 followed on from the standards and examined the models and risk assessment standards for data security and privacy in technical development. This section concentrated on threat modeling, as a natural progression from the previous recommendations of the literature review. The chapter continues with section 2.8, outlining existing frameworks in this domain. Finally, the chapter ended in section with a discussion on the standards against which security and privacy controls can be obtained. It was considered that part of the requirement to show compliancy in the medical domain was the ability to apply controls from the standards. Sections 2.5, 2.6 and 2.9 were examined with a view to incorporating the appropriate aspects from the standards and approaches into software engineering practices.

On conclusion of the literature review, the researcher determined that in order to provide support for inexperienced developers and SMES in this domain to meet the GDPR data protection requirements a framework encompassing many aspects from various standards, models and guidelines would be necessary. The researcher on completion of the review decided to build the framework directly from the seven GDPR principles. The GDPR data protection principles would be translated into security and privacy properties, to support language developers could understand. The developed framework should have a straightforward approach for SMEs and developers to show how their product or system meets the GDPR data protection principles legal

requirements. It should also encompass threat modeling to meet the risk assessment requirement. In addition, to take the guess work away the developers and SMEs should be provided the capability to show how any threats discovered have been mitigated in accordance with the domain’s requirements. The literature review established that any framework built should align to the data protection principles of the GDPR and SbD and PbD. Figure 2.7 presents the influence of the literature review on the elements of the framework. The aspects researched through the literature review are presented on the left in Figure 2.7 and the features of the framework influenced by these aspects are presented on the right. The researched security and privacy principles were applied to cultivate the data protection principles of the framework. The literature review on the properties needed to uphold the data protection principles resulted in the development of the framework properties. These properties were founded in the literature review of the threat models used to defend security and privacy of data in software development. The final part of Figure 2.7 reflects the literature review on security and privacy controls to demonstrate that any extracted risks have been mitigated. This literature review of standards used in the medical device security for controls influenced the development of the data flow security and privacy controls for the framework.

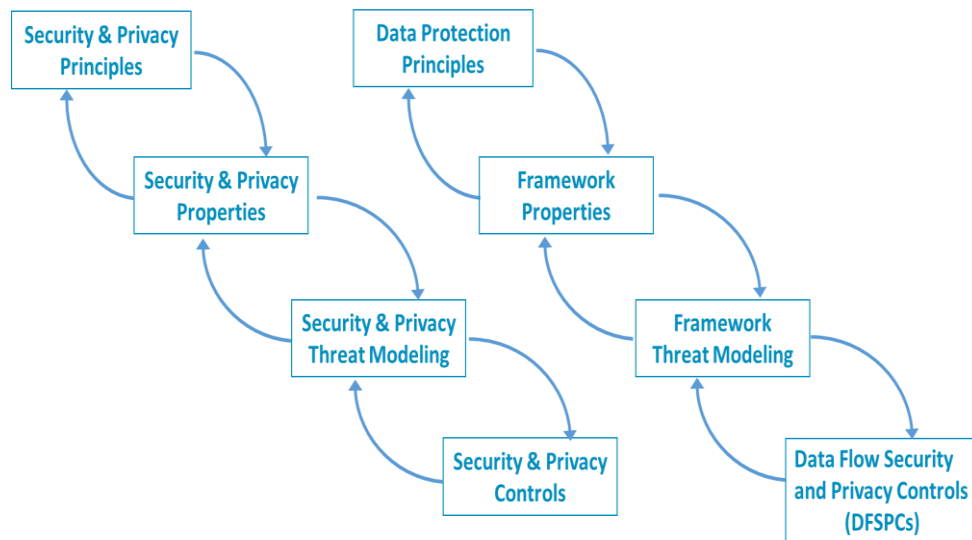


Figure 2.7 Elements of the framework

Chapter 3 will present a research methodology that is suitable to the research problem; allows the flexibility necessary for investigation in this area; and can be used for assessing the contributions of this dissertation.

Part 2 Research Methodology

Part 2 of this thesis contains one chapter as shown in Figure Chapter 3 outlines the fundamental theoretical approaches to research. It describes the various research methodologies that were considered and justifies the selection of the research methodology chosen to accomplish the research objectives of this study.

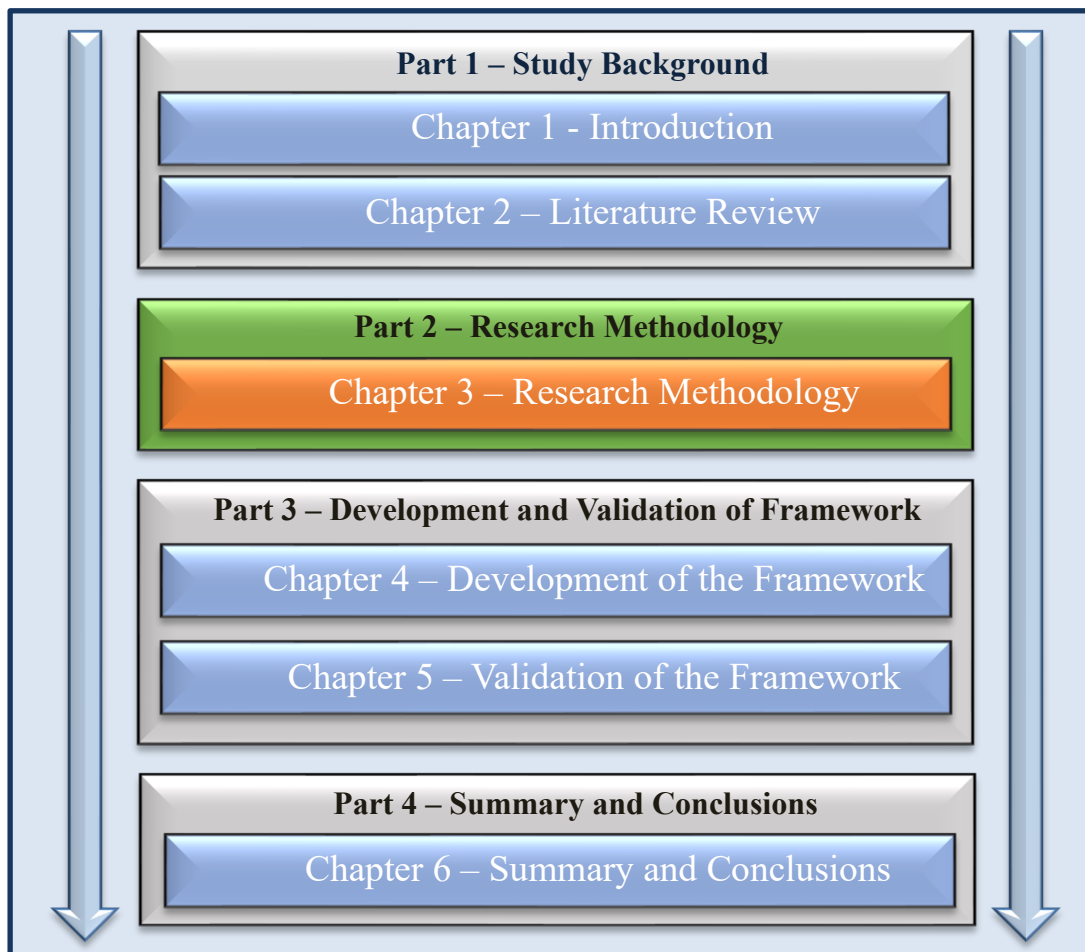


Figure 0.3 Map of the Thesis - Part 2

3 Research Methodology

3.1 Introduction

There are many ways to complete the research process and the choice of research methods is influenced by various considerations (Creswell 2003). The key considerations included the research questions and objectives presented in Figure 3.1, and the nature of the research problem, which is to link theory with practice within solving a specific problem for a specific client.

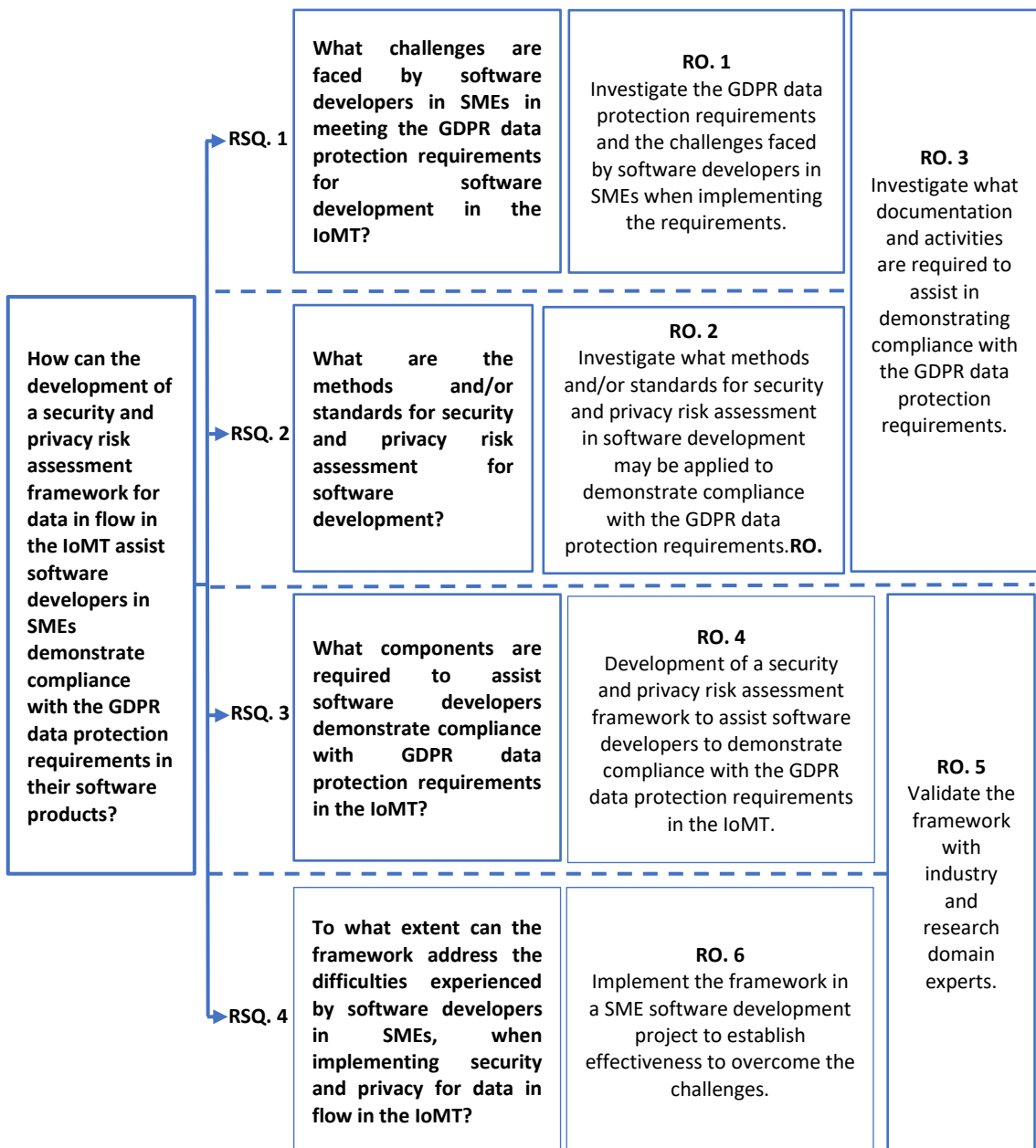


Figure 3.1 Summary of research question, sub-questions, and objectives

Chapter 3 Research Methodology

Dawson, presents research methodology as “*the philosophy or the general principle which will guide your research*” (2009, p.6). This chapter will present the general principles, methodology and techniques used to conduct the research.

This research followed the research approach developed by Saunders et al. (2009), known as the research onion. Saunders et al. (2009) developed this approach in consideration of the real-world complexity of the research process. The aim of this approach was to simplify the complexity of research so that the research process could be completed in a step-by-step manner. The research onion has six layers and includes: research philosophies; approaches; strategies; choices; time horizons; techniques; and procedures (Saunders and Tosey 2012). The research method used for this study follows the layers of the research onion, which are presented in Figure 3.2 Overview of research methods used from the layers of the research onion for this research project

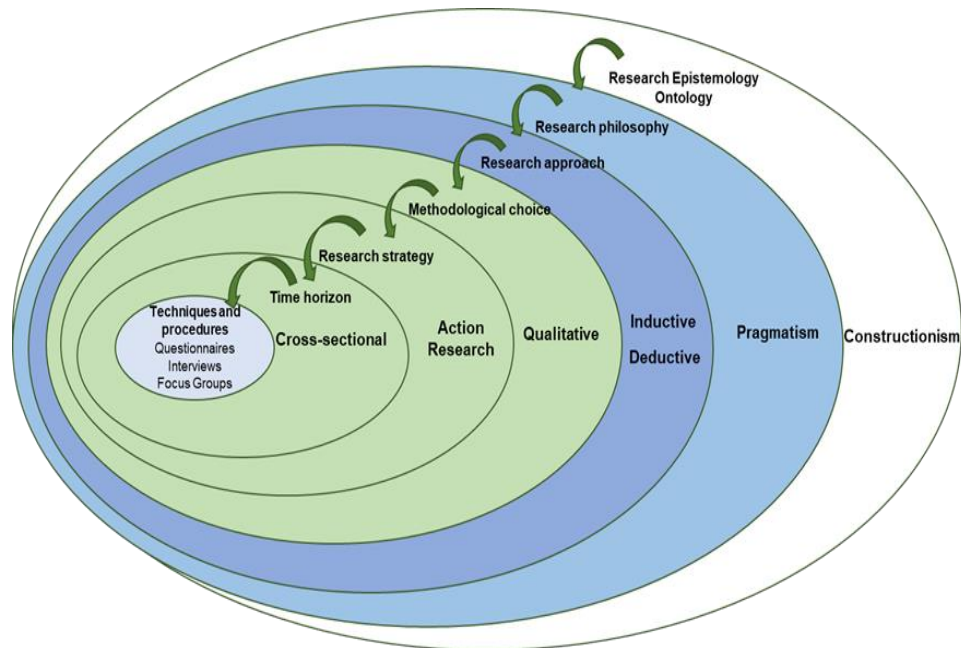


Figure 3.2 Overview of research methods used from the layers of the research onion for this research project

Figure 3.2 presents the relationship between the layers of the research onion and approaches used for this research project. The outer layer of Figure 3.2 Overview of research methods used from the layers of the research onion for this research project presents the overall epistemology for this research as constructionism. Moving toward the centre, a pragmatism philosophy was adopted incorporating both inductive and deductive research approaches. The methodological choice was qualitative to support an in-depth understanding of the situation investigated. Action research was chosen as the research strategy. The time horizon for the research was cross-sectional, which means

that data was collected at a single point in time, rather than being collected over a longer period. To collect the data, mixed method data collection techniques, survey, and interviews, were adopted for this research project.

3.2 Epistemology/Ontology Approach - Constructionism

The research project adopted the constructionism epistemology/ontology approach. Constructionism is the view that knowledge is socially constructed and meaning is not created but constructed out of the world and objects in that world that is already there (Illing 2014). Constructionism examines learning as building, which occurs irrespective of the circumstances in which the learning takes place; “*learning-by-making*” (Papert and Harel 1991, p.1). This research project involved the development of an object, artifact, through “*reflecting upon the use of those artifacts*” (Cross 2001).

The framework was developed in collaboration with the participants of the research project. These participants included the STATSports software development team and experts from the domains of medical, security and privacy software development. That is, the framework was developed from the interaction between the researcher and participants. This process is defined by Guba and Lincoln (2003) as transactional epistemology. For this research the researcher was the sole investigator who interacted with all participants. The researcher was embedded in STATSports (the test bed organisation). This facilitated the collection of the research information from within their software development team. Feedback and analysis of data collected from experts throughout the study was performed by the researcher.

3.3 Research Philosophy Approach - Pragmatism

The pragmatism philosophical approach was adopted for this research project. Saunders et al. (2009) argue, that if choosing between one research philosophy and another in practice is observed as unrealistic, due to the real-world intervening, the research philosophy position adopted is pragmatism. The basis of the pragmatic philosophy is the linking of practice and theory. In this research project, theory and practice influenced the design of the artifact and as such a pragmatic philosophy was appropriate. Also, this study used a mixed method approach and pragmatism represents the single most appropriate approach to such studies (Morgan 2007). Pragmatism proposes that researchers adopt a needs-based or possibility approach to selecting methods and approaches (Johnson and Onwuegbuzie 2004).

3.4 Research Approach - Deductive and Inductive

For this research project, a combination of inductive and deductive approaches was adopted. This research initially focused on identifying the challenges for software developers in SMEs with security and privacy of data in flow in the IoMT. This research was performed through the completion of a literature review, using inductive research. The literature reviewed the challenges for software developers from SMEs in applying security and privacy in software development. The literature review, also investigated GDPR data protection requirements, the standards and best practice in security and privacy for software development.

The researcher considered how the literature review could assist the developers in meeting regulatory requirements for the security and privacy of data in flow in the IoMT. The information gathered through the literature review was assessed alongside the needs identified for STATSports. The framework was developed from the findings of the literature review to address the organisation's needs and validated in multiple ways. This part of the research is deemed deductive. This follows the approach defined by Gray (2014), where on completion of inductive research the study follows deductive research. The researcher established a theory, developed a hypothesis, tested the hypothesis, analysed the outcome, and then confirmed or rejected their hypothesis.

3.5 Methodological Choices - Qualitative

The three layers following the approach layer of the research onion, focus on the research design (Saunders et al. 2009). These stages are shaded green in Figure 3.2 Overview of research methods used from the layers of the research onion for this research project presented earlier on pg. 87. The first of the design focus layers is the research strategy section. This study used a qualitative approach as the research was in collaboration with industry to explore a solution to an ever-changing situation. Within the qualitative approach the research used multi-methods. Multi-method refers to, using more than one method of qualitative collection technique, combining data collection techniques and corresponding analysis technique. A multi-method qualitative approach combining the use of questionnaires, expert review and focus groups has been used in this research.

3.6 Research Strategy - Action Research

The researcher considered several research strategies for this project; Action Research (AR) (Dawson 2009); Design Research (DR) (Dorst 2008) (also known as Design

Science Research (DSR) (Sein et al. 2011)) and Action Design Research (ADR) (Sein et al. 2011). Iivari and Venable (2009, p.3), specifies that while AR and DR are “*compatible and may significantly overlap, they are decisively different.*” The authors support their argument using Rapoport’s (1970) widely adopted definition of AR that “*assumes that there is a concrete client involved*” (Iivari and Venable 2009, p.4). This differs with DR which does not assume a specific client; “*DSR creates new means for achieving some general (unsituated) goal, as its major research contributions*” (Iivari and Venable 2009, p.4). DR addresses research through the building and evaluation of artefacts designed to meet identified business needs (Hevner et al. 2004). Additionally, there is differing roles of the researcher and the practitioner between DR and AR (Iivari and Venable 2009; Järvinen 2012). AR is defined as “*an iterative process involving researchers and practitioners acting together on a particular cycle of activities, including problem diagnosis, action intervention, and reflective learning*” (Avison et al. 1999, p.94). DR does not assume joint collaboration between researchers and the client. Given this research is based in solving the situated need of a specific client, the researcher is embedded in the organisation and the solution is developed through collaboration between researchers and the client so, DR was determined inappropriate.

Sein et al. (2011, p.37), define ADR “*as a new research method for Design Research that draws on Action Research.*” The authors propose that DR does not acknowledge that the artifact develops from interaction within the organisational context. They argue that “*while the researcher may guide the initial design, the ensemble artifact emerges through the interaction between design and use*” (Sein et al. 2011, p.40). ADR is built on the approach advocated by Iivari (2007) and Cole et al. (2005) in which an artifact is designed using DR and subsequently evaluated using AR. It was determined that ADR was not a suitable research strategy for this project. While ADR incorporates AR, ADR has a number of stringent requirements that AR does not. These requirements include a DR contribution in the form of design principles, which did not fit with the needs of the client project. ADR also requires that these principles should address a class of problems.

The research performed in this project sought to link theory with practice, and thinking with doing, within solving a specific problem for a specific client. AR is a research strategy suited to researching and supporting change, which the client of the research required. On consideration of these different research strategies, AR was considered the most appropriate research strategy for this research project. One of the

more widely practised and reported forms of AR in the information systems literature is Canonical Action Research (CAR) (Davison et al. 2004; Davison et al. 2012; Cruzes et al. 2018). This research adopted the research strategy CAR. In CAR, the researcher works collaboratively with a group of people to establish an improvement path for a given situation (Cruzes et al. 2018). Section 3.6.1 discusses the conditions required for AR.

3.6.1 Conditions Required for Action Research

This research project was positioned in the three conditions required for AR as outlined by Baskerville & Wood-Harper (1998).

3.6.1.1 Active Involvement

The first condition required for AR is that the researcher is actively involved, with explicit benefit for the researcher and organisation. The goal of the researcher (*which is by nature epistemological*) and that of STATSports (*which is by nature practical*) was maintained for outcome success (Cole et al. 2005, p.5). There was an importance and focus on a collaborative democratic partnership between the researcher and STATSports. The researcher was embedded in STATSports and collaborated directly with the software development team. This collaboration resulted in the change process to resolve the problem. The developed solution assisted STATSports to demonstrate to their clients, customers, and external ISO 27001 auditor, that their products met GDPR data protection requirements. The project supported the researcher's goal to expand scientific knowledge where the framework could inform other SME software development teams in the medical domain. The AR approach for this project assisted in practical problem solving for STATSports but also expanded scientific knowledge (Baskerville 1999; Saunders et al. 2009).

3.6.1.2 Applied Knowledge

The second condition for AR is that knowledge can be applied immediately. The emphasis in the AR approach is on an action rather than research about action. The components of the framework were developed following this process. The approach applied in this project corresponded with the typical AR iterative spiral process of diagnosing, planning, taking action and evaluating, presented in Figure 3.3 Action design research cyclical process (Sein et al. 2011) on the next page.

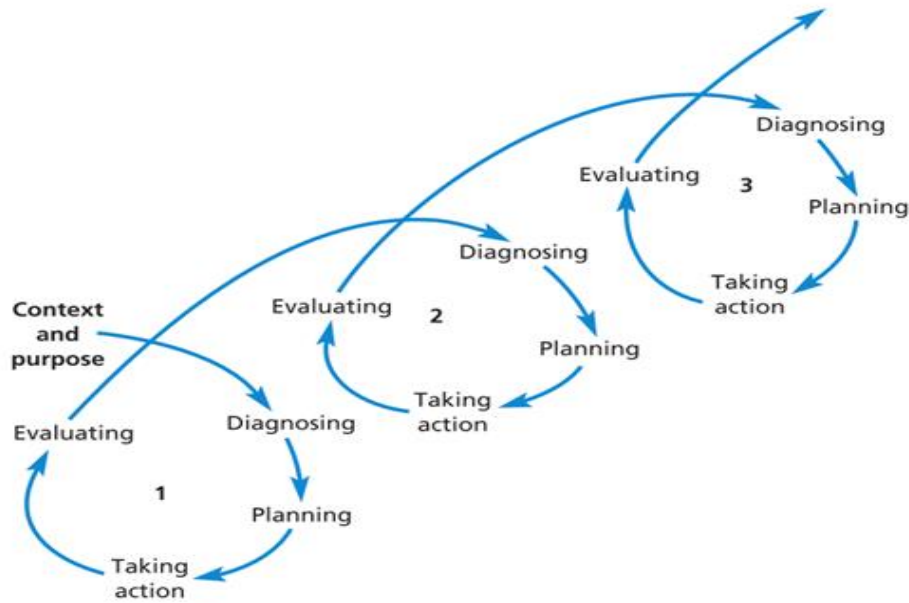


Figure 3.3 Action design research cyclical process (Sein et al. 2011)

3.6.1.3 Theory and Practice Linked

The third condition for AR is that the process links theory and practice. The researcher bridged the concepts between academia, which included the experts' feedback, to assist in the development of the solution.

Action research has been interpreted by researchers in a variety of ways and is sometimes referred to as a class of research approaches rather than a single uniform method (Baskerville 1999). Baskerville & Wood-Harper (1998) identify and describe ten forms of AR, their different models, structures and goals..

3.6.2 Canonical Action Research

As stated previously, the AR approach used in this project is Canonical Action Research (CAR) (Davison et al. 2004; Cole et al. 2005). Davison et al. (2004) applies the term canonical to formalise the association with the iterative, rigorous and collaborative cyclical orientated AR process developed by Susman and Evered (1978), illustrated in Figure 3.3 Action design research cyclical process (Sein et al. 2011) What makes CAR distinctive, is that other forms of AR do not combine these three attributes. The CAR cyclical process has five phases: diagnosing, action planning, action taking, evaluating, and specifying learning, presented on the following page in Figure 3.4 Canonical action research process (Davison et al. 2004; Smith et al. 2010). The first four phases of CAR

follow the cyclical process outlined above. The fifth phase in CAR, completing the loop, is Specifying Learning, which identifies the general findings (Smith et al. 2010).

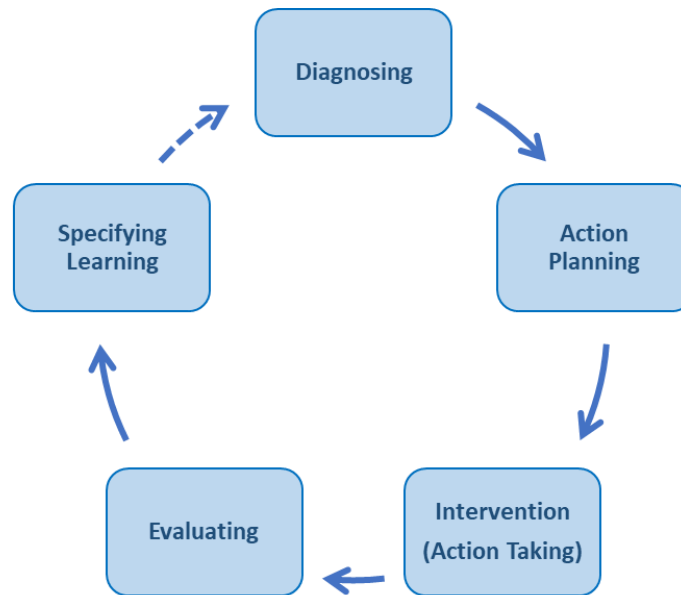


Figure 3.4 Canonical action research process (Davison et al. 2004; Smith et al. 2010)

The CAR approach was considered most appropriate for this project as it involved the development, implementation, and validation of the framework. Within information technology, the development of the framework included the iterative engagement of the researcher with experts and the software development team within STATSports. The CAR approach adapted for this project is presented in Figure 3.5 on the next page. This adaptation was used due to the broad collaborative nature of the development of the various aspects of the framework. CAR is distinctive among all the forms of AR in that it is collaborative, iterative, and rigorous and involves focus on both organisational development and the generation of knowledge (Davison et al. 2004).

The researcher took into consideration the research conducted by Cruzes et al. (2018) presented in the paper "*Challenges and approaches of performing canonical action research in software security*". The paper discusses the challenges and approaches of conducting CAR in the area of software security and privacy in relation to the GDPR. The authors argue that the application of CAR in software security and privacy can enhance the understanding of this complex technical domain (Cruzes et al. 2018). The paper assisted in identifying potential challenges that may hinder the successful application of CAR in this research through highlighting the challenges they encounter. These challenges include difficulty in researcher-client agreement, trust and

commitment. Other challenges such as the complexity and managing the research process in the software development environments were highlighted and difficulties in systematic analysis and reporting of data collected from different sources (Cruzes et al. 2018). They underlined the need for a structured approach to conducting CAR in this field to ensure the sustainability and scalability of the proposed solutions.

The learnings from the paper for the researcher was to adopt the approaches the authors recommended that can enhance the success of CAR in software security research. The paper offered the five phases for performing CAR, presented in Figure 3.5 below. The authors provide recommendations for each of these phases, which the researcher adopted. These approaches include developing a clear research question, involving relevant stakeholders from the outset, using multiple sources of data, establishing a collaborative research team, adopting an iterative and adaptive research process, and leveraging existing tools and frameworks. Overall, the paper provided insights into the challenges of conducting CAR in software security and assisted in developing a structured approach.

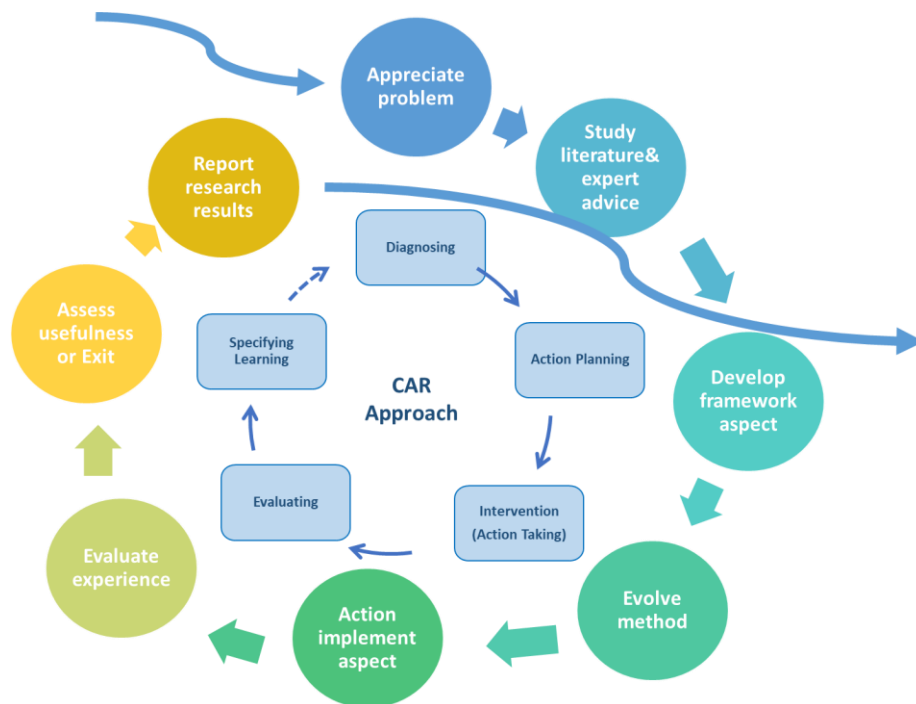


Figure 3.5 Adaption of the CAR approach for this research project

3.6.3 Diagnosing

Diagnosing in the CAR approach starts with a detailed diagnosis of the current organisational position (Davison et al. 2004). Davison (2004; 2012) asserts, it is vital that

the researcher understands the problem but, also identify the scope of the investigation and the specific processes to determine an appropriate intervention. The diagnosis will inform the planning of actions (Davison et al. 2004). Diagnosing in this research included the steps, appreciate problem and study literature and expert advice. This stage involved RSQs. 1, 2 and 3 and encompassed ROs. 1- 3, shown in Figure 3.6 below.

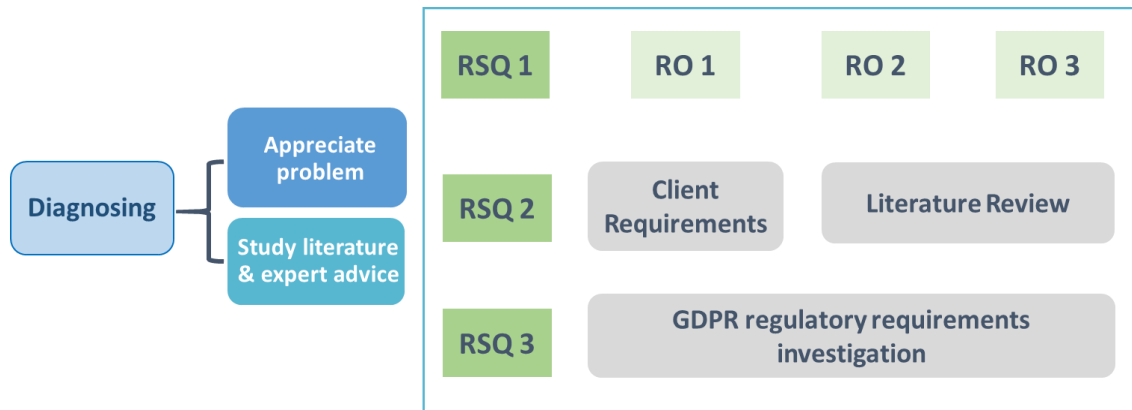


Figure 3.6 Diagnosing stage of study

This research began with identifying the challenges experienced through a literature review and by the client. The challenges of the software development team in relation to compliancy requirements for security and privacy of data in flow for their software products was investigated. The compliancy requirements were driven by the GDPR regulation (EU General Data Protection Regulation (GDPR) 2016), and certification for the ISO 27001:2013 – Information Security Management Systems standard and best practice. The challenge was established by the researcher in collaboration with the client and the software developers. The development of the comprehensive framework solution was completed through the CAR approach presented in Figure 3.5 Adaption of the CAR approach for this research project on pg. 94. There were four cycles in this research approach. There is no fixed number of cycles that are recommended for CAR. The iterative “*characteristic of CAR infers a cyclic process of intervention, with the conduct of (rarely) one or (more usually) several cycles of activities that are designed to address the problem(s) experienced in the organisational setting*” (Davison et al. 2004, p.68). The CAR research in security of software systems by Cruzes et al. (2018) discussed in section 3.6.2, did not reveal how many cycles they implemented. They did state that there were many cycles running at the same time with different focus and noted that in two years they have performed some full cycles of CAR. Each cycle began with diagnosing the task for the distinct component of the framework. The diagnosing process included

appreciation of the problem followed by a study of the literature and advice from experts. When the decision was made on the appropriate component solution, the focus of the research changed from exploratory to explanatory. The explanatory aspect was the development of the individual framework element to address the challenge faced. It was agreed each framework component would be evaluated by the client software development team. It was also agreed the framework solution would be implemented into the client software development cycle of a new cloud solution product.

3.6.4 Planning

The planning stage occurs when a detailed situation and problem diagnosis has been completed and a focal theory identified (Davison et al. 2012). In this research this stage included the steps, develop framework aspect, and evolve framework aspect. This step involved RSQs. 2 and 3 and encompassed ROs. 3 and 4, shown in Figure 3.7 Action planning stage of study

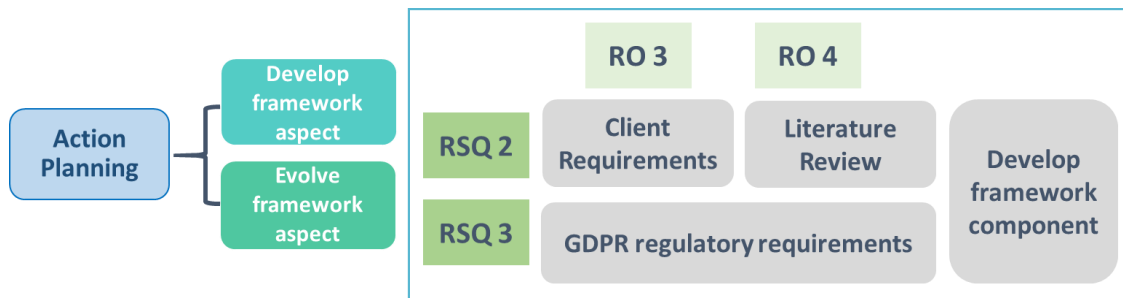


Figure 3.7 Action planning stage of study

At the planning stage, two distinct aspects of this research were completed:

- The researcher would develop the framework component from the literature review, expert advice the diagnosing phase.
- The framework component was developed to solve the challenge for the software development team and appropriate experts.

There were many components required for the final framework. The decision was to develop a framework comprised of the distinct components. The framework would be intended for inexperienced developers in SMEs to assist in meeting GDPR data protection requirements for security and privacy of data in flow in the IoMT. Inexperienced developers in the context of this research represents developers that have limited knowledge and hands on practice in implementing security and privacy in software development. It was decided the documentation of this systematic process

would be in an innovative DPIA. A DPIA is a requirement of the GDPR for any product processing personal information. The development of the framework and the DPIA was completed simultaneously. This resulted in the majority of the cycles being developed at the same time.

3.6.5 Action Taking

The action taking stage is when a focal theory identified is put into practice (Davison et al. 2012). In this research, this stage comprised the steps of action implement aspect and evaluate experience. The development of the framework for this study used the input of both experts and the STATSports software development team. This meant that the action implementation intersected with the evaluate experience step. This stage involved RSQ. 3 and encompassed ROs. 4, 5 and 6, shown in Figure 3.8 Action taking stage of study below.

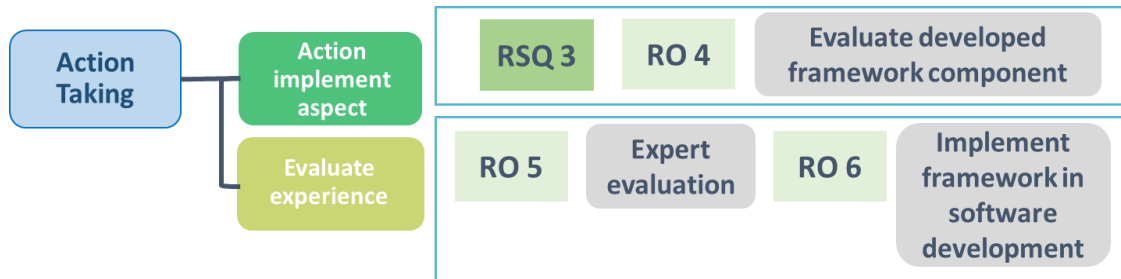


Figure 3.8 Action taking stage of study

Action taking in this study was completed in two ways. The first action taking occurred with the development of the components of the framework. As previously stated, each component developed for the framework was supported with expert feedback and the STATSports software development team. The researcher gathered feedback during the development of each component. The development team would discuss the individual component or step with the researcher providing guidance as required to keep the process within their requirements. The guidance involved revision of each component or step. The researcher aided the development team and each expert as and when it was needed.

This process took place through each of the six steps of the framework. Once the framework was developed, the second action taking included implementation of the framework in a software development project. At this stage the researcher collaborated with the head of software engineering and the software architect in the implementation of the framework. It was decided that the implementation would be completed step by

step as per the framework. Each step’s implementation commenced with training for the development team. Training was provided by the researcher to key members of the software development team. This training involved a thorough explanation of the step and included performing model aspects in accordance with the step. This implementation is outlined in detail in chapter 4 and involved the organisation adopting the framework.

3.6.6 Evaluating

When an action taking intervention has been performed, its impact on the problem situation needs to be evaluated (Davison et al. 2012). In this research, this stage comprised the steps, evaluate experience and assess usefulness or exit. The evaluating stage involved RSQ. 4 and encompassed ROs. 5 and 6, shown in Figure 3.9 Evaluating stage of study.



Figure 3.9 Evaluating stage of study

On completion of each distinct step the researcher met with key members of the development team to collect feedback and make changes through collaborative discussion. The researcher guided the discussions to evaluate the usability, usefulness, and requirements coverage of the framework. Other features considered naturally through these discussions included ease of implementation and understandability. During the development of the steps the researcher also obtained feedback from various experts. This is outlined in more detail in chapter 4.

The framework was also evaluated with an international expert. This was done with a semi-structured interview (SSI) led by the questionnaire. Prior to implementing the framework, the development team had not delivered a DPIA covering security and privacy. After implementing the framework in this research, the development team identified that this model could accommodate the risk assessment process for the security and privacy of a software product. The developers considered that the assessment contained in the framework would be transferable to other software product development projects. The SME were able to provide the completed DPIA to the ISO 27001 external auditors to provide evidence of the risk management process for security and privacy of data within the software product. From a business perspective, the SME provided the

DPIA in tenders to provide evidence of security and privacy of data risk assessment, regulatory compliancy, and conformity to best practice for security and privacy by design. A final focus group was conducted with the development team to evaluate the overall framework after implementation.

3.6.7 Report Research Results

The aim of specifying learning in this research is twofold. It is to consider the evaluation of the activity and how it impacted change for the organisation. Secondly it is to report the research results, reporting on the problem, the artifact, its utility and originality, the rigor of its design and its effectiveness to the participants, researchers, and other relevant audiences. This will be achieved through publication of this thesis, publications in international conference proceedings, an international journal, workshops, and presentations at international medical and security and privacy seminars.

3.7 Time Horizon – Cross-Sectional

Gray's (2014) theory is that most research studies are cross-sectional, primarily because of the pressure of time and resources. This was true for this project as the collaborative aspect was with a software development team that had time constraints. This meant the time-scale available was limited and involved looking at data from the software development team at one specific point in time. The implementation of the framework adopted a cross-sectional time horizon to be compatible with the product's development process. The interview data was also cross-sectional and included both developers and experts. The expert review was completed at the specific point in time of the framework development. This point in time was when the framework had been developed through collaboration with the software development team and experts. The focus groups were based on the current organisational structure and role the participants and corresponded to the framework at the specific point in time of the framework development.

3.8 Techniques and Procedures Choices

The tools used to collect the data in this research project was an important aspect because the study required discussion and collaboration. The main method of data collection for this research was survey. Cross-sectional studies often use a survey approach (Gray 2014). This research is collecting information on a cross-sectional specific action therefore, the survey approach was considered suitable. Survey collection of information typically involves one or more data collection techniques such as: questionnaires,

structured or SSI, focus groups, observations, attitude scales, and standardised tests of attainment or performance (Cohen et al. 2005; Saunders et al. 2009). This research used the survey data collection techniques of questionnaires with SSI and focus groups. These methods of data collection were performed with the international expert and the STATSports software development team. The results of these data collection techniques are discussed further in chapter 5.

3.8.1 Introduction

This section will discuss the survey techniques to collect the information from the expert and STATSports' software development team. Firstly, the questionnaire survey approach for this research will be outlined to collect information from the STATSports' software development team and the expert. The discussion will include how the questions were determined and the question types, sequence and questionnaire layout are discussed. This section will next discuss the survey techniques, focus group interviews and SSI. The focus group interviews relation to and purposes in the research is discussed. Finally, the SII use in the research is discussed and introduces the six stages presented by Rabionet (2011) to carry out a qualitative SSI.

3.8.2 Questionnaire

The questionnaire is one of the most extensively used data gathering techniques within the survey approach (Saunders et al. 2009). Saunders et al. (2009) do suggest that with exploratory research, such as this research, questionnaires are valuable when linked with other data collection methods like interviews. This was the approach taken with this research. The questionnaire was used to lead the discussions in the SSI and focus group. The researcher used the questionnaire in this way to keep the SSI and focus group in line with the overall research aims. Given the smaller size of the sample for this research project, the questionnaire was less structured, more open and word-based (Cohen et al. 2005). By using the questionnaire, the researcher was able to leave the interview with feedback that was easy to record, summarise and analyse.

The researcher took a typical approach with the questionnaire, gathering information from participants on demographic characteristics, level of experience and information regarding factors relevant to the study. The information gathered included:

- The importance of data security and privacy in their area;
- The domain, safety critical or not;

- Their level of experience;

The researcher added additional space for the participant to provide any further information around their experience and involvement in the domain. The questionnaire was developed according to Burgess (2001, p.6), guide to the design of questionnaires three elements:

1. Determine the questions to be asked;
2. Select the question type for each question and specify the wording, and;
3. Design the question sequence and overall questionnaire layout.

The questionnaire was internally validated by three members of the Regulated Software Research Centre (RSRC) within Dundalk Institute of Technology. The RSRC members were Prof. Fergal McCaffery, Dr. John Loane and Catherine McEnroe. Both Prof. Fergal McCaffery and Dr. John Loane have over 15 years' experience in research and provide experienced knowledge through their own research and supervision of Masters and PhD students for validation of the questionnaire. Catherine McEnroe has over 10 years' experience within industry and implementation of research through questionnaires and focus groups. The final questionnaire including the expert review information leaflet and participant profile is available in Appendix A

3.8.2.1 Determine the Questions to be Asked

This was a key part of the development of the questionnaire. A link needs to be established between the research aims and the individual questions via the research issues (Burgess 2001). The development of the questionnaire was completed with the creation of a matrix for mapping the steps and components of the framework to the questions to meet the overall research aim. The purpose of creating this matrix was to help display whether any gaps exist in what was being asked. This matrix is provided in Appendix B. The questions were determined around the themes of value, composition, and usability of the framework. The matrix considered each question according to the RSQs. Using the questionnaire this way the researcher was able to ensure that the specific data required to answer the research question(s) and achieve the research objectives was collected. As stated by Burgess (2001), making sure that the questionnaire design addresses the needs of the research is a critical part of good research design.

3.8.2.2 Question Types

The questions were divided into open and closed. The closed questions were on a Likert scale to collect broad opinion and feedback around the value, composition, and usability

of the framework. There was additional space to give the participants the opportunity to provide further information and insights as they deemed necessary. The open questions were used to lead the discussions around the research questions and objectives in the SSI and focus group. The questionnaire incorporated both more theoretically driven and open-ended key questions as a starting point for the interviews.

The researcher assessed and adjusted the interview questions to ensure there were not too many related to one research question and too few to other research questions. The questions were reviewed by two members of the RSRC to assess if they:

- Were concise and unambiguous;
- Avoided questions involving negatives;
- Ask for precise answers;
- Avoided leading questions (Burgess 2001).

3.8.2.3 Question Sequence and Questionnaire Layout

The questionnaire was preceded with an information leaflet that provided the title of the research, background information, participant consent form, participant profile and instructions on how to complete the questionnaire. When designing the questionnaire, the researcher considered the wording of individual questions prior to the order in which they appear. Category themes were used to separate the questionnaire into three parts: value, composition, and usability. The questions were ordered and flowed within these chosen themes. Within the themes the questions were numbered to ensure the questions were logical to the participant. The questions were designed to elicit feedback and opinions on specific areas related to the framework. These areas were grouped into three sections as follows:

1. The value of the framework for the SME software developers and meeting the GDPR data protection requirements;
2. The composition of the framework to direct the SME software developers meet the GDPR data protection requirements;
3. The usability of the assessment framework for SME software developers.

These areas were chosen as they had been identified through the literature review and in discussion with the developers, as being areas that the framework would need to address to meet the GDPR data protection requirements.

The questions in section 1 of the questionnaire addressed the value of framework. These questions concentrated on the areas of value of the framework for SME software

developers. Specifically, as regards to security and privacy risk assessment, the main benefits, obstacles, or problems they encounter with the framework.

Section 2 focused on the composition of the framework. Questions in this section assess how practical the separate steps and their corresponding activities are for SME software developers. The ease with which SME software developers can use these is also examined. The appropriateness of the structure of the framework and the flow of the steps and corresponding activities were also addressed in this section.

The questions in section 3 address the usability of the framework. This section focuses on the implementation of the framework by SME software developers. The focus was on assessing the level of ease, the potential difficulties in the different steps and the corresponding implementation activities. Questions also focused on the ability of the framework to be tailored for use in a SME software development team. At the end of each section there was an opportunity to suggest improvements and highlight deficiencies.

3.8.3 Focus Groups and Semi-Structured Interviews

Focus groups and SSI methods of data collection fall under the category of interview (Cohen et al. 2005; Saunders et al. 2009). Interviewing is key to many forms of qualitative educational research. The categories of interviews vary broadly in accordance to the source. Saunders et al. (2009) provide a typology, presented in Figure 3.10 below.

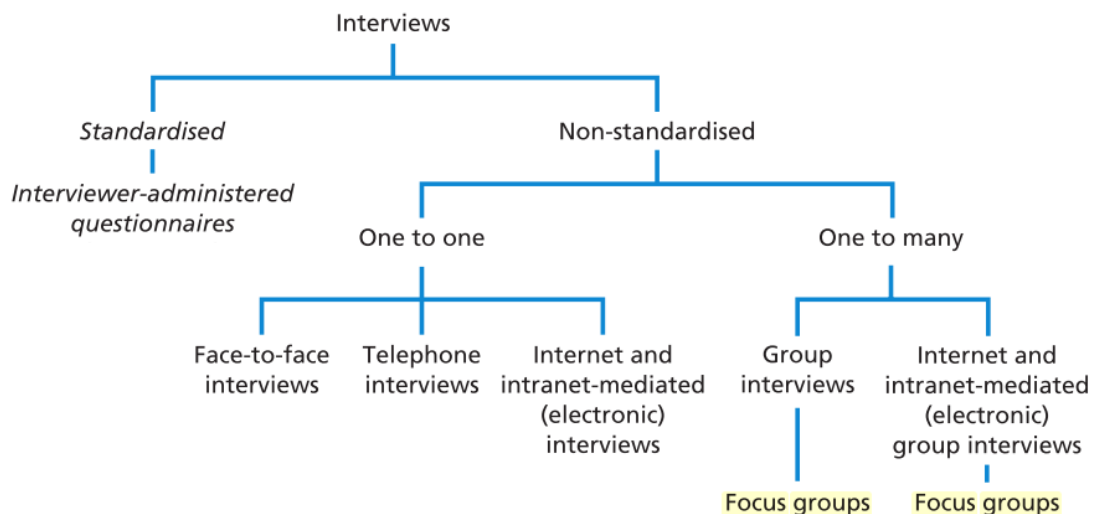


Figure 3.10 Typology of interviews (Cohen et al. 2005; Saunders et al. 2009)

Interviewing was selected for this study because it offered the ability to establish if the framework answered the overall research question and RSQ.4 and the research objectives 5 and 6. The researcher considered the importance of the form of interview used, and its level of formality, given the researcher was embedded in the organisation. In addition, the researcher recognised the interview structure should answer the research questions and objectives in a structured way, i.e., fitness for purpose (Cohen et al. 2005; Saunders et al. 2009).

3.8.3.1 Focus Group Interviews

Focus groups “*is where a number of people are asked to come together in order to discuss a certain issue around research*” (Dawson 2009, p.79). Kitzinger and Barbour (1999), assert that existing groups can be used in focus group interviews, which is the case in this study. The developed artifact, the framework, would be used in an existing group context of the software development team. Consequently, the feedback on the framework was gathered from this group. This approach fitted very well with the overall research aim of exploring if the framework addresses the difficulties experience by the software developers and RSQ. 4. This type of focus group interview assisted in the validation process throughout this study when working with the software development team. The focus group interviews served four purposes in the research:

- To gain an understanding of the challenges that were faced by the software development team when implementing data privacy and security in their products;
- To present to the software development team the proposed action research approach. To ensure that the software team understood the purpose of the framework and its requirements in terms of the responsibilities to meet GDPR regulatory requirements and data privacy and security requirements for their products;
- To ensure that the framework was compatible with software development by obtaining feedback from the software team and make changes to the framework when considered appropriate;
- To evaluate if the challenges that were faced by the software development team when implementing data privacy and security in software development for their products were addressed.

These interviews facilitated the collection of unique data on the framework. The researcher is not aware of what she does not know, and relied on the feedback of the

software developers (Cohen et al. 2005). The focus group interviews were completed in an informal setting to promote free exchanges of opinions, ideas, and feedback. These interviews were led by the researcher. During the formal validation phase of the study the final focus group was guided by the questionnaire and directed by the researcher. To ensure the reliability of data collected during the final focus group session, a findings report was circulated to all focus group participants following the session. The circulation of the report was used to allow participants to confirm the findings of the focus group session and correct any errors or omissions.

3.8.3.2 Semi-Structured Interview

A semi-structured interview (SSI) was chosen to collect qualitative feedback data from the international expert. Adams, describes semi-structured interviews as, “*Conducted conversationally with one respondent at a time, the SSI employs a blend of closed- and open-ended questions, often accompanied by follow-up why or how questions*” (2015, p.492).

The SSI was used in this research to capture opinion and feedback on the value, composition, and usability of the framework from the international expert. The purpose of this approach was to inform the framework with a practical process and components for implementation that is correct and validated through expert review. The expert was sent an information pack before the SSI took place, which included the questionnaire. The open-ended questions in the questionnaire were used to allow the researcher flexibility. This was to provide an environment so that other important information, from the knowledge and experience of the expert could still occur (Dawson 2009). The researcher followed the six stages presented by Rabionet (2011) to carry out the qualitative SSI and focus group interviews for this research:

1. Selecting the type of interview;
2. Establishing ethical guidelines;
3. Creating the interview protocol;
4. Conducting and recording the interview;
5. Analysing and summarising the interview;
6. Reporting the findings.

The six stages are discussed in chapter 5. To ensure the reliability of data collected during the SSI, the transcript and discussion analysis was sent to the expert. This was to allow the expert to confirm the findings of the SSI and correct any errors or omissions.

3.9 Methodology Approach Summary

This section outlines the research methodology applied to this project, a synopsis of which is presented in Figure 3.11 Summary of the research methodology, below.



Figure 3.11 Summary of the research methodology

This research methodology was completed to answer the overall research question:

How can the development of a security and privacy risk assessment framework for data in flow in the IoMT assist software developers in SMEs demonstrate compliance with the GDPR data protection requirements in their software products?

To answer this overall research question four research sub questions (RSQs.) were developed. Each RSQ. had several research objectives (ROs.). How the RSQs. and their corresponding ROs. were applied during this study is presented in Figure 3.12 Canonical action research strategy applied to this research

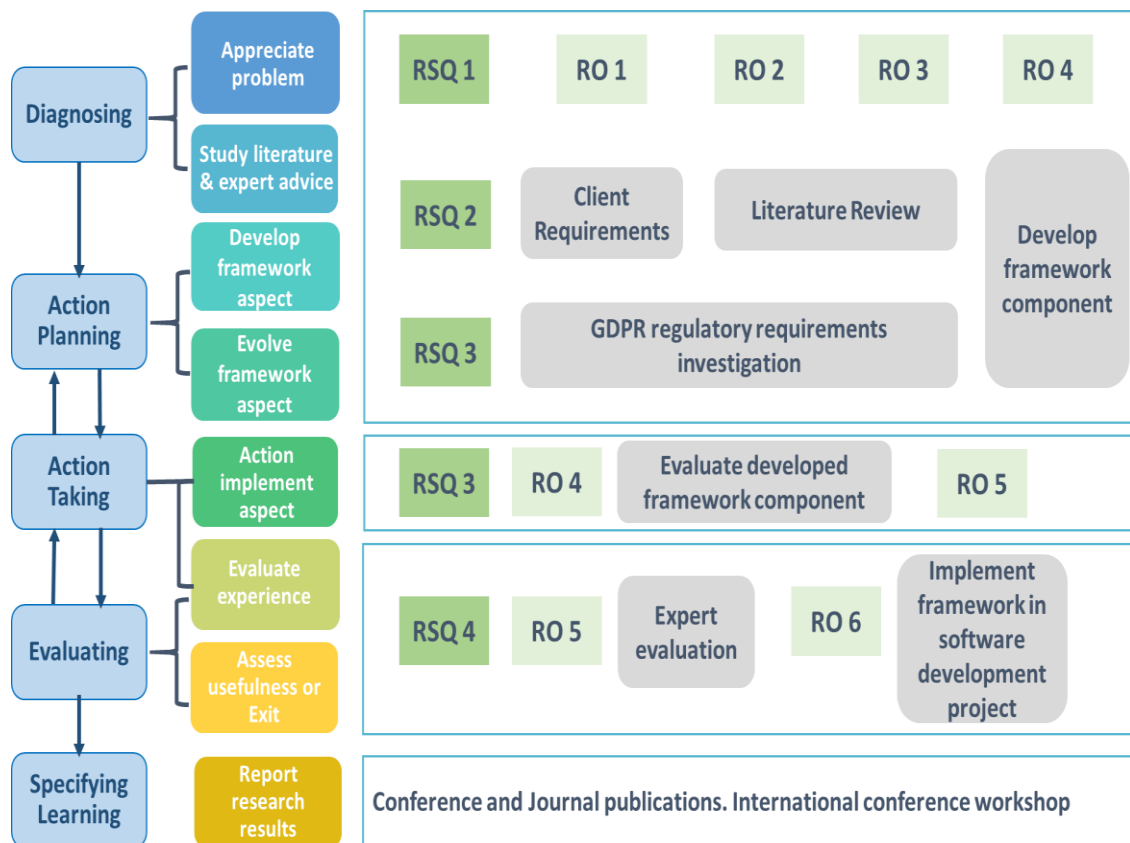


Figure 3.12 Canonical action research strategy applied to this research

The first stage; Diagnosing, provides answers to RSQ. 1 and RSQ. 2. The literature review considered the challenges for the STATSports development team. This guided the literature review to investigate:

- Current practices for security and privacy of data in flow in the IoMT and software development;
- Current security and privacy standards;
- Application of security and privacy controls in software development;
- GDPR regulation and data protection requirements;
- GDPR DPIA requirements;
- Current security and privacy risk assessment models employed in software development.

The action planning included the literature review and development for the individual framework components and provided the answer for RSQ. 2. The action planning stage was completed in collaboration with the client, the software development team and security and privacy experts. The action taking stage implemented the

framework within a software development project. During this part an iterative approach was taken using feedback and focus groups to make changes and improve the implementation and aspects of the framework. The evaluating and specifying learning stages of this Action Research answered RSQ. 3 and RSQ. 4. The evaluation and specific learning was discussed in the focus groups with the developers. The expert review evaluated the framework through the questionnaire and follow-up SSI driven by the questionnaire. The specific learning was communicated through an international conference and journal publications.

3.10 Research Quality

It is essential to assure research quality. To evaluate qualitative research, reliability and validity are two important concepts (Cohen et al. 2005; Braun and Clarke 2013). Reliability is concerned with the degree to which a measure gives consistent results and is also a prerequisite for validity (Mathers et al. 1998). Validity is the degree to which a study measures what it purports to measure (Mathers et al. 1998). Within research, triangulation is fundamentally *“important to ensure reliability and validity of the data and results”* (Fusch et al. 2018, p.23). Cohen et al. cautions *“it is impossible for research to be 100 per cent valid,”* however, if *“a piece of research is invalid then it is worthless”* (2005, p.105). There are several different types of validity, for this research three criteria for validity were selected: internal, external and construct.

3.10.1 Reliability

Reliability is the extent to which a test or process produces similar results if the test or process is replicated under constant conditions and yields the same results on all occasions (Bush 2007; Easterbrook et al. 2008; Bell 2014). However, concerning this research, reliability is to provide a measure of confidence that repeating the process would ensure consistency and replicability over methods, over time and over groups of respondents (Cohen et al. 2005; Bush 2007). Within the study the researcher adhered to these recommendations. An example would the use of investigator triangulation was employed to reduce bias; this is further discussed in section 3.10.2 below. There were several experts consulted during the development of individual components of the framework throughout. The use of experts was not depended on one individual and they were mixed gender. In addition, the research included different type of personnel involved within the company and also mixed gender.

There are a number of steps taken during this research to consider reliability. Consideration in the research was applied to potential issues of bias, introduced by either the researcher, developers, or experts. The use of the external experts and implementation into a development team reduced introduction of bias by the researcher (Easterbrook et al. 2008).

Two of the experts involved in the framework development were engaged in security in software development and the other expert is established in the security and threat modeling domains. The external expert reviewer of the framework has more than 10 years' experience in security and privacy in software engineering with specialties that include: threat modeling, privacy engineering, security engineering and data protection. Implementation of the framework into the development team was guided as necessary by the researcher. The software development team completed the questionnaire collectively as a team. The questionnaire was used as the basis for the development of the focus group questions. The returned questionnaires from the software development team and the expert provided additional follow-up questions in the focus group. The analysis of the interviews was provided to the expert and the software team participants, to allow for agreement on the interpretation of data and to resolve conflicts. The researcher followed the proposal from Flick (2009) of documenting the research process in a comprehensive and reflexive way. This included explaining the decisions that were taken during the research process and reflecting on why the decisions were taken. To complement this process all interview transcripts and focus group findings were circulated to participants to ensure their accuracy.

3.10.2 Internal Validity

“Internal validity relates to the validity of the study itself, including both the design and the instruments used” (Mathers et al. 1998, p.53). The purpose of internal validity is to demonstrate that the event, issue or set of data the research provides can in fact be upheld (Cohen et al. 2005). A technique to strengthen internal validity is triangulation (Flick 2008; Saunders et al. 2009). Throughout this research, a number of forms of triangulation were used that belong to the four basic types developed by Denzin (Denzin 1978).

1. Data triangulation is the use of two or more independent sources of data (Easterbrook et al. 2008). Data triangulation was used throughout the AR process. During the development of the framework the literature review, multiple experts and participants were used to discover the appropriate components and processes

for the framework. Triangulation was achieved with the framework review phase, a domain expert was used to assess the value, composition, and usability of the framework. The feedback from this review was used to inform the follow up questions for the focus group review with the software development team. This triangulation corroborates findings between the expert review and focus group and provides greater overall confidence in the research.

2. Investigator triangulation “*refers to the use of more than one observer (or participant) in a research setting*” (Silverman 1993, p.99). Investigator triangulation is important to reveal and minimise biases coming from the individual researcher (Flick 2008). Investigator triangulation was provided by the researcher’s supervisors and security experts in the development of the Data Flow Security and Privacy Controls (DFSPCs). Triangulating the findings from the three examiners and the researcher allowed the approach, biases, and findings to be directly compared and resulted in the final DFSPCs. Corroborating the controls and verifying their interpretation with multiple investigators increased the value of the findings. Investigator triangulation was employed with a second researcher assisting during the focus group sessions to ensure understanding of the data collected and to minimise biases.
3. Theory triangulation was supported using external domain experts, which involves “*approaching the data with multiple perspectives and hypotheses in mind*” (Fox and Denzin 1979, p.297).
4. Method triangulation “*involves a complex process of playing each method off against the other so as to maximize the validity of field efforts*” (Denzin 1978). Method triangulation was also used in the research with data being collected through expert review and focus group sessions. Saunders et al. (2009) provides an example of using semi-structured or group interviews as a valuable way of triangulating quantitative data collected by other means such as a questionnaire. There was triangulation between the questionnaire, the interviews, and the participants of the interviews. The research questionnaire was based on open ended questions followed up with focus groups and semi-structured interviews (SSIs). These questionnaires provided the discussion basis for the focus groups and SSIs. This produced “*a sample which is representative of the particular population under study and produced findings which may be generalised to the wider population.*” (Mathers et al. 1998, p.7).

3.10.3 External Validity

“External validity relates to the extent to which the findings from a study can be generalised” (from the sample) to a wider population (and be claimed to be representative) (Mathers et al. 1998, p.52). To assess the applicability of the research results to other SMEs and development teams, the description of the context in which the framework was implemented is described in chapter 5. This implementation was conducted in a SME development team that comprised of members ranging from those who had no experience and knowledge through to members that had limited levels in this domain, predominantly in security. The development team structure is outlined in chapter 5. Even though the action research project was conducted in an SME setting, the framework is based on the principles of threat modeling and aligned to the risk assessment processes of ISO 14971 and AAMI TIR 57. Thus, the framework has been designed to be adapted for use in a variety of development settings.

3.10.4 Construct Validity

Construct validity *“is the extent to which the measurement corresponds to the theoretical concepts (constructs) concerning the object of the study”* (Mathers et al. 1998, p.50). It is a demonstration that a test is measuring the construct it claims to be measuring. Cohen et al. (2005, p.132) present two aspects that threaten construct validity:

- Under representation of the construct, i.e., the test is too narrow and neglects significant facets of a construct;
- The inclusion of irrelevancies - excess reliable variance.

Construct validity can be demonstrated from several perspectives. A study has construct validity if the inferences that are made can be tied to the conceptual framework of the study. In this research the construct validity is to demonstrate that the categories used for the framework are meaningful to the client and developers. The construct validity is supported by the questionnaires followed by the focus groups. The researcher used the feedback from the expert to construct the follow up questions for the focus group. In addition, the questionnaires were returned to the researcher before the focus group. This assisted in verifying the researcher’s interpretation of the questionnaire answers. This is to ensure the researcher’s analysis truly reflects the way in which the developers experience and interpret the framework. In addition, the research engaged external experts to interpret the construct validity of methods used by the framework. As construct validity is an assessment of how well the research has translated their ideas or theories

into actual programs or measures, the use of external experts in the domain to review the framework was employed. The experts considered the use of the methods applied to the framework and if these methods were applied in accordance to the meanings of the theoretical terms, as defined by Easterbrook et al. (2008).

3.11 Summary

This chapter presented an outline of the research methodology used for this study. This research will be conducted using the four fundamental elements outlined by Crotty (1998) in alignment with the layered structure of the research onion (Saunders et. al. (2009). The data collection method was completed using questionnaires, focus groups and semi-structured interviews, which were embedded within the methodology of Action Research. This methodology is adapted through the theoretical philosophy of pragmatism which exemplifies a constructionism epistemology. This approach was deemed appropriate for completing research of a specific identified requirement as related to the research study. The last section of this chapter considered research quality in terms of reliability and validity. This section detailed the steps that this study has taken to mitigate threats to the reliability and validity of this research.

The following section, Part 3, discusses the AR conducted and the development and validation of the framework. This section includes details of the AR cycles conducted, data collection, analysis, and interpretation.

Part 3 Development and Validation of the Framework

Part 3 of this thesis contains two chapters as shown in Figure 0.4 below. Chapter 4 discusses the development of the framework. Chapter 5 discusses the validation of the framework by expert review and implementation into a software development team.

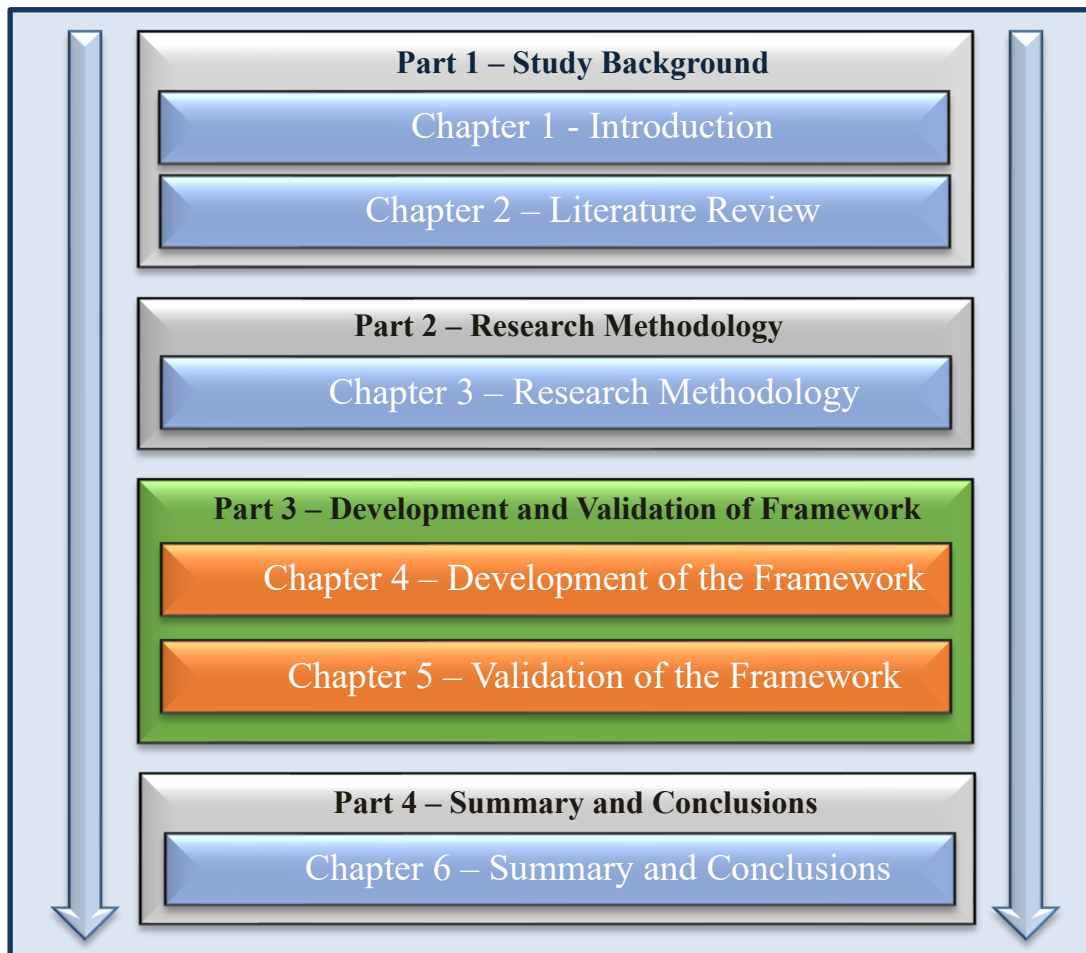


Figure 0.4 Map of the Thesis - Part 3

4 Development of the Framework

4.1 Overview

In this chapter the development of the developer driven framework for security and privacy of data in flow in the Internet of Medical Things (IoMT), henceforth referred to as the framework will be discussed. The aim of the framework is to assist SMEs in providing evidence of compliance with the GDPR data protection principles in their software systems or products. The framework is built on the preservation of security and privacy properties. These properties are violated by corresponding threats. Potential threats to software systems and products are risk assessed via threat modeling. The extracted prioritised threats are mitigated through the implementation of data flow security and privacy controls (DFSPCs). The DFSPCs were developed from international standards for security and privacy used for the medical domain. The processes of the framework are documented through a data protection impact assessment (DPIA) template. A DPIA is a GDPR requirement for any software system processing personal data.

4.2 Introduction

The framework was developed when the researcher was embedded in an SME, STATSports. The key reason for engaging with STATSports was to solve the problem on how to provide evidence of regulatory compliance and best practice for data security and privacy in their products. The task involved solving how the software developers could demonstrate compliance with the GDPR data protection requirements through security and privacy best practice. The solution would also need to comply with the STATSports ISO 27001 certification. The framework was developed in collaboration with STATSports and their software development team. The framework was defined and tailored in four iterative cycles over a period of 36 months through Action Research (AR). The cycle applied in this research is presented in Figure 4.1, on the next page. This section presents the cycles in the development of the different aspects of the framework and accompanying Excel document. STATSports and their software system is outlined in the following section.

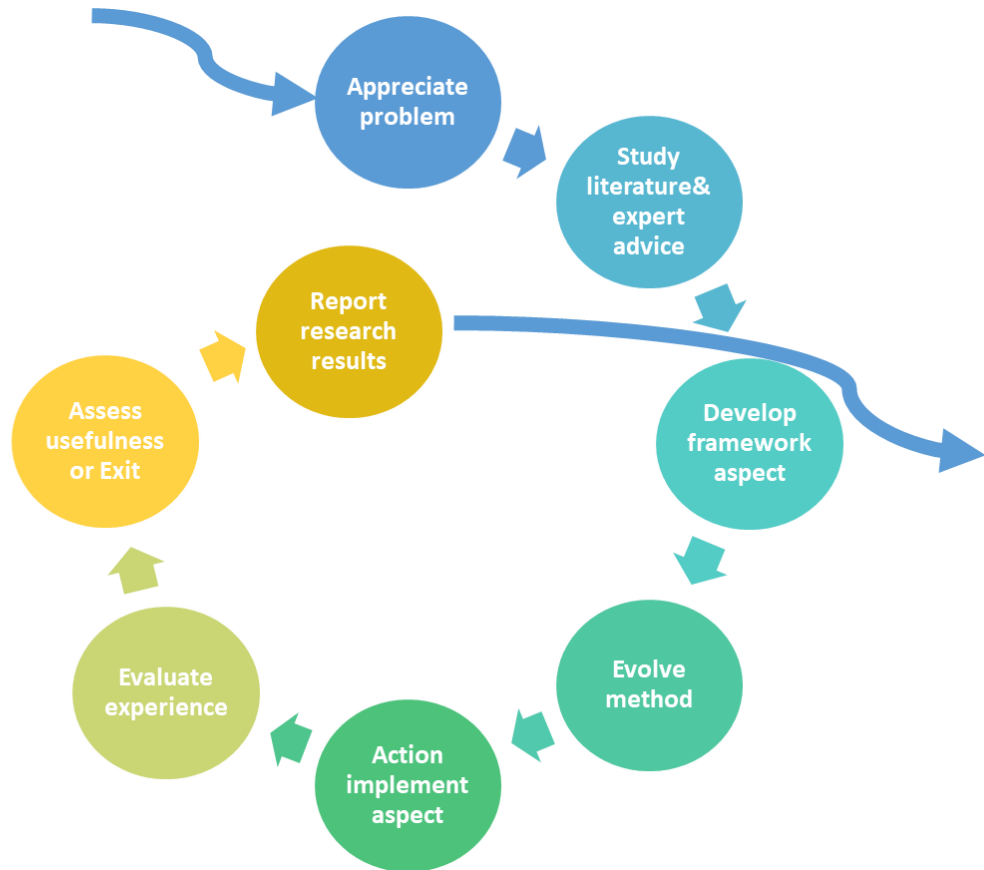


Figure 4.1 Outline of the cycles used to develop the framework

This section presents the four cycles used in the development of the framework:

1. **Cycle 1** – The problem was defined within the requirements of STATSports, through a literature review and with expert participation.
2. **Cycle 2** – The information gathered is used to develop the basis of the GDPR data protection principles, requirements for STATSports and the framework. This cycle provided the outline of the DPIA template, and the Privacy Policy used in the framework.
3. **Cycle 3** - The information gathered is used to develop the security and privacy properties to defend the GDPR data protection principles for security and privacy of data in flow in the IoMT. Threat modeling was established as a suitable risk assessment model for the framework.
4. **Cycle 4** - The information gathered is used to develop the data flow security and privacy controls (DFSPCs). The DFSPCs aim to assist in providing evidence for the development team of implementation of suitable security and privacy controls for data in flow in the IoMT.

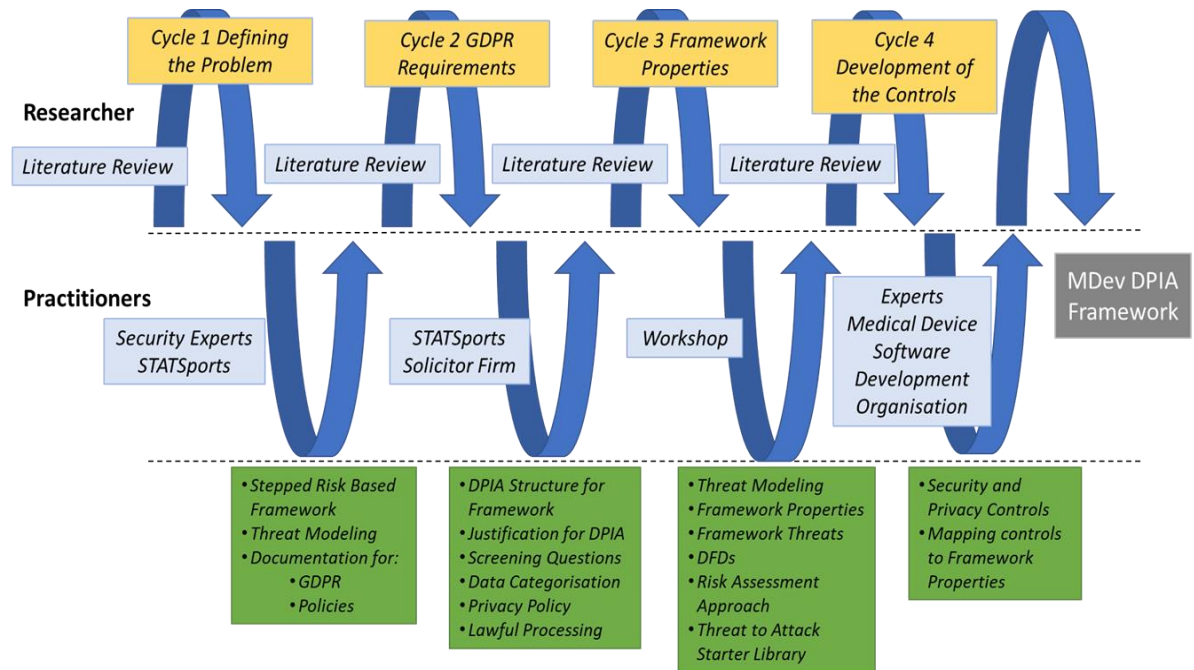


Figure 4.2 Evolution of the framework

Figure 4.2 above, presents an overview of the evolution of the framework through the four cycles of CAR. Each of the cycles were completed with the researcher and practitioners. The diagram outlines the practitioners involved at each cycle. The cycles were in development at the same. Figure 4.2 also presents the features contained within each cycle in the green boxes, to demonstrate the evolution of the framework development.

The outcome of the four research cycles is the background section and a framework containing six steps that make up the DPIA. Each step has individual attributes. The framework incorporated into a DPIA structure is presented in Figure 4.3 overleaf.

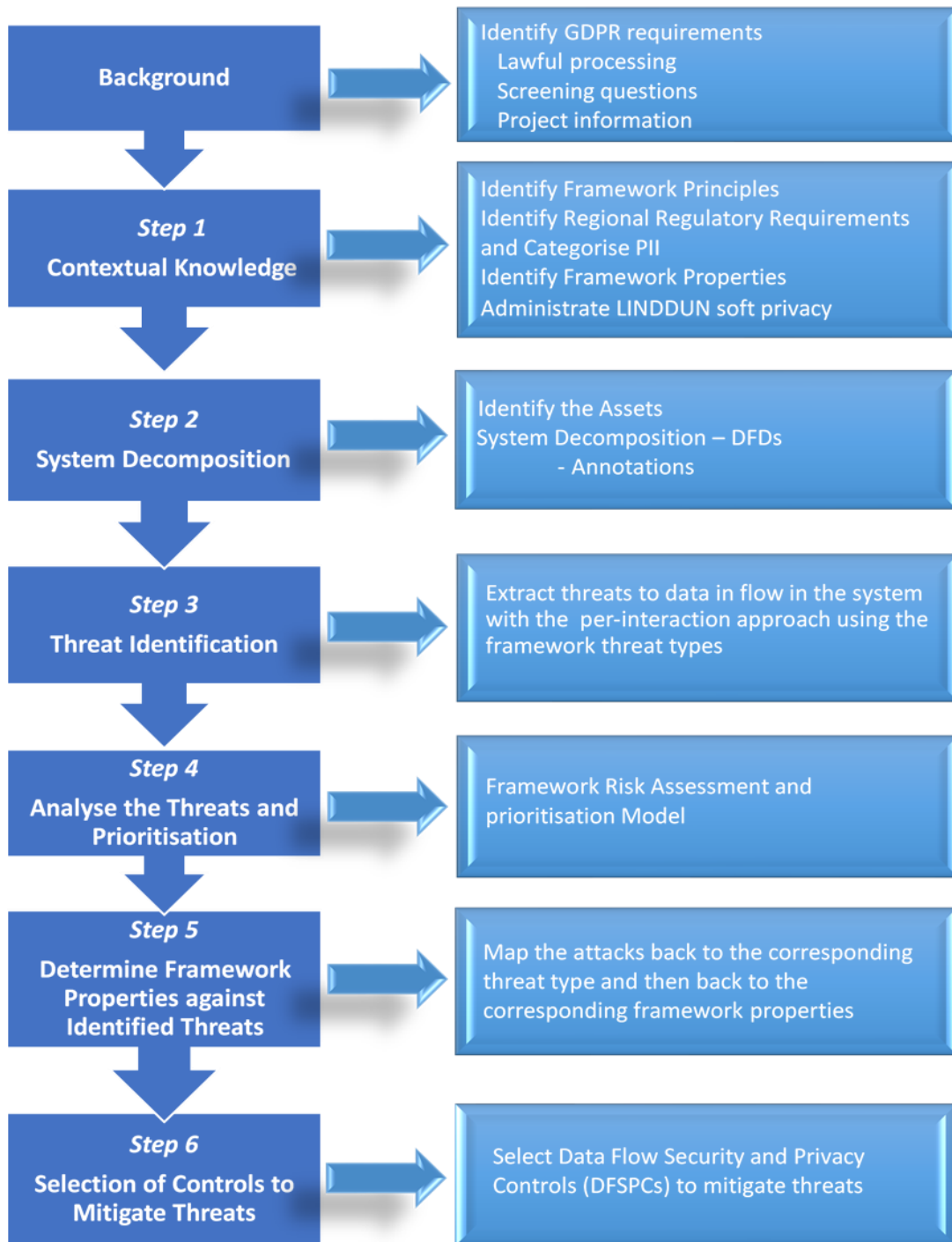


Figure 4.3 Background section and framework six steps that make up the DPIA

The next section of this introduction will provide a background for STATSports and their software system.

4.2.1 The SME and Background to the Software System

STATSports is an Irish SME employing approximately 132 people. STATSports initially contacted the RSRC to seek guidance and assistance around the requirements and implementation of data security and privacy within their products. This contact was prompted by requests from STATSports' customers. STATSports were entering the US market on a sports federation level and were involved with European sports at federation level. These organisations had requested the company demonstrate the processes and policies they had in place to assure data security and privacy in both their organisation and products. This was the first time the company had encountered data security and privacy evidence requirements from customers. STATSports were also aware of the GDPR and required assistance in ensuring the organisation and products complied with the regulatory requirements. STATSports products track performance and fitness to both elite professional athletes and the general public. The products consist of a combination of web, native app, and an external Bluetooth performance tracking device. The native app has the capability to pair with other external personal tracking devices. The STATSports software product collects and processes Key Performance Indicators (KPIs) from the external Bluetooth device. This data is processed and delivers a set of exact and unique performance session metrics for an individual to track their performance and fitness.

The roles between STATSports and the researcher within this research process were established over three meetings. These meetings provided an insight into STATSports' requirements and knowledge in the domain of data security and privacy plus agreement on the researcher's role within the organisation. The first two meetings included the director of the RSRC, the author and several STATSports employees i.e., the Chief Technical Officer (CTO), software architect and a senior developer. The STATSports CTO had been working with the company for over five years. The software architect was newly promoted from the position of senior developer, and had five years' development experience, four within the organisation. The senior developer had four years' development experience within STATSports.

These meetings established that:

- STATSports had limited knowledge, experience and understanding of data security and privacy regulatory or best practice requirements;
- The development team had limited experience in implementing data security and privacy in the software development process. All current software products had not implemented any security or privacy controls.

The third meeting was an exchange of information between the researcher, the director of the RSRC, and several STATSports staff i.e., the CTO, head of software development, the executive management team, including one of the company's owners. I presented a high-level introduction to the GDPR regulations, how these mapped to STATSports customers' requirements, existing cybersecurity frameworks and standards discussed in the literature review. Some of the standards presented included ISO/IEC 27001/27002, ISO 15408, ISO 64334, IEC/TR 80001-2-8 and NIST SP 800-53r4. The final meeting led to the researcher joining the organisation. A key objective being that the researcher will develop a framework for the software development team. The framework will assist the software development team implement data security and privacy measures to protect user data. This will assist STATSports in the provision of evidence for compliance with GDPR data protection and customer requirements. The agreement included:

- The researcher would assist STATSports in meeting GDPR compliance throughout;
 - The organisation to include policy documents, some of which evolved from the research;
 - Software development and post-release within their products.
- The research would be completed with the STATSports software development team;
- The research approach will be an iterative process involving close collaboration with the software team;
- STATSports agreed to apply the framework within the development process of their cloud-based product;
- The specific learning of the research will be communicated through international conferences, journal publications and presentations in other academic and related settings.

4.3 Cycle 1 – Defining the problem

Cycle 1 identified the problem for STATSports and established how the research would begin to address the problem. The CAR cycle was outlined previously in section 3.6.2; problem identification, data collection and analysis, action planning and taking and reflection and evaluation on the action. Figure 4.4 presents a high-level summary of each phase in cycle 1 of the CAR approach completed in this part of the research.

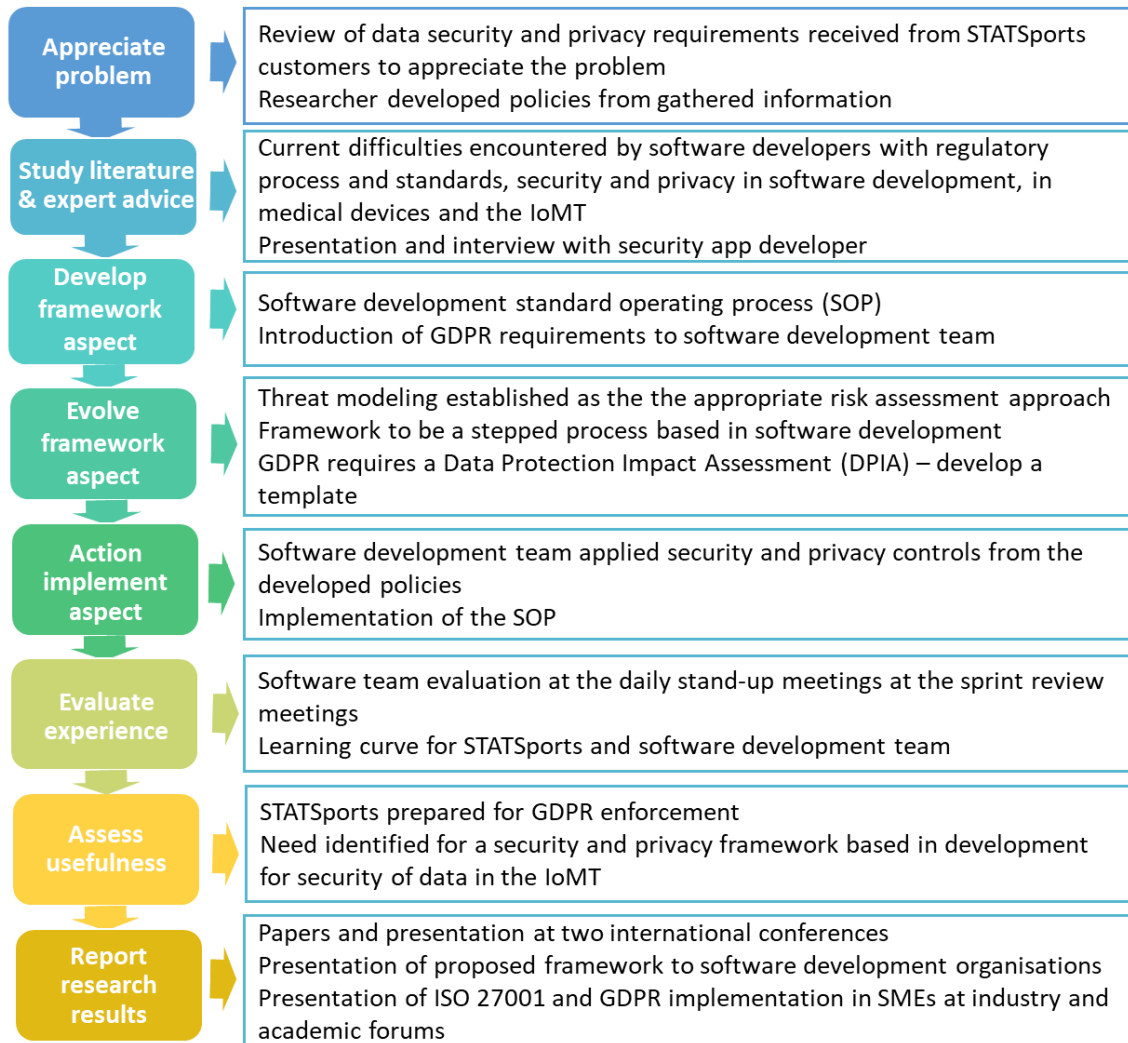


Figure 4.4 Cycle 1 summary

4.3.1 Appreciate the Problem

Figure 4.5 outlines what is discussed in this section.

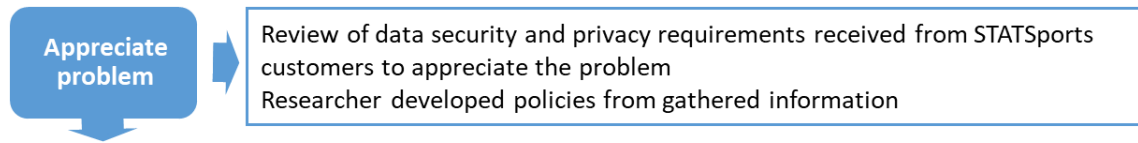


Figure 4.5 Cycle 1 appreciate the problem outline

As discussed, this research began with an approach by STATSports. The researcher followed up with a number of data collection practices. This was done to appreciate the problem for STATSports and software developers in meeting data security and privacy best practice and regulatory compliance. These data collection techniques included:

- Review of data security and privacy requirements received from STATSports customers;
- Traditional literature review;
- Presentation and interview with security app developer, discussed in section 4.3.2.1.

The data showed that software development teams face a variety of challenges with implementing data security and privacy into the software development lifecycle (SDLC). The researcher examined the STATSports customers' requirements and the literature on GDPR requirements. The information gathered was used to create a list of 18 policies, presented in Table 4.1, overleaf. The researcher prioritised and wrote these policies in collaboration with STATSports senior management and the software development team. The prioritisation of the policies was influenced by the STATSports' clients and the GDPR coming into force. The clients' priorities included understanding how the organisation would be implementing its policies and procedures to meet the GDPR requirements. They also required corroboration in relation to the data being processed, how access would be controlled, how changes in the system would be controlled to meet the GDPR requirements and the policies STATSports had in place in the case of a data breach and how the breach would be handled and the impact it could have on the data, client organisation and STATSports. The researcher collaborated with the software development team to address the gaps in the software products to meet the client's immediate needs.

Table 4.1 STATSports' customer and GDPR requirements triggered policies

Policy Name	Description	Priority
Policy Management Policy	Outlines how the organisation will manage the policies	1
System Access Policy	Processes and controls for access to STATSports systems	2
Roles Policy	Defines who is responsible for the security and privacy within the organisation	3
Configuration Management Policy	Establishes procedures for identifying configuration items throughout the STATSports systems and SDLC	4
Data Integrity Policy	Requirements applied to data (both paper and electronic) throughout the organisation and their products life cycle	5
Disaster Recovery Policy	Tools and procedures to enable the recovery or continuation of technology infrastructure and systems following a natural or a human induced disaster	6
Data Management Policy	Focuses on the management and governance of data assets throughout the organisation and in their products	7
Employees Policy	Describes how all employees are expected to conduct themselves, including duties for data security and privacy	7
Breach Policy	Provide a process to report suspected data thefts, data breaches or exposures (including unauthorised access, use, or disclosure) and to outline the response based on the type of data involved.	8
Vulnerability Scanning Policy	Establish the procedures for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in STATSports and their products	9
Third Party Policy	Process of analysing and controlling risks associated with outsourcing to third-party vendors or service providers for the STATSports systems and their products	10
Facility Access Policy	Procedures to limit physical access to STATSports electronic information systems and the facility or facilities in which they are housed	11
Incident Response Policy	Defines the responsibilities of each member of STATSports computer security incident response team	12
Risk Management Policy	Instructions that define STATSports approach and stance on risks, risk assessment and risk management for the whole organisation and in software development	13
Disposable Media Policy	Procedures on proper use and disposal of media on for example USB/external storage, phones	14
Data Retention Policy	How long and keeping track of information, how to dispose of the information when it's no longer needed and outlines the purpose for processing personal data	15
Auditing Policy	The framework within which internal audit will be completed and provides objective and independent confidence that the policies and process and procedures are being implemented and work within STATSports	16
Intrusion Detection Security Policy	Outlines the monitoring, logging and retention of network packets that traverse STATSports networks, observation of events to identify problems, document existing threats and evaluate/prevent attacks	17
Approved Tools Policy	List of approved software tools for internal use by STATSports workforce	18

The policies affected data security and privacy implementation within the development process and the software. Examples include:

- The risk management and data integrity policies required a documented software development process that included focus on data security and privacy risk assessment;
- The system access policy determined the requirements for access to systems including a minimum password requirement;
- The breach and incident response policies outlined the processes in response to data being accessed by unauthorised persons;
- The data integrity policy outlined the transmission protocols and minimum cryptography in software development.

4.3.2 Study Literature and Expert Advice

Figure 4.6 outlines what is discussed in this section.

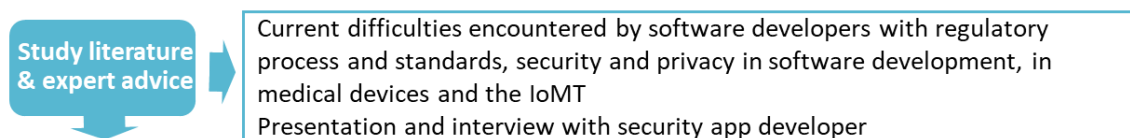


Figure 4.6 Cycle 1 literature studied and expert advice

The author explored the current difficulties encountered in the fields of data security and privacy, medical device regulatory and standards knowledge and understanding in the software development domain. The review uncovered many difficulties encountered by software development teams when implementing data security and privacy for data in flow. These difficulties reflected the same hurdles encountered by STATSports. In summary the difficulties included:

- Current regulatory process and standards entail many overlapping considerations that developers and organisations need to consider with regard to security and privacy. There are no one set of data security and privacy standards and processes for developers. This results in a lack of understanding and direction and confusion for developers and organisations. Implementing and providing evidence of regulatory compliant requirements, is a struggle for developers in SMEs due to lack of knowledge, experience, understanding and concise guidance (Wagner et al. 2020);

- In the IoMT sensitive personal and health data can flow through a diversity of apps, systems, devices and technologies, public and open networks. This exposes data in the IoMT to additional attack surfaces, which requires the hardening of these surfaces (Brien et al. 2018; Papageorgiou et al. 2018; Gebremichael et al. 2020);
- Data security and privacy in software development is an evolving field. Software developers have little knowledge and experience in data security and privacy risk assessment. They also have little knowledge of standards and best practice controls to provide evidence of mitigation of threats (Acar et al. 2017; Wagner et al. 2020);
- Currently software development in the medical device domain does not have a framework to addresses both security and privacy risk assessment and to implement appropriate controls to assist in providing evidence for regulatory and best practice compliance. There is an absence of an approach that considers the combined impact of security and privacy risks on human health within the medical device standards and their mitigation (Yaqoob et al. 2020).

4.3.2.1 App Security Experts

Guidance to understand the problem and provide feedback was obtained from app security experts from the financial and health domains in two meetings. Expert A has over 20 years' experience in secure software development in the financial and health domains. They are an accomplished security professional delivering a broad range of information security services to the private and public sectors. They have extensive experience in the delivery of penetration testing and both manual and automated static/dynamic application security testing. They are a key influencer in the development of security strategies, policies and guidelines and an advocate of Secure Software Development Lifecycle (SSDL) practices. They are currently a software security research engineer at a new start-up company. Expert B has 25 years in software engineering. They have five years in security software development in the financial domain and three years' experience in software engineering in medical devices. They have held positions in cyber security risk management with strong experience in banking and healthcare sectors. As a software engineer in the medical device industry, they developed software for critical medical devices, working to ensure compliance with medical safety and security standards. Expert B now works as a senior cybersecurity engineer with a medical device

company. Both experts have years specialising in secure application design, development and testing with full lifecycle security and development experience in major IT projects.

The initial meeting was fact finding and commenced with a presentation by the author on the findings from the literature review and STATSports. It included an overview of the concepts for inclusion in the research. It presented the state of the art in regulations, medical device standards, security development, data transmission and security controls. It provided an outline of risk management and threat modeling as aspects for inclusion in the framework. The presentation was used to facilitate a discussion with the experts around the development of the framework to garner their expertise. This presentation is provided in Appendix C. An informal discussion followed on the research concept and the potential benefits the framework could provide for developers. The experts confirmed the gap in the lack of knowledge and understanding in security and privacy in software development. The experts supported the literature findings and agreed there is a lack of knowledge from within the software development domain on how to assess and implement security and privacy controls. They stated this is attributed to some extent to aspects such as:

- Lack of developer training, experience and understanding of data security and privacy requirements. The deficiency of data security and privacy education and training provided from the educational institutes for developers was expressed by the experts;
- The fragmented standards and lack of knowledge, training, and enforcement of their requirements;
- There were no comparable frameworks to the Payment Card Industry Data Security Standard (PCI DSS) standards to assist developers to select appropriate security controls to secure data in flow for the software or medical development domains. The PCI DSS provides a baseline of technical and operational requirements designed to protect account data for cardholders (PCI Security Standards Council 2018);
- That data security and privacy within development generally is a subject stumbled into by developers. They maintained there is a growing community in development security and privacy, driven in part with the rise in ransomware but also, due to the demand from industries that previously did not have to consider security and privacy;

- The introduction of new legislation and the bad publicity associated with data breaches has pushed security and privacy into the main frame. They discussed the “push left” model promoted by security professionals. The idea that security should be pushed to the very beginning of the development process, that is to the left of the development lifecycle. Security traditionally has been a matter addressed at the end of development, a “bolt on”. Both experts agreed that research and experience is now presenting that this “bolt on” security leads to vulnerabilities in code and added expense as fixing these vulnerabilities retrospectively is costly. Both also agreed smaller development organisations struggled to apply data security and privacy. These organisations look to “bolt on” often as they look to outside to fix security and privacy on completion of the development, an extra cost.

The experts were presented a rough outline of a potential framework. They agreed that a framework could improve current practice in the domain as there is limited understanding of the necessity of data security and privacy for the lifecycle of the data, i.e., data in flow. They encouraged a stepped straight forward and concise framework would be the ideal solution. They referenced the overwhelming 180 individual PCI requirements in 12 categories, written in the language of sophisticated information security technology. They were interested in the idea to provide support for regulatory driven development for developers within what they perceive as the data lifecycle. The discussion also considered storage of data within the data lifecycle as this is one of the key PCI DSS requirements. However, it was decided that this was outside the scope of this research due to the time and resource constraints of PhD research.

The need for risk management for data security and privacy was determined as a key component in demonstrating regulatory compliance for medical devices. The risk management standards ISO/IEC 27005 (ISO/IEC 2018a), ISO 14971 (ISO 2012), AAMI TIR57 (AAMI 2016) and NIST SP 800-30 (NIST 2012) from the literature review were discussed as potential models for risk assessment. The experts expressed that the structure and most of the guidance in ISO 14971 and AAMI TIR 57 is high level but is well structured and outlines a good process for risk management based in NIST SP 800-30. Both experts noted that TM is a common software development practice to identify and prioritise potential threats and mitigations to protect confidential data. The experts stated that TM would be a specialised level of expertise within the app security community. The researcher included TM in the ongoing development of the framework. The experts

stressed the lack of security and privacy controls to address network/wireless, secure development, and layered access security in the early framework. The absence of logging and monitoring security controls was also stressed. Both experts reflected the standards mapped to build IEC/TR 80001-2-8 would provide adequate security and privacy controls. On conclusion of the meetings, the author had included for further investigation for the framework:

- Threat modeling and its application to security and privacy and the risk assessment standards in the literature review for the framework;
- Of the standards mapped for the development of IEC/TR 80001-2-8 standard for potential security and privacy controls for data flow. The experts agreed to another meeting to validate the controls extracted for the framework when the researcher had completed this body of work;
- A stepped process for documenting the framework.

4.3.3 Develop the Framework

Figure 4.7 presents an outline on development of the framework aspect in cycle 1.

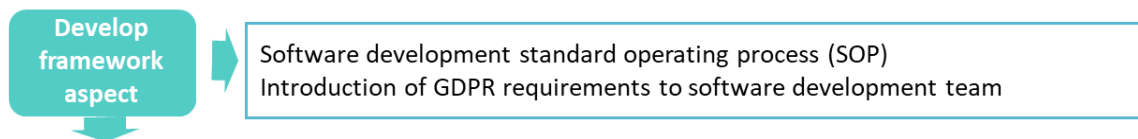


Figure 4.7 Cycle 1 outline on development of the framework aspect

The STATSports chief scientist and development team developed a software development standard operating process (hence forth known as the SOP), with input from the researcher. Creation of this SOP assisted the researcher and the software team to introduce formal practices into the development process. The SOP defines the key aspects involved in the software development and maintenance lifecycles. The document outlines the tools and processes that are followed throughout the development, testing and validation lifecycle. The software development processes in the SOP that are followed are based upon IEC 62304. These include:

- Software development planning - the software development process uses the agile Scrum methodology in a two-week sprint cycle. User stories, issues, and bugs are logged in Jira and assigned a unique ID for traceability. The team works together to define goals at the start of each sprint and holds daily stand-up meetings to review progress and address any blocking issues. Completed features are demonstrated for review and feedback at the end of each sprint. The software

development lifecycle follows a hybrid V-model with agile practices integrated into the traditional V-model, including risk and requirements management, project and configuration management, traceability, and testing.

- Software requirements analysis - the process of software requirements analysis, is completed by the product owner. They define high-level user requirements and the software architect defines associated software requirements, including functional, interface, security, usability, and database requirements, among others. The requirements are assessed for risk and checked for consistency, clarity, testability, and traceability. User acceptance criteria and system acceptance test cases are defined and linked to each requirement in Confluence and TestRail. The product owner signs off the requirements before creating Jira tasks for implementation, and the team uses Confluence to document and manage requirements, including user stories, preconditions, acceptance criteria, test cases, user interaction and design, and notes.
- Software Architectural design and Software detailed design – the detailed design process, is where the software architect transforms requirements into a documented architecture, verified by the product owner/developer. Associated Jira tasks are created for each requirement. QA defines software integration test cases to ensure no negative impacts on code integration. The implementation Jira tasks are placed into the Ready Backlog after verification, and are selected for a two-week sprint by the development team. Testing tasks involve writing and running test cases in stages including code review and QA, with the feature only released once all test cases have been passed. Requirements, design and test case IDs are linked and updated by the developer, with change requests handled by the change request process.
- Software Unit implementation and verification - developers implement code for Jira development tasks during the sprint, and then create and run unit test cases to verify the functionality correctness for each software unit. The unit tests should check various aspects such as programming procedures, fault handling, initialization of variables, memory management, and boundary conditions. The developer will perform the software unit verification and document the results. All code is checked in against a Jira task for traceability, and the architect reviews any documentation updates.

Chapter 4 Development of the Framework

- Software integration and integration testing/Software System testing - Developers integrate software units into the development branch after code inspection by the software architect or team lead. The deployment/continuous integration process includes several steps, such as running all unit tests, completing static analysis, deploying to local test servers, and conducting regression testing. QA executes integration software test cases defined in TestRail and documents the results, including any anomalies. When software integration failures occur, QA raises a bug in Jira. The section also covers software system testing, including establishing tests for software requirements, retesting after bugs have been fixed, and verifying that test results meet required criteria. QA documents the results of running acceptance/system test cases and produces an acceptance test record.
- Software release - the procedures for managing the release of software products at STATSports is outlined in the STATSports Software Change and Release Management SOP. This SOP covers specific software applications, including their release cycle and defines key terms. The SOP outlines responsibilities and procedures for change requests, sprint planning, testing, and release, including specific steps for each type of software application. The text emphasises the importance of following defined processes and seeking approval from specific stakeholders before moving to production.

The additional practices included application of security and privacy risk assessment and controls into the STATSports software development process. The SOP implementation set the groundwork for the integration of the framework into the software development process. It introduced the requirements for GDPR and the STATSports elite customers' organisations into the development process. It provided understanding and education on the requirements for data security and privacy for the software development team. It also introduced appreciation for regulatory compliancy and best practice for data security and privacy in the development process.

4.3.4 Evolve the Framework

Figure 4.8 outlines how the framework evolved in cycle 1.

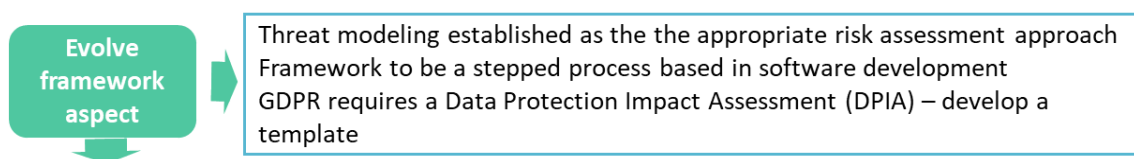


Figure 4.8 Cycle 1 evolve the framework outline

Chapter 4 Development of the Framework

The researcher evolved the framework from learnings in this cycle to include investigation of:

- A software development risk-based approach presented by the data gathered from the security experts. This required investigation of TM applicable to security and privacy in software development. The risk assessment method investigation would include consideration of frameworks from standards in the security, privacy, generic software development and medical domains;
- Create a stepped process in the framework to employ data security and privacy TM and risk assessment;
- Investigate how to apply appropriate controls to mitigate extracted and prioritised risks;
- Support documentation of the framework to fulfil GDPR DPIA requirements;
- Development of the policy documents outlined in section 4.3.1 and development of processes for data security and privacy to address STATSports customer requirement prompted the organisation to move forward to expand current processes and procedures to achieve ISO 27001 certification.

4.3.5 Action

Figure 4.9 presents the actions taken in cycle 1, discussed in this section.

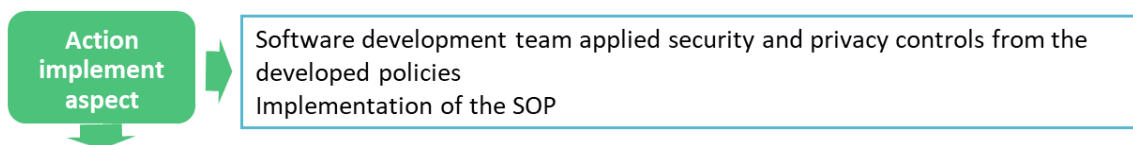


Figure 4.9 Cycle 1 action outline

The software development team implemented the data security and privacy controls from the developed policies. Some of the security controls included bringing the password requirements for their products in line with the system access policy requirements and applying encryption to stored PII and PII in transmission. The SOP was implemented into the software development process, which included security controls applied to code review and separation of production, development, and testing systems. The SOP formalised the SDLC and agile processes of software development. The SOP established data security and privacy consideration in all parts of the development process. This was a steep learning curve for the software development team that required broad cooperation between the author and the team. The development of the system was completed over 20

months, there were 11 Sprint planning meetings and associated retrospectives. Difficulties in relation to completion of security and privacy were discussed at the retrospective meetings. The difficulties experienced by the developers were in relation to navigating the framework and on occasions understanding some tasks of the framework. An example would be the application of the annotations to the DFDs and disguising between security and privacy. The researcher clarified that both aspects would need to be addressed but with the understanding that privacy could not be side-lined. The researcher expanded the 19 policies in Table 4.1 to 27 to fulfil the needs for STATSports ISO 27001 certification. The STATSports ISMS was developed and managed by the researcher. STATSports achieved ISO 27001 certification eleven months after completing GDPR conformity.

4.3.6 Evaluate Experience

Figure 4.10 summarises the evaluation of the processes developed in cycle 1 discussed in this section.

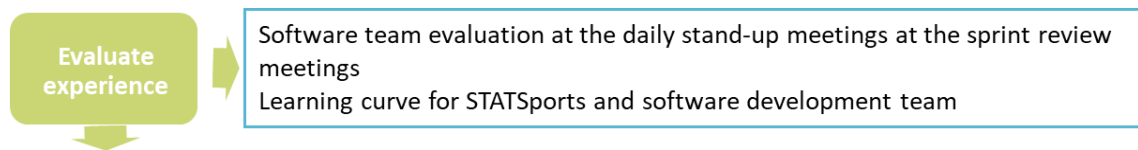


Figure 4.10 Cycle 1 evaluate experience summary outline

The software team got the opportunity to evaluate the process at the daily stand-up meetings and to a greater level at the sprint review meetings. The author considered the steep learning curve required to get the SOP procedures and processes in place. The introduction of the formalisation of the agile development process and controls from the developed policies, was a considerable task. There was a significant shift required from within the development team but also throughout the organisation. An example being the development team and process was inclined to be altered abruptly at the behest of management, owners, and account managers. This generally meant the development process, which included data security and privacy considerations, were circumvented. This underlined the need for the framework to be a stepped concise approach rooted in the software development process.

The STATSports ISMS received ISO 27001 certification. This validated the procedures and processes implemented from the policies through an external third-party auditor. This included the SOP and processes implemented for software development.

4.3.7 Assess Usefulness

Figure 4.11 presents an overview of the assessed usefulness of the research from cycle 1.

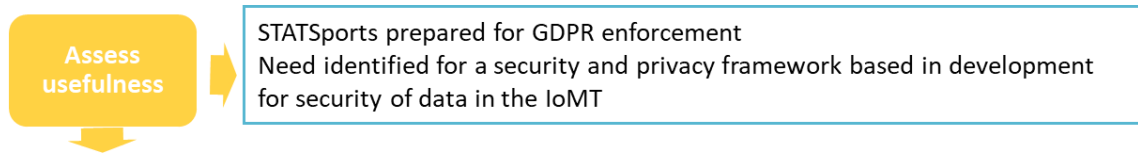


Figure 4.11 Cycle 1 summary usefulness assessment

The outputs from cycle 1 included:

- An understanding of the data security and privacy requirements for STATSports software from the GDPR and their customers;
- Prompted the development of organisational wide policies for data security and privacy and the decision to work toward and achieve ISO 27001 certification;
- A wider understanding of the domain of data security and privacy in software development and in the medical domain. The field of data security in software development has many publications and is thoroughly researched by previous researchers. The field of data privacy in software development is comparatively new and have less publications and examination by previous researchers. Privacy has increased in importance in software development due to regulation, such as the GDPR. Research conducted to date has been either specific to security or privacy in software development. Most of the current research around security or privacy in software development is completed in the generic software, medical device and IoT development domains. However, research is emerging in the past three years on considering both data security and privacy in software development in the medical software and IoMT domains;
- Risk assessment for data security in development is an established field. Threat modeling methods offer the ability to accommodate risk assessment requirements in software development for apps and the IoT. For this reason, it would be prudent that the researcher would include TM practices in the framework;
- Inclusion of TM in the framework could provide evidence of data security and privacy risk assessment. This could assist in compliance with GDPR and customer requirements for STATSports.

4.3.8 Report Research Results

Figure 4.12 provides a summary of the reporting of the research results from cycle 1.

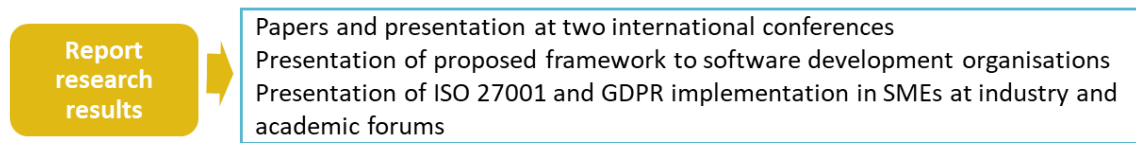


Figure 4.12 Cycle 1 report research results summary

Cycle 1 facilitated papers and corresponding presentations at two international conferences.

1. Treacy, C., McCaffery, F. and Finnegan, A. (2015). Mobile Health & Medical Apps: Possible Impediments to Healthcare Adoption. In: eTELEMED, The Seventh International Conference on eHealth, Telemedicine, and Social Medicine. Lisbon, Portugal: IARIA, 2015, pp.8–11.
2. Treacy, C. and McCaffery, F. (2016). Medical Mobile Apps Data Security Overview. In: SOFTENG: The Second International Conference on Advances and Trends in Software Engineering. Lisbon, Portugal, pp.123–128.

The SOFTENG conference led to an invite to extend the conference paper for publication in an international journal. Treacy, C. and McCaffery, F. (2016). Data Security Overview for Medical Mobile Apps Assuring. International Journal on Advances in Security, 9(3 & 4), pp.146–157. The researcher also presented the research concept at the HIS 2017 High Intensity Software Conference, Safety and Security Processes for Medical Device Software (McCaffery and Treacy 2017) and to the Managing Director and Head of Software Security Testing with Expleo in Ireland in 2017. The researcher presented the implementation in a SME of GDPR requirements, an ISMS and attaining ISO 27001 certification to an Irish based SME in the IoMT, Salaso.

The author presented the framework model at this juncture to the STATSports development team, management, and owners. The agreement at this point was the framework would be:

- Based on the GDPR protection principles and documentation would align with GDPR DPIA;
- Be a stepped process;
- The framework documentation would follow the risk assessment process employed in ISO 14971 and AAMI TIR 57;

Chapter 4 Development of the Framework

- Threat modeling would be applied for risk assessment of security and privacy within the risk assessment process;
- The author would provide a set of controls for both security and privacy that could be applied by the developers to assist in showing compliance with best practice and standards requirements.

The immediate priority for STATSports was GDPR compliance and included the development of a DPIA and Privacy Policy. It was decided these would be the next step of the framework development.

4.4 Cycle 2 – GDPR Requirements

Cycle 2 identified the immediate GDPR requirements for STATSports and established how these would confront the problem and apply to the framework. Cycle 2 was completed in parallel to cycle 3. Figure 4.13 presents a summary of cycle 2, which will be discussed next.

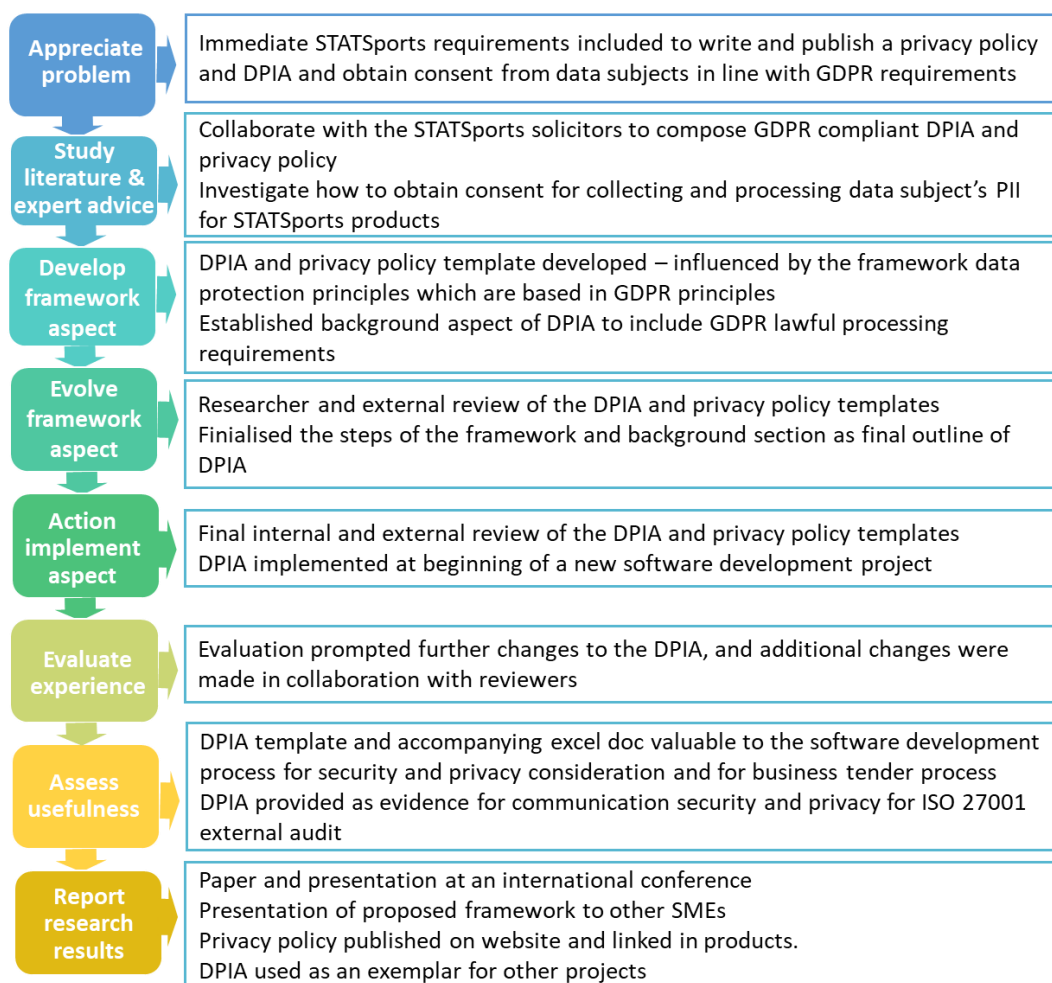


Figure 4.13 Cycle 2 summary

4.4.1 Appreciate the Problem

Figure 4.14 outlines what is discussed to appreciate the STATSports problem in cycle 2.

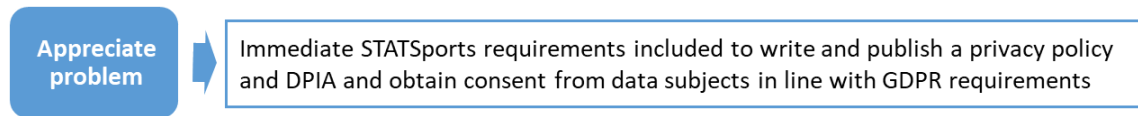


Figure 4.14 Cycle 2 appreciate the problem outline

Information was gathered about GDPR data protection principles, privacy policy, and DPIA requirements. The researcher investigated how these applied to STATSports and could help to solve the research problem. The researcher found three immediate requirements for STATSports, in order to comply with GDPR. The organisation did not have a privacy policy drafted or published for users or employees. STATSports had not obtained appropriate consent to collect and process PII in their products in line with GDPR requirements. Part of obtaining consent is also linked to the privacy policy. The organisation had not prepared a DPIA for any of their products. STATSports had no awareness and experience in delivering these tasks. The researcher collaborated with STATSport's solicitor firm in developing the requirements. The solicitor firm were relatively inexperienced in implementation of these requirements in real time since the GDPR was a new regulation. The firm had a draft DPIA and privacy policy that they shared with the researcher. The draft DPIA and privacy policy documents were developed from the legal requirements of the GDPR by the firm's GDPR specialist. The researcher collaborated with the specialist via online meetings and email, to develop the DPIA and the privacy policy specific to STATSports and their product. Changes made to the draft documents provided by the solicitor firm were sent to the GDPR specialist. Any changes made by the researcher were assessed by the GDPR specialist to ensure the DPIA and privacy policy complied to the regulatory legal requirements of the GDPR. The solicitor firm's role was to ensure the DPIA and privacy policy met the regulatory legal requirements of the GDPR.

4.4.2 Study the Literature & Expert Advice

Figure 4.15 provides an outline of the literature studied and expert advice applied for cycle 2.

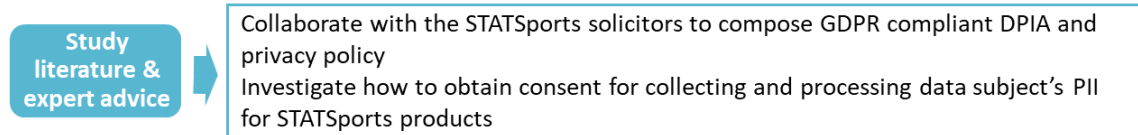


Figure 4.15 Cycle 2 literature study and expert advice outline

The researcher examined the GDPR regulation, publications from the Article 29 Data Protection Working Party and from the Irish and British information commissioners, on the requirements of a privacy policy and DPIA. There was limited research completed in these areas in the academic literature because the regulation was new.

The researcher found that the following were required to be GDPR compliant:

- DPIA;
- Privacy policy;
- Procurement of consent for collecting and processing of PII.

The data gathered also included GDPR guidelines on the security and privacy requirements for PII data collected and processed. The author collaborated with STATSports' solicitor firm in drafting the privacy policy and DPIA. The solicitors provided high level legal guides for a privacy policy and DPIA, written in legal vernacular that mirrored the language of the regulation itself. Any changes made to the DPIA and privacy policy were assessed by the solicitor firm to ensure they met the regulatory legal requirements of the GDPR.

4.4.3 Develop Framework Aspect

Figure 4.16 provides an overview of the developed aspect of the framework in cycle 2.

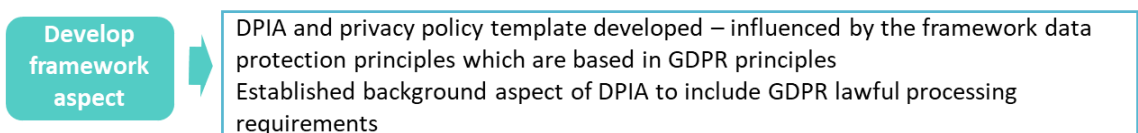


Figure 4.16 Outline on aspect of the framework development in cycle 2

The privacy policy was drafted from the high-level legal template provided by STATSports' solicitors. The researcher refined the language to meet the plain language requirements of the GDPR. The substance of the privacy policy was established from the

information gathered from the regulation, UK and Irish information commissioners' guidance on requirements for a privacy policy. The software development team collaborated to provide information on the PII types, and summary of the processing and storage of PII for the policy.

The DPIA was drafted from a high-level legal template provided by STATSports' solicitors. This template provided guidance on what the DPIA should contain, what PII should be addressed and the legal wording around PII and the GDPR. This DPIA template was a very high-level description of the privacy requirements around the processing of PII for the STATSports consumer product. The researcher investigated the required content of a DPIA and established the legal template did not provide guidance on:

- How to interpret the requirements of the GDPR articles to real world settings and apply these to software development;
- How to demonstrate data security and privacy compliance within the GDPR data protection principles;
- Risk assessment processes for data security and privacy and how to document or present this in a DPIA to provide evidence of compliance;
- What to provide as evidence that the data protection principles have been met.

The researcher included guidance on these points in the DPIA template and divided the processes involved into the steps of the framework. This was completed to provide an effective way to assess and demonstrate a software project's compliance with the GDPR data protection principles and obligations (ICO 2020). The stepped process was designed to describe the processing, assess the necessity and proportionality of the processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing them and determining the measures to address them (Article 29 Data Protection Working Party 2017). The DPIA framework encompassed the two parts of Article 5 of the GDPR. Article 5(1) outlines six principles in relation to the processing of personal data. Article 5(2) pertains to accountability and defines the data controller as responsible for complying with the principles. These were incorporated into the framework data protection principles. These data protection principles are the foundation for the DPIA and what the framework was developed to help in providing compliance with.

The researcher added a background part to the draft DPIA. This was to provide support to developers in establishing the lawful processing and explanation on DPIA

requirements of the regulation. The lawful processing was based on questions formed to interpret GDPR articles 5, 6, 8, 12, 13, 15, 44 and 45. These questions assisted STATSports to:

- Assess the minimum amount of data required to fulfil the purpose of the product;
- Where, when, and how the process of obtaining consent for the collection, processing, and storage of the PII was completed.

The researcher drafted the wording of the consent to align with the GDPR plain language requirement. The development team inserted a feature in the products to obtain GDPR compliant consent. The screening questions were developed to provide explanation on why a DPIA is required. These screening questions were prompted by the software development team. They needed help to interpret the requirements of the GDPR articles to real world settings. The screening questions were developed using the international standard ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework (ISO/IEC 2018b) and the data protection principles of the GDPR. The screening questions translated the GDPR data protection principles and requirements to a language understandable for the STATSports' software development team.

4.4.4 Evolve the Framework

Figure 4.17 provides an outline of the progress in the framework development during cycle 2.

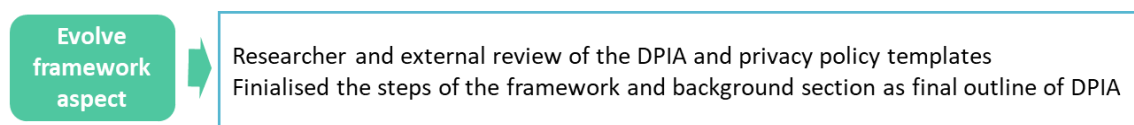


Figure 4.17 Cycle 2 progress in the framework development outline

The initial drafts of both the DPIA and the privacy policy were reviewed by the STATSports' solicitors to ensure they were legally compliant with the GDPR. The author discussed with the solicitors what their template DPIA lacked to comply with the GDPR risk assessment requirement. There were also gaps on demonstration of the flow of the PII through the system and a risk assessment of the security and privacy of the PII and controls implemented to mitigate any potential threats. The framework's risk assessment is discussed in cycle 3 and controls for mitigation are discussed in cycle 4. The solicitors did not provide any objection to the use of TM as a risk assessment method, or controls for mitigation of threats. However, it must be noted there was a lack of expertise from

Chapter 4 Development of the Framework

the solicitors on risk assessment and mitigation controls for data security and privacy. The solicitors simply followed the legal interpretation. The firm was interested in obtaining the draft DPIA to understand the process and potentially share with other clients. The solicitors advised three additions to the privacy policy:

1. The inclusion of the contact details for the Data Protection Representative (DPR);
2. Addition of the location of the data centres used for storage;
3. The inclusion of a live link to the privacy policy.

The privacy policy was validated by the solicitor firm and published on the STATSports website. A link to the privacy policy was provided for users through the STATSports products. The privacy policy became a part of the STATSports ISMS and was published for employees within the organisation. This was the template encompassed into step 1 of the framework.

The initial DPIA draft was amended to include the stepped procedures and processes of the framework. The final DPIA template would include a backdrop section and the six steps of the framework. Added to the background section of the DPIA was an outline on what data protection principles and framework properties are. The development of the framework's properties is discussed in cycle 3. Also added was a part on regional regulatory requirements if the project would process PII outside the EU. The administration of two soft privacy properties, content awareness and policy and consent compliance and management of their LINDDUN threat categories Unawareness and Non-compliance respectively were included in step 1 of the framework. These soft properties and corresponding threats were linked to step 1 of the framework through the:

- GDPR data protection principles requirements through the screening and lawful processing questions and the privacy policy;
- Where, when and how to obtain consent, which was agreed before development and monitored throughout;
- STATSports organisational policies in the software development SOP.

4.4.5 Action

Figure 4.18 outlines the actions taken in cycle 2, discussed in this section.

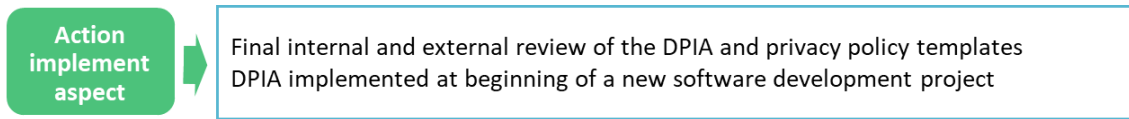


Figure 4.18 Cycle 2 action outline

The DPIA draft went through an internal review within the RSRC. The two research supervisors conducted this review. Another internal reviewer included a member of the RSRC working as a project manager in a cybersecurity in medical networks SME. The project manager implemented and managed the SME's ISMS and regulatory requirements under the GDPR. The internal review was conducted individually on a completed draft of the DPIA. Each reviewer returned the DPIA with comments and corrections. The author and reviewers had a follow up discussion on the comments and corrections.

The DPIA was implemented into the STATSports at the beginning of a rebuild of a current product and extension into cloud services. The members of the software team included were the head of software engineering, the software architect, the product owner, the head developer and two developers one of which was appointed the security champion for the project.

4.4.6 Evaluate Experience

Figure 4.19 summarises the evaluation of the DPIA draft implemented in cycle 2 discussed in this section.

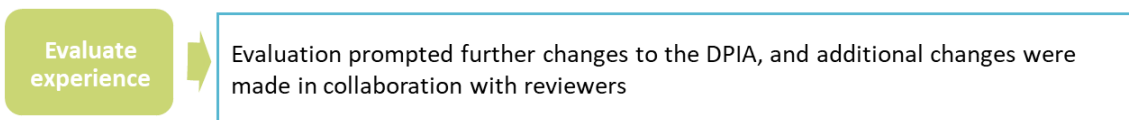


Figure 4.19 Evaluation of the DPIA draft implemented in cycle 2

The DPIA draft was reviewed by the STATSports development team and internally within the RSRC. The evaluation prompted various changes to the DPIA, and changes were made in collaboration with the reviewers.

The development team suggested that Word was not a suitable format to document the outcomes. Word was too cumbersome to navigate particularly when the DPIA sections were reported chiefly through tables. The stepped processes of the framework

Chapter 4 Development of the Framework

required adding to tables as one moved through the DPIA. This required continual updating of the tables. The research and development team agreed that Excel would be a better format to document the tables. The researcher developed an accompanying Excel sheet separated by sections containing the tables. On a follow up review the tables were interlinked as necessary throughout the Excel document. The index tab was positioned next to the open tab, to make navigation through the Excel document easier. In addition, the Excel document tabs followed the layout of the steps in the DPIA Word document for continuity between the documents.

The background section was added to the framework to address the following feedback:

- The development team suggested a section to pull all the information on the project together before step 1. The team had information on different projects scattered through various documents, development platforms and tools. This was a hindrance for STATSports, particularly when the organisation was required to submit security and privacy compliance evidence for business tenders and external audits for ISO 27001 certification and clients. Having all the security and privacy compliance evidence for each software project in one document would simplify answering these requirements. The backdrop section gathered all the information in relation to the specific software project;
- The internal review recommended providing instructions on how to use the framework and the accompanying Excel sheet in the suggested background section. The idea was to have the user familiarise themselves with the DPIA and Excel document before beginning the implementation. Reviewers reported finding it difficult to find their way back and return to the start of a step or section after hitting links to appendices, tables or other sections. Links were inserted into appendices, tables and section headings back to related parts. The author also added navigation tips to the how to use this document section. The author provided two diagrams at the beginning of the DPIA. The first mapped the framework and DPIA documentation and the AAMI TIR 57 security risk process. The second diagram outlined the six steps of the framework;
- On recommendation from the software development team directions were added at the start of each section of the DPIA. They found following the section processes difficult when left to their own practice and found it generally difficult

to navigate through the DPIA. A table was provided at the beginning of each section that outlined the components within the section and the outcomes. Each component in the table had links to the relevant tables and additional information for that component.

The software development team did not have any difficulty with the language used throughout the DPIA. They did note that there were occasions when they looked up some of the terminology or asked the researcher directly after the initial presentation and when working as a team without the researcher. However, this did not inhibit understanding the components of the DPIA and what the outcomes of each component should be. The development team welcomed the DPIA providing the outcomes for the relevant components.

4.4.7 Assess Usefulness or Exit

Figure 4.20 presents a summary of the assessed usefulness of the research from cycle 2.

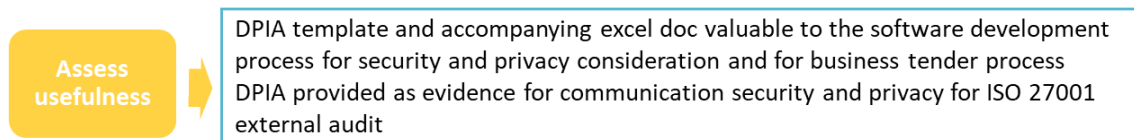


Figure 4.20 Assessed usefulness of the DPIA and accompanying excel document from cycle 2.

The internal reviewers identified that the DPIA and the accompanying Excel document was beneficial for an SME. It provided all the components required to provide evidence of data security and privacy in a software project. The internal reviewers commented that the framework was very thorough and contained a great deal of information. On completion of the STATSports and internal RSRC evaluation, the DPIA and accompanying Excel document was sent an external expert for validation. STATSports began implementing the framework for the new project. The organisation was scheduled for an ISO27001 external audit, which included an audit of the security and privacy controls in the new software project. The DPIA was used for the external ISO 27001 audit and fulfilled the requirements of the audit. In addition, a refined version of the DPIA is used by STATSports as evidence for compliance to regulatory data protection requirements in the business tendering process. The software development team have developed a number of SOPs around the processes for security and privacy for the many forums, platforms and libraries used in the development process. They have linked these into the framework and the DPIA within the organisation.

4.4.8 Report Research Results

Figure 4.21 provides a summary of how the research from cycle 2 was reported.

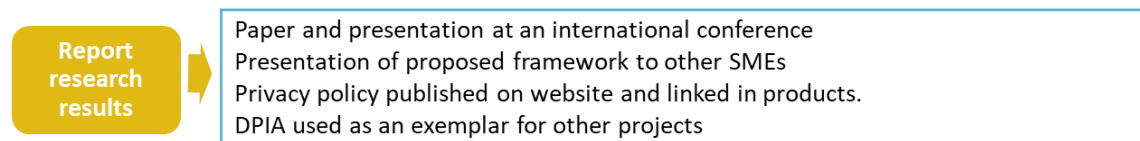


Figure 4.21 Cycle 2 research results report summary

The researcher presented a paper at the EuroAsiaSPI 2018 conference.

- McCaffery, F., Özcan-Top, Ö., Treacy, C., Paul, P., Loane, J., Crilly, J. and Mahon, A.M. (2018). A Process Framework Combining Safety and Security in Practice. In: Communications in Computer and Information Science. pp.173–180.

The author also presented the implementation of the framework and GDPR requirements for data security and privacy to a SME medical software development organisation BlueBridge Technologies. The researcher assisted the head of software engineering in BlueBridge with threat modeling for a new software project. The privacy policy is published on the STATSports website and in their products. The DPIA is used as an exemplar and foundation for development of future STATSports software projects.

4.5 Cycle 3 – Framework Properties and Risk Assessment

Cycle 3 developed the framework properties and adapted three models, two threat models STRIDE and LINDDUN and the risk assessment model in NIST SP 800-30. This provided key aspects for steps 1-4 of the framework, highlighted in Figure 4.22 below.

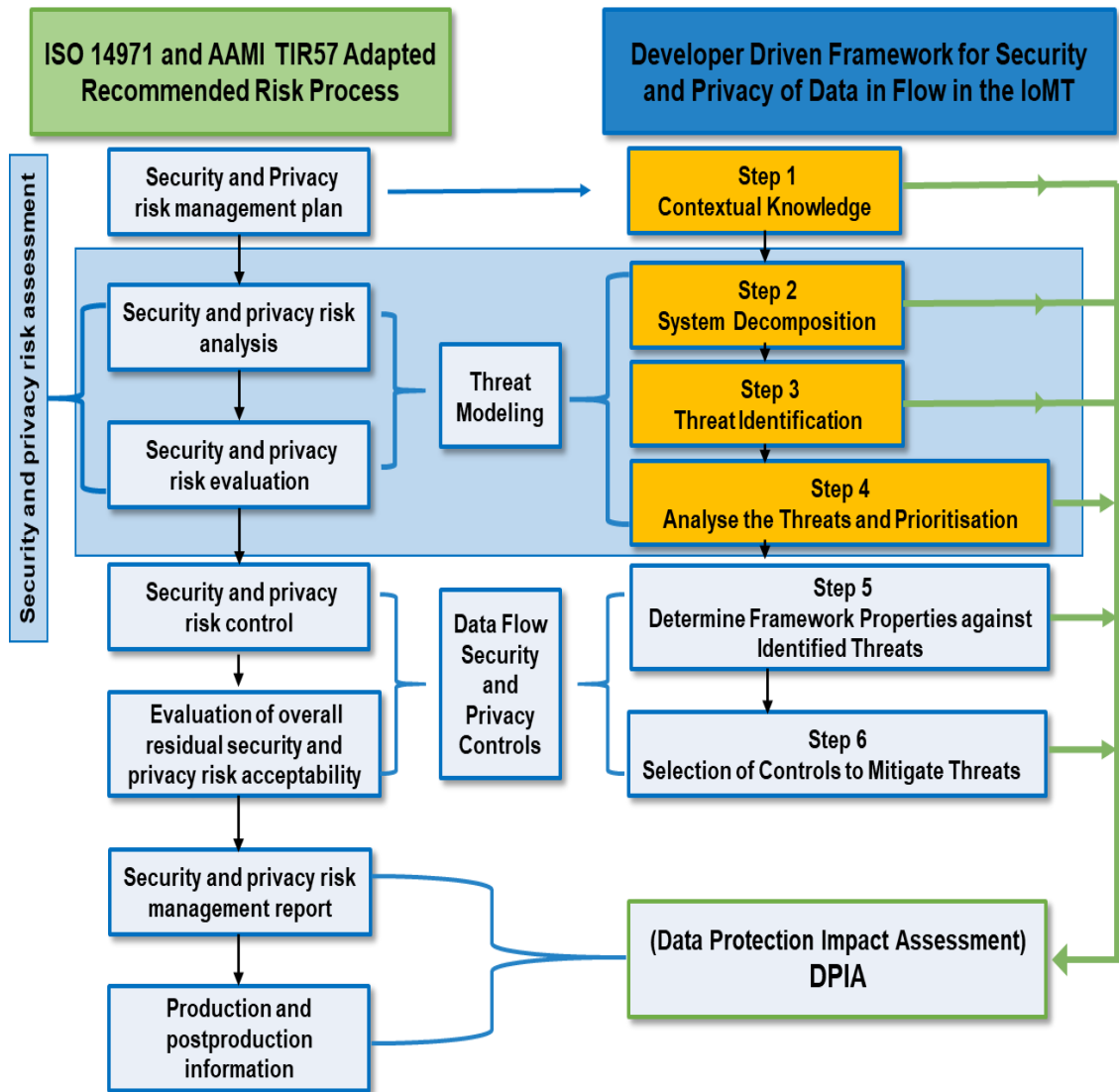


Figure 4.22 Steps 1-4 of the framework

Figure 4.23, presents a summary of cycle 3, which will be discussed in this section.

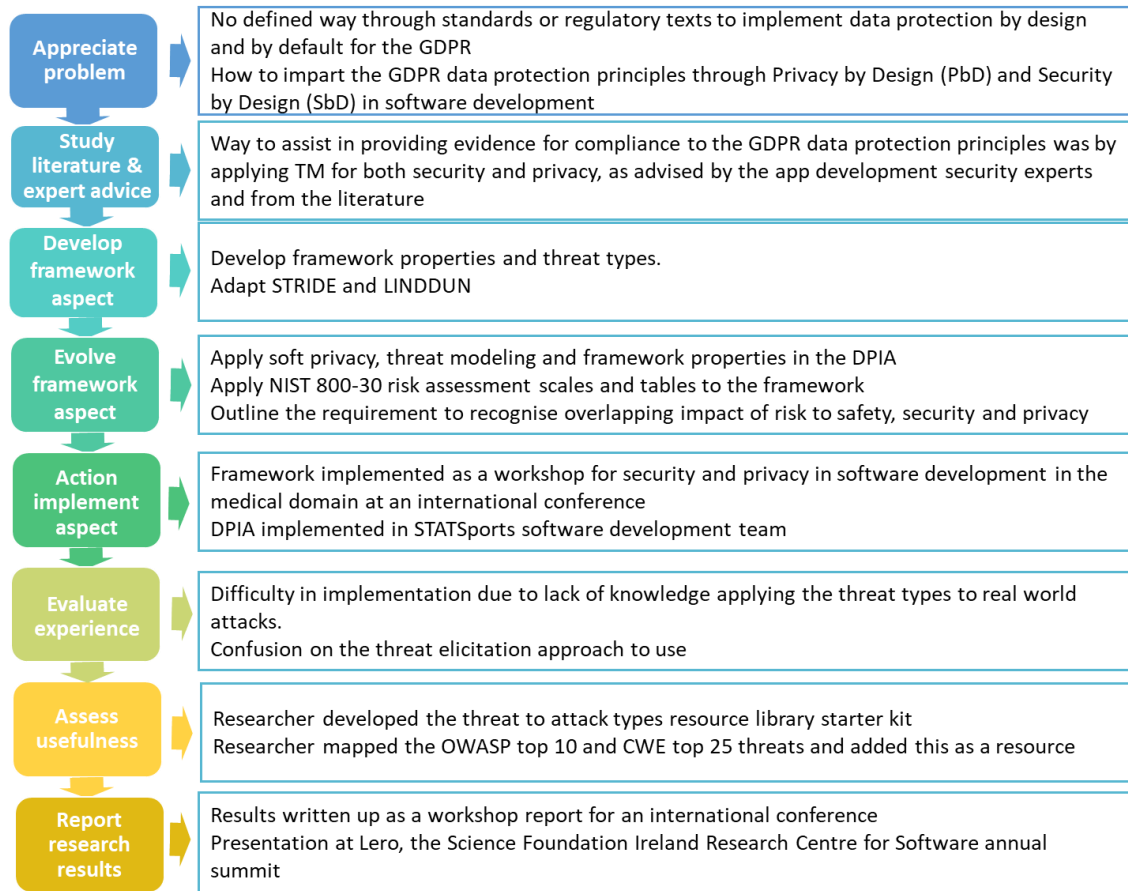


Figure 4.23 Cycle 3 summary

4.5.1 Appreciate the Problem

Figure 4.24 outlines the step, appreciate the problem, in cycle 3.

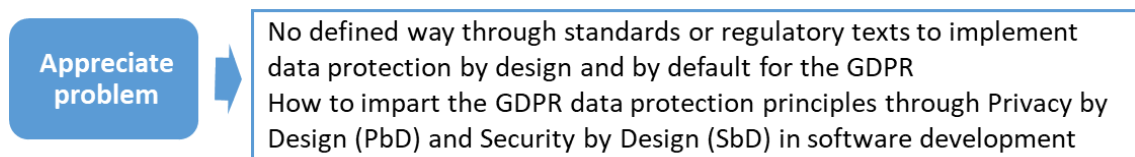


Figure 4.24 Cycle 3 appreciate the problem outline

The researcher and STATSports appreciated that the GDPR is like most regulations and standards is broad and ambiguous in what measures are used to provide evidence for compliance. The GDPR states that data protection is implemented into any system, *by design and by default* through observing the data protection principles (EU General Data Protection Regulation (GDPR) 2016 Art. 25). The problem stands that there is no defined way through standards or regulatory texts to implement data protection by design and by

default for the GDPR. The researcher first gathered data to understand the meaning of by design. By design in software engineering, means security and privacy are designed into a development project from initiation, into the devices, the communication protocols and the services (Mouratidis and Kang 2013; McManus 2018; De Francesco 2019). Sion et al. (2018) maintains that the data protection principles of the GDPR incorporate PbD and SbD, for any system or service that involves processing personal data. The problem was how to relate these data protection principles through PbD and SbD to software development. GDPR by design and by default, also requires that risks to the data protection principles have been assessed and addressed, which presented another problem. There was no established risk-based approach for security and PbD for data in flow in the IoMT based in the GDPR data protection policies.

4.5.2 Study the Literature & Expert Advice

Figure 4.25 outlines what literature and expert advice was used in this cycle.

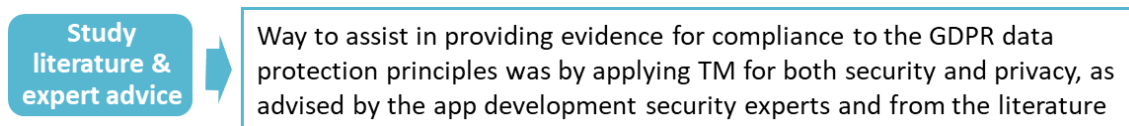


Figure 4.25 Cycle 3 literature studied and expert advice outline

The researcher investigated the literature and consulted with the app development security experts to gather information on how software engineering applied security and privacy by design. The researcher reviewed security and privacy in the domains of:

- Generic software development;
- Medical device software;
- Networks;
- IoT; and
- IoMT.

The researcher concluded the way to assist in providing evidence for compliance to the GDPR data protection principles was by applying TM for both security and privacy, as advised by the app development security experts. Threat modeling is based on the preservation of properties. It was determined the preservation of security and privacy properties could be used to provide evidence of compliance to the GDPR data protection principles. This resulted in the development of the framework properties. The researcher considered the expansion of the traditional data security properties confidentiality,

integrity, and availability, also known in information security as the CIA triad model. Both the literature and the security experts stated that the CIA triad model no longer adequately addresses the constantly changing security environment of the IoT and IoMT and increased cybersecurity risks. The literature was limited in relation to privacy properties and the security experts had no knowledge or had never implemented privacy properties. The security experts stated privacy was addressed primarily through encryption. The STRIDE and LINDDUN threat models were selected for adaptation into the framework. They were chosen because both use a similar systematic TM approach based in the preservation of security and privacy properties. STRIDE is a popular and widely used TM tool for evaluating security threats (Hussain et al. 2014; Sommer et al. 2019). However, STRIDE does not consider privacy, the LINDDUN model addresses privacy (Deng et al. 2010).

4.5.3 Develop Framework Aspect

Figure 4.26 provides an overview of the developed aspect of the framework in cycle 2.



Figure 4.26 Outline on aspect of the framework development in cycle 3

The researcher expanded the traditional security CIA triad model to include additional security properties and add privacy properties. The framework properties were gathered and merged from the STRIDE and LINDDUN models and the ISO 27033-3 standard, developed from ITU-T X.805. The framework properties sources are presented in Figure 4.27 on the next page. The framework tracked the STRIDE and LINDUNN models, where each property has a corresponding threat that could violate that property. These TMs consider threats to data security and privacy of the system and could provide evidence for the assessment of risk as expected in the GDPR DPIA.

There were two security properties not in the STRIDE model but based in ISO/IEC 27033-3, communication or transport security and opacity (privacy ITU-T X.805). The researcher met the opacity and privacy properties and corresponding threat types through the adoption of the LINDDUN model. The inclusion of communication or transport security as a distinctive property was deemed important given the framework is based in end-to-end security of data in flow in IoMT. This property did not align with any of the

STRIDE or LINDDUN threat types. The researcher explored the OWASP Top 10 mobile risks for a potential threat type to this property. The threat type insecure communication was adapted into the framework. The insecure communication threat type involves exploiting vulnerabilities when the data is transmitted.

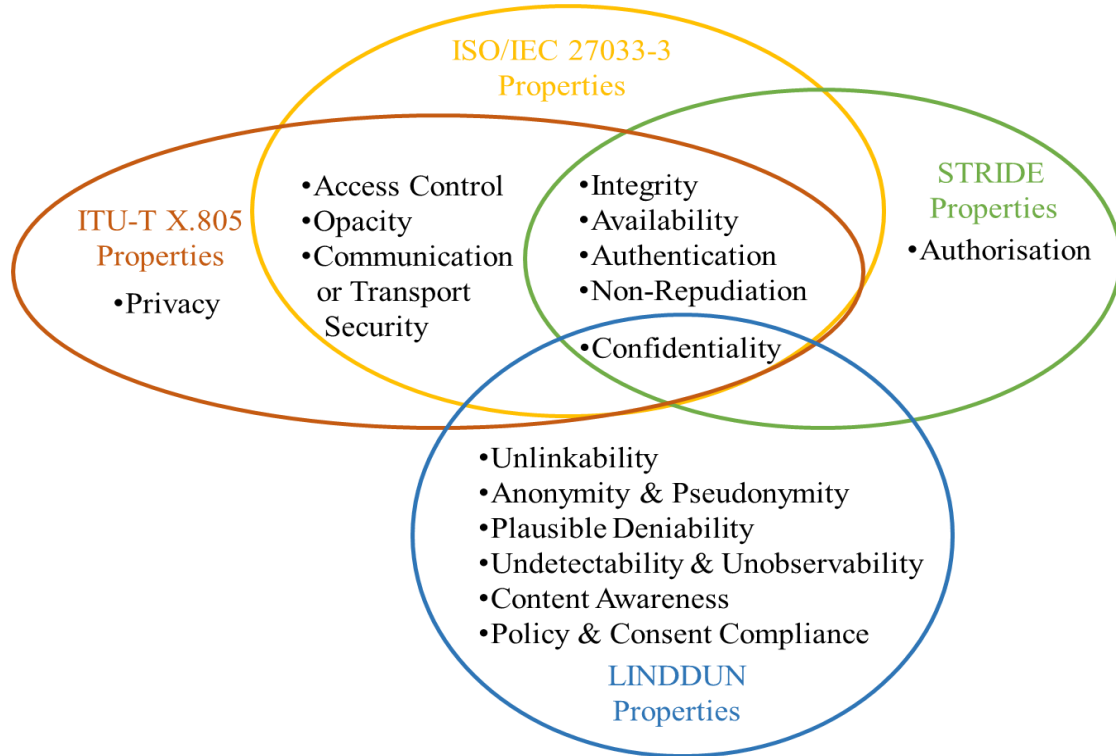


Figure 4.27 Framework properties sources

The security property authorisation was embedded in STRIDE and not in ISO 27033-3. The security property access control was embedded in ISO 27033-3 and not in STRIDE. The researcher included both access control and authorisation properties as distinct security properties after consideration of the definition of access control in ISO/IEC 27033-3:

“access control provides, through the use of authentication and authorisation, control to enforce access to network devices and services, and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications” (ISO/IEC 2010, p.5).

Both the access control and authorisation properties were determined to be interdependent and violated by the threat type elevation of privilege. The framework properties with corresponding threats and definitions are presented in Table 4.2 in the following pages.

Table 4.2 Framework Properties and Threat Types with Definitions and Descriptions

Property Description	Framework Properties Security (s) Privacy (p)	Framework Threat Types	Threat Description
<p>ISO 27001 (2013a) definition - Provision of assurance that a claimed characteristic of an entity is correct.</p> <p>ISO/IEC 27033-3 definition - <i>Concerned with confirming or substantiating the claimed identity of a user or communicating parties when used by access control for authorization, and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.</i> (ISO/IEC 2010, p.5)</p>	<p>Authentication (s)</p>	<p>Spoofing</p>	<p>Impersonating something or someone else, pretending to be something or someone other than yourself (Shostack 2014b).</p> <p><i>Allows an adversary to pose as another user, component or system that has an identity in the system being modeled</i> (Swiderski and Synder 2004, p.104).</p>
<p>ISO/IEC 27033-3 (2010) definition - Property of accuracy and completeness.</p> <p>Concerned with maintaining the correctness or accuracy of data and protecting against unauthorized modification, deletion, creation, and replication.</p>	<p>Integrity (s)</p>	<p>Tampering</p>	<p><i>The modification of data within the system to achieve a malicious goal</i> (Swiderski and Synder 2004, p.104).</p> <p>Modifying data or code. The modification of something you're not supposed to modify. It can include packets on the wire (or wireless), bits on disk, or the bits in memory (Shostack 2014b).</p>
<p>ISO 27002 definition - Ability to prove the occurrence of a claimed event or action and its originating entities (ISO 27002)</p> <p><i>Concerned with maintaining an audit trail, so that the origin of data or the cause of an event or action cannot be denied. Identifying the authorized person that performed an unauthorized action on protected data has nothing to do with the data's confidentiality, integrity, availability</i> (ISO/IEC 2010, p.5).</p>	<p>Non-repudiation (s&p)</p>	<p>Repudiation</p>	<p><i>The ability of an adversary to deny performing some malicious activity because the system does not have sufficient evidence to prove otherwise</i> (Swiderski and Synder 2004, p.104).</p>

Chapter 4 Development of the Framework

<p><i>...plausible deniability refers to the ability to deny having performed an action that other parties can neither confirm nor contradict (Wuyts and Joosen 2015, p.5).</i></p> <p>Wuyts and Joosen (2015) quote Roe (2010, p.55) on the relationship between non-repudiation and plausible deniability “...the goal of the non- repudiation service is to provide irrefutable evidence concerning the occurrence or non-occurrence of an event or action. If we believe that there is a need for this as a security service [...] we must also concede that some participants desire the opposite effect: that there be no irrefutable evidence concerning a disputed event or action.” This “complementary service” is plausible deniability.</p>	<p>Plausible deniability (p)</p>	<p>Non-Repudiation</p>	<p><i>Non-repudiation allows an attacker to gather evidence to counter the claims of the repudiating party, and to prove that a user knows, has done or has said something (Wuyts and Joosen 2015, p.8).</i></p>
<p><i>Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (McCallister et al. 2010).</i></p> <p>Property that information is not made available or disclosed to unauthorized individuals, entities, or processes</p>	<p>Confidentiality (s&p)</p>	<p>Information disclosure</p>	<p><i>The exposure of protected data to a user that is not otherwise allowed access to that data (Swiderski and Synder 2004, p.104)</i></p> <p><i>Exposing information to someone not authorised to see it (Wuyts and Joosen 2015, p.15).</i></p>
<p>ISO/IEC 27033-3 - Ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points) (2010, p.5).</p>	<p>Communication or Transport Security (s)</p>	<p>Insecure Communication</p>	<p><i>Threat agents might exploit vulnerabilities to intercept sensitive data while it’s traveling across the wire (OWASP 2020a).</i></p> <p><i>Getting data from point A to point B insecurely allowing interception of data via communication channel (OWASP 2020a).</i></p>
<p>ISO/IEC 27001 definition - Property of being accessible and usable upon demand by an authorized entity.</p> <p><i>Concerned with ensuring that there is no denial of authorized access to network elements, stored information, information flows, services, and applications (2010, p.5).</i></p>	<p>Availability (s)</p>	<p>Denial of Service</p>	<p><i>Occurs when an adversary can prevent legitimate users from using the normal functionality of the system (Swiderski and Synder 2004, p.104).</i></p> <p><i>...to prevent a system from providing service, including by crashing it, making it unusably slow, or filling all its storage (Shostack 2014b, p.10).</i></p>

Chapter 4 Development of the Framework

<p>ISO 27033-1 (2015b) definition - The granting of rights, which includes the granting of access based on access rights.</p>	<p>Authorization (s)</p>	<p>Elevation of Privilege</p>	<p><i>Occurs when an adversary uses illegitimate means to assume a trust level with different privileges than he currently has (Swiderski and Synder 2004, p.104).</i></p>
<p>ISO/IEC 27002 (2013b) definition - Means to ensure that access to assets is authorized and restricted based on business and security requirements. <i>Provides, through the use of authentication and authorization, control to enforce access to network devices and services, and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. (ISO/IEC 2010, p.5).</i></p>	<p>Access Controls (s)</p>		<p><i>...is when a program or user is technically able to do things that they're not supposed to do (Shostack 2014b, p.10). Gain capabilities without proper authorization. Allowing someone to do something they're not authorised to do.</i></p>
<p>Is <i>hiding the link between two or more actions, identities or pieces of information (Items of Interest (IOI))</i> (Wuyts and Joosen 2015, p.5).</p>	<p>Unlinkability (p)</p>	<p>Linkability</p>	<p><i>Being able to sufficiently distinguish whether 2 Items of Interest (IOI) are linked or not, even without knowing the actual identity of the subject of the linkable IOI. Not being able to hide the link between two or more actions/identities/pieces of information. (Wuyts and Joosen 2015, p.12).</i></p>
<p>Anonymity - <i>Anonymity of a subject from an attackers perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set (Pfitzmann and Hansen 2010, p.10). Anonymity can also be described in terms of unlinkability (Wuyts and Joosen 2015, p.5). Anonymity is unlinkability between identity and other properties.</i></p> <p>Pseudonymity - <i>The pseudonymity property suggests that it is possible to build a reputation on a pseudonym and possible to use multiple pseudonyms for different purposes (Wuyts and Joosen 2015, p.5). A subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names (Pfitzmann and Hansen 2010, p.21).</i></p>	<p>Anonymity & Pseudonymity (p)</p>	<p>Identifiability</p>	<p><i>Being able to sufficiently identify the subject within a set of subjects (i.e., the anonymity set). Not being able to hide the link between the identity and the IOI (an action or piece of information) (Wuyts and Joosen 2015, p.13). Identifiability of a subject from an attacker's perspective means that the attacker can sufficiently identify the subject within a set of subjects, the identifiability set (Pfitzmann and Hansen 2010, p.35).</i></p>

Chapter 4 Development of the Framework

<p>Undetectability and unobservability involves the ability to act without the action being known e.g. to be able to be in a particular place without being observed - <i>hiding the user's activities</i> (Wuyts and Joosen 2015, p.6).</p> <p>Undetectability - Undetectability of an item of interest (IOI) from an attackers perspective means that the attacker cannot sufficiently distinguish whether it exists or not. If we consider messages as IOIs, this means that messages are not sufficiently discernible from, e.g., random noise (Pfitzmann and Hansen 2010, p.35).</p> <p>Unobservability - Unobservability of an item of interest (IOI) means</p> <ul style="list-style-type: none"> • undetectability of the IOI against all subjects uninvolved in it and • anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI (Pfitzmann and Hansen 2010, p.35). 	<p>Undetectability & Unobservability (p)</p>	<p>Detectability</p>	<p><i>An attacker can sufficiently distinguish whether an item of interest (IOI) exists or not</i> (Wuyts and Joosen 2015, p.16).</p>
<p><i>...focuses on the user's consciousness regarding his own data. The user needs to be aware of the consequences of sharing information. These consequences can refer to the user's privacy, which can be violated by sharing too much personal identifiable information, as well as to undesirable results by providing incomplete or incorrect information</i> (Wuyts and Joosen 2015, p.6).</p>	<p>Content Awareness (p) Soft Privacy</p>	<p>Unawareness</p>	<p><i>Not understanding the consequences of sharing personal information in the past, present, or future.</i> (Wuyts and Joosen 2015, p.18).</p>
<p><i>...requires the whole system – including data flows, data stores, and processes – as data controller to inform the data subject about the system's privacy policy or allow the data subject to specify consents in compliance with legislation, before users access the system. This property is closely related to legislation</i> (Wuyts and Joosen 2015, p.7).</p>	<p>Policy and consent compliance (p) Soft Privacy</p>	<p>Non-compliance</p>	<p><i>Not following the (data protection) legislation, the advertised policies or the existing user consents</i> (Wuyts and Joosen 2015, p.19).</p>

4.5.4 Evolve the Framework

Figure 4.28 is an outline of the progress in the framework development during cycle 3.

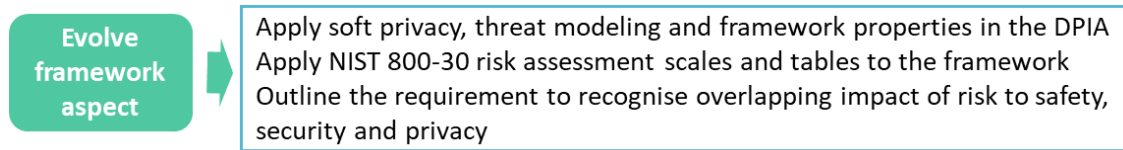


Figure 4.28 Cycle 3 progress in the framework development outline

The properties and threats were adapted into the framework. The adaptation started with the LINDDUN classified soft privacy properties and corresponding threats. LINDDUN classifies privacy as either hard privacy or soft privacy. These are listed in Table 4.3 below. The soft properties were employed in the framework in the background and step 1 sections of the DPIA. Deng et al. (2010), contend that the two soft privacy properties are not fully and clearly expressed or demonstrated in the literature. They maintain soft privacy is based on the assumption that data is given away and therefore, it is necessary to use policies, regulations and consent to manage it (Deng et al. 2010). The researcher delivered the soft properties and opportunity to mitigate the corresponding threats through the draft privacy policy, screening and lawful processing questionnaires. These aspects included consideration and planning for consent in the documentation and software development process.

Table 4.3 LINDDUN classification of hard and soft privacy with properties and corresponding threats

Privacy Properties	Privacy Threats
Soft Privacy	
Content awareness	Content Unawareness
Policy and consent compliance	Policy and consent noncompliance
Hard Privacy	
Unlinkability	Linkability
Anonymity & Pseudonymity	Identifiability
Plausible deniability	Non-repudiation
Undetectability & unobservability	Detectability
Confidentiality	Disclosure of information

LINDDUN defines hard privacy as the aim of directly controlling data before it is given away and is applied in software development (Deng et al. 2010). These hard privacy properties and corresponding threats were merged with the security properties and corresponding threats. The confidentiality property and its disclosure of information

threat was the single property that overlapped between privacy and security. The framework properties were employed to steps 5 and 6 of the framework.

The TM process was adapted to enable the risk assessment piece of the ISO 14971 and AAMI TIR57 recommended security risk process, outlined in Figure 4.29. The framework adapted three of the conventional TM steps, model the system step 2, find the threats step 3, and analyse and prioritise the threats step 4. The framework threats, excluding the soft privacy ones, were applied to the TM process embedded in these steps of the framework. The system decomposition is completed through DFDs. The researcher provided a standardised table of elements and rules for drawing the DFDs as the users are inexperienced. Annotation was added to provide security and privacy references to the DFDs and shift security and privacy into a visual for the software development team, customer and tender process and the ISO 27001 certification.

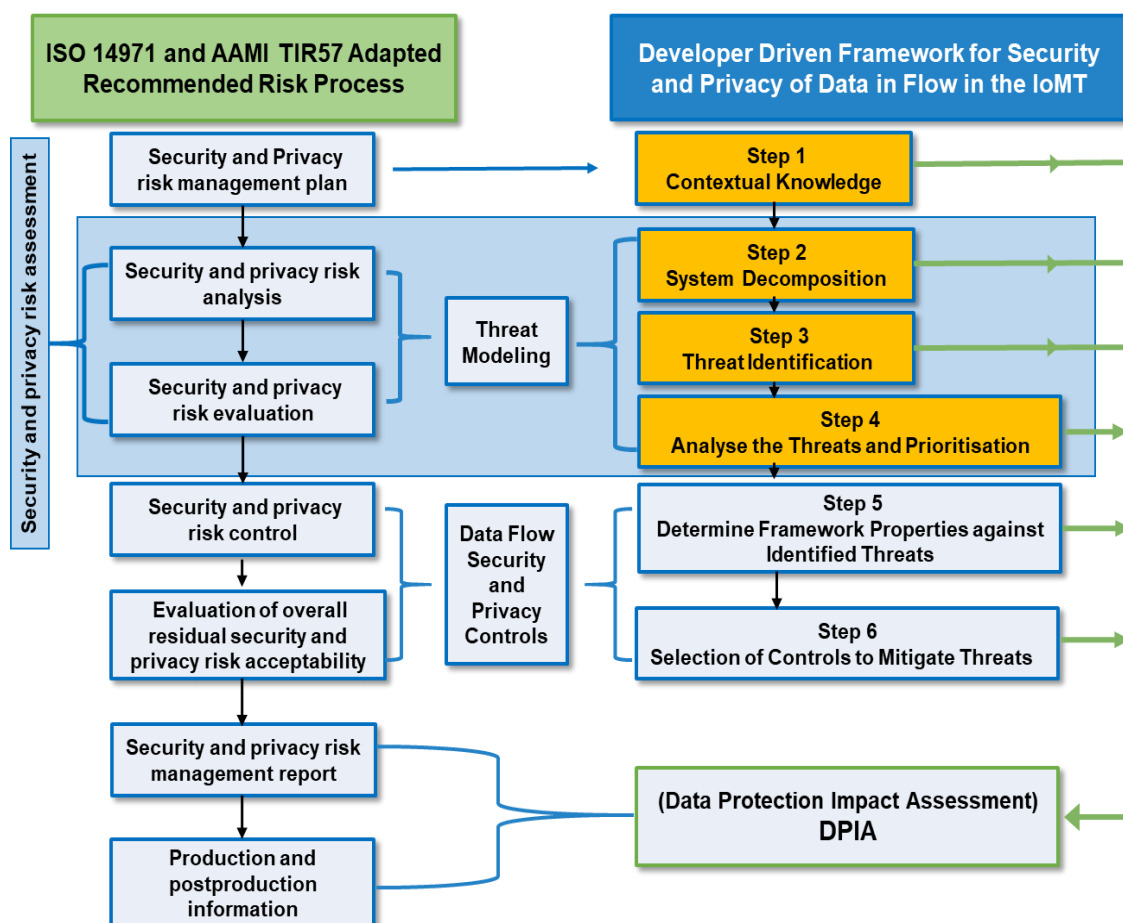


Figure 4.29 Framework adaption of TM process to the risk assessment part of ISO 14971 and AAMI TIR57 recommended security risk process

There are two approaches used with the STRIDE TM, per-element, and per-interaction (Shostack 2014b), considered for threat identification at step 3 of the framework. The STRIDE per-element approach focuses on identifying threats against each element of the system. However, as stated by Shostack (2014b, p.80), “*threats don’t show up in a vacuum. They show up in the interactions of the system.*” As the framework concentrates on data in flow through a system the recommendation in the framework is to use the per-interaction approach. Per-interaction means threats would be identified for each interaction of data in the system. As the framework is based on data in flow, it is recommended that threat elicitation is completed with the per-interaction approach. This approach was developed in relation to STRIDE by Larry Osterman and Douglas MacIver of Microsoft (Shostack 2014b).

In addition, the LINDDUN TM developed a template for per-interaction mapping, using the same concept of tuples of origin, destination, and data flow though, changing the term origin to source (Sion, Wuyts, et al. 2018). The LINDDUN per-interaction mappings template is based on all possible combinations of DFD elements interactions (Sion, Wuyts, et al. 2018). This threat elicitation approach is completed by examining all the different interactions between the elements of the software system. The per-interaction approach to threat enumeration considers tuples of **origin, interaction, and destination**. This involves all communication between a source and destination. This approach is recommended as focusing on “*interactions are a good focal point for threat modeling because a system that can’t be interacted with can’t be attacked* (Dhillon 2011, p.43)”. This approach links firmly with the research’s aim of security and privacy of data in flow in the IoMT. Step 3 would result in a set of extracted threats, which require analysis and prioritisation, done in Step 4.

At step 4, the researcher applied the procedures in the NIST SP 800-30 standard for risk assessment as it was recommended in both ISO 14971 and AAMI TIR 57. The framework employed the qualitative formula assessment models of likelihood and impact from NIST SP 800-30. The qualitative tables to apply this formula included:

- Assessment scale that uses the five-point rating system – Very Low, Low, Moderate, High, and Very High;
- Likelihood assessment scales;
- Impact assessment scales;
- Risk matrix for assessment of risk.

Chapter 4 Development of the Framework

The qualitative assessment approach was selected because of the framework's target audience and the lack of knowledge and understanding. A qualitative assessment, using only a few factors was seen as appropriate for inexperienced SMEs and their developers. It was also chosen because data security and privacy risks, whether intentionally for example through an attacker or unintentionally through lack of regulatory understanding, resulting in a vulnerability being exploited involves human behaviour (AAMI 2016). The qualitative approaches allow for adjustment to adverse human actions.

The researcher also used the options for risk mitigation from NIST SP 800-30. These options for risk mitigation determine how each risk will be handled. The applied options for risk mitigation are presented in Table 4.4 below.

Table 4.4 Options for risk mitigation (NIST 2012)

Options for Risk Mitigation	Description
Accept Risk	If falls within established risk acceptance criteria
Avoid Risk	Eliminating it entirely, remove the process, asset or requirement that involves the risk
Share Risk	Insurance or outsource
Modify Risk	Apply Security Controls to reduce the risk

The option to accept risk is determined by the organisation. ISO 14917 identifies risk acceptability,

“as reducing risk as low as reasonably practicable, reducing risk as low as reasonably achievable, or reducing risk as far as possible without adversely affecting the benefit-risk ratio” (2019, p.8).

The researcher employed the EU Medical Device Regulation (MDR) guidance that you must reduce risks as far as possible to an acceptable level (Medical Device Coordination Group 2019). This means that SMEs and developers in the EU need to consider risk reductions for all risks, regardless of the risk level. This in turn means, the threats determined for risk reduction require prioritisation for mitigation. The framework follows the grouping options for risk mitigation from NIST SP 800-30, as guidance for SMEs and developers presented in Table 4.5 overleaf. For ease of prioritisation recognition, the numerical scale is 1-5 was implemented by the researcher, where risks scaled at very high unacceptable risk has top priority (1) for modification and mitigation. The prioritisation scale moves down to low and very low scale of 4 and 5 respectively, which will not require modification.

Table 4.5 Risk mitigation and prioritisation

Scale for level of risk	Level of Impact	Prioritisation
Very High	Modify Risk/Avoid/Share	1
High	Modify Risk	2
Moderate	Modify Risk	3
Low	Acceptable	4
Very Low	Acceptable	5

As recommended in both ISO 14971 and AAMI TIR 57, the framework advises that treatment of any risk corresponding to security and privacy should also involve consideration in relation to the safety risk assessment. Particularly in the medical domain, prioritisation of safety of the patient should always be considered. This could provide potential conflict with the data security and privacy risk assessment. The framework advises that developers will have to assess how the application of a control for security or privacy could impact the safety of the medical device. Equally, consideration must be given to the impact of a safety control on the security or privacy of the data. The framework emphasises that any risk control measure should be applied with consideration for all the risk assessment models. It is also noted that a specific risk assessed as a must mitigate in one risk assessment model, might be assessed as does not need further mitigation in another risk assessment model. This means it is important that the risk assessment approach is a shared between security, privacy and safety within the medical domain.

4.5.5 Action

Figure 4.30 outlines the actions taken in cycle 3.

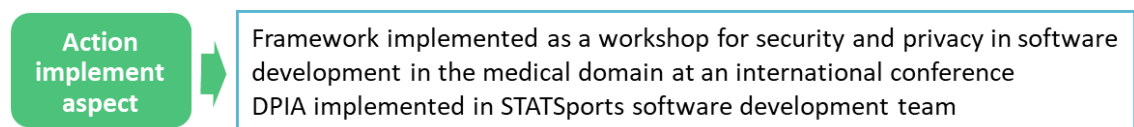


Figure 4.30 Cycle 3 action summary

The framework was implemented into the STATSports software development team. In addition, the framework was implemented as a workshop for security and privacy in software development in the medical domain at the international 26th EuroSPI

conference. Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: 26th EuroSPI Conference. Edinburgh: Springer. The workshop provided insight into aspects of the framework that needed development if it is to be applied by inexperienced users.

4.5.6 Evaluate Experience

Figure 4.31 summarises the evaluation of the DPIA draft, implemented in cycle 3 and discussed in this section.

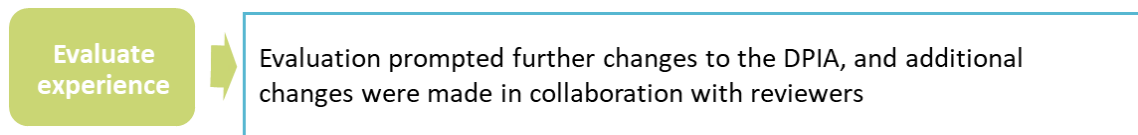


Figure 4.31 Evaluation of the framework implemented in cycle 3

At implementation, both the development team and the participants of the workshop were able to follow the framework with ease until step 3 and threat identification. The software development team were confused which TM approach to take for threat identification. The researcher had included the two TM approaches, per-element, and per-interaction. On discussion with the security experts and the development team the per-interaction approach was endorsed for use because:

- It is a simplified approach for inexperienced developers (Shostack 2014b; Dhillon 2011), which fits the proposition of the framework;
- Per-interaction analysis can reduce the duplication of threat elicitations because there is a clear distinction between these different roles involved in a single interaction, using the tuple of origin, data flow and destination (Sion, Wuyts, et al. 2018); It should be noted that Shostack (2014b) and Dhillon (2011) use the term interaction and Sion et al. (2018) use the term data flow. This framework will use the term data flow;
- Limiting the number of analysis points is important for complex systems and is less dependent on attack knowledge. This is especially important when threat modeling resources are limited (Dhillon 2011) and developers are inexperienced
- Focusing on interactions rather than elements yields comparable results with fewer analyses (Shostack 2014b; Dhillon 2011);
- Threats show up in the interactions of the system and tend to cluster around trust boundaries (Shostack 2014b). Many threats occur where the data flow crosses the

boundaries but, may appear anywhere that information is under the control of an attacker. These could include authorisation boundaries, local or internal process boundaries or machine boundaries (trust boundaries);

- When discussing the trust inside systems, it is important to note that trust boundaries are not fixed. They are subject to change as information leaves and enters the different parts of the system. Threat identification per-interaction assists in focusing on these changes in boundaries and considering the potential threats to information with the changes.

The researcher provided information on the per-element approach in the framework however, it was minimal. The framework does suggest that the per-element approach could be beneficial for a risk identification of large databases.

When it came to threat identification via per-interaction both the development team and the participants of the workshop struggled. The lack of experience and knowledge in this area hindered the ability to diagnose and extract potential threats from the threat types to real world attacks. The description of the threat types was not enough to bridge this gap in knowledge. This impeded and slowed the completion of the framework. There was a significant need for help from the researcher to complete step 3 in the workshop time period. Due to the time constraint and lack of knowledge to extract threats to attacks, there was a small number of threat to attack examples used to complete the framework during the workshop.

4.5.7 Assess Usefulness or Exit

Figure 4.32 presents a summary of the assessed usefulness of the framework from cycle 3.

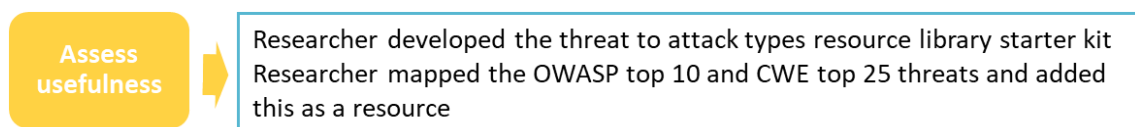


Figure 4.32 Assessed usefulness of framework from cycle 3.

The workshop participants and the software development team feedback was the framework was very useful. The per-interaction approach was a process familiar to the developers and workshop participants. Feedback from the workshop revealed that the framework would be more useful if it provided intelligence on framework threat types into real world attacks. This prompted the researcher to develop the threat to attack library

starter kit from the literature. In addition, the researcher mapped the OWASP top 10 and CWE top 25 threats and added this as a resource to step 3. Again, this is an additional resource to build knowledge and understanding which comes from experience. The researcher also advised that the OWASP top 10 and the CWE top 25 could be used to prioritise the mitigation of threats as these threats are rated according to influence in the real world. Other resources added as references included the OWASP API (application programming interface) Security Top 10 and the OWASP Mobile Top 10.

4.5.8 Report Research Results

Figure 4.33 provides a summary of how the research from cycle 3 was reported.

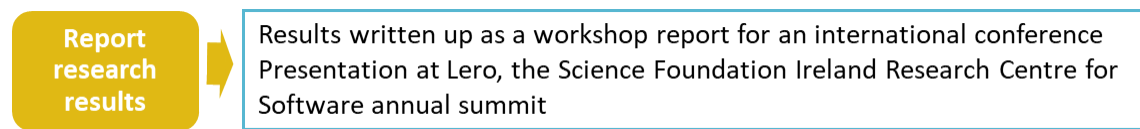


Figure 4.33 Cycle 3 research results report summary

The results were written up as a workshop report for the international conference. Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: 26th EuroSPI Conference. Edinburgh: Springer (Treacy and Macher 2019).

The researcher also presented the Lero Research Project in STATSports at the Lero annual summit. The presentation addressed the data security and privacy evolution within STATSports including:

- Implementing GDPR requirements throughout the organisation and including within software products;
- Completing a gap analysis and meeting elite customer data security and privacy requirements;
- Development of policies and procedures to develop an ISMS within STATSports;
- STATSports' ISO 27001 certification.

4.6 Cycle 4 – Development of the Framework Security and Privacy Controls

Cycle 4 was the development of step 5 and 6 of the framework, highlighted in Figure 4.34 below.

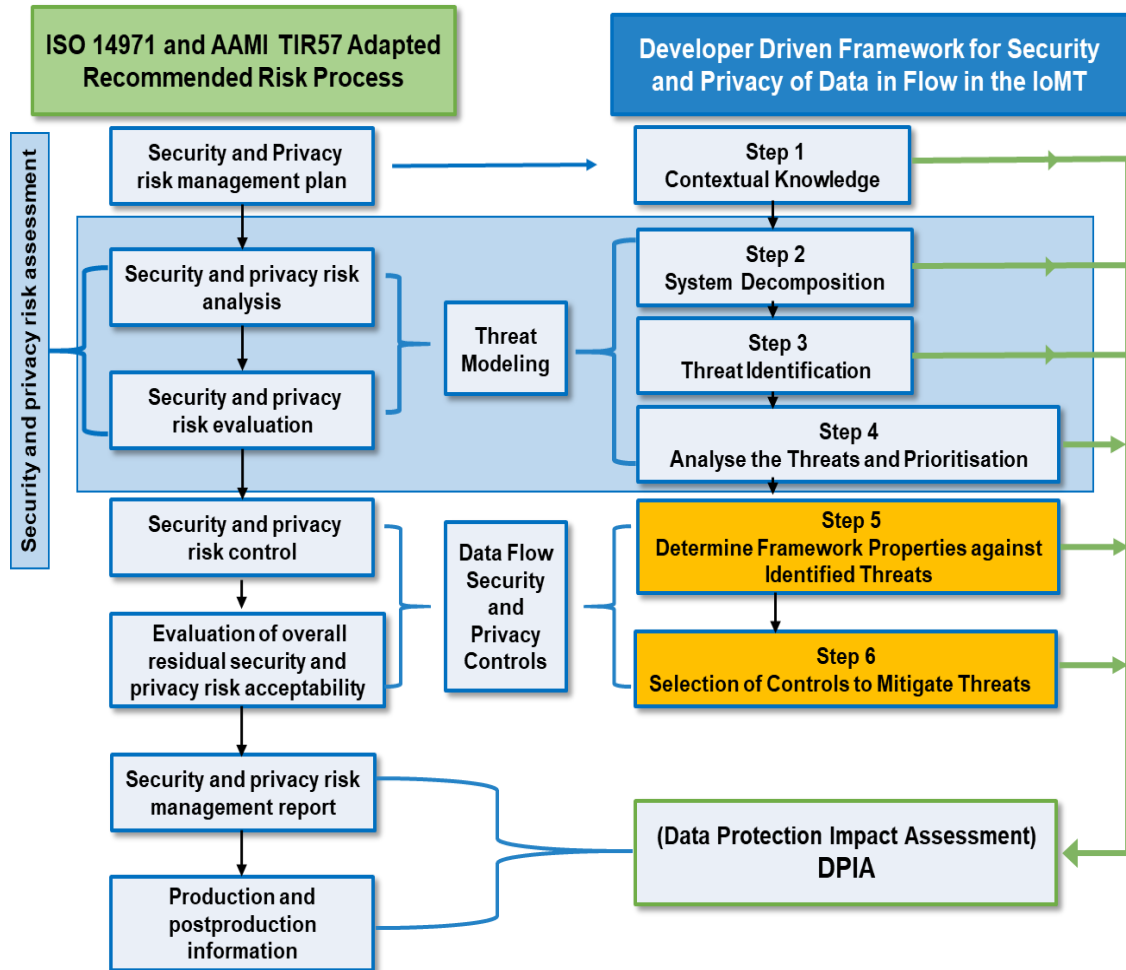


Figure 4.34 Steps 5 and 6 of the framework

Figure 4.35 presents a summary of cycle 4, which will be discussed in this section.

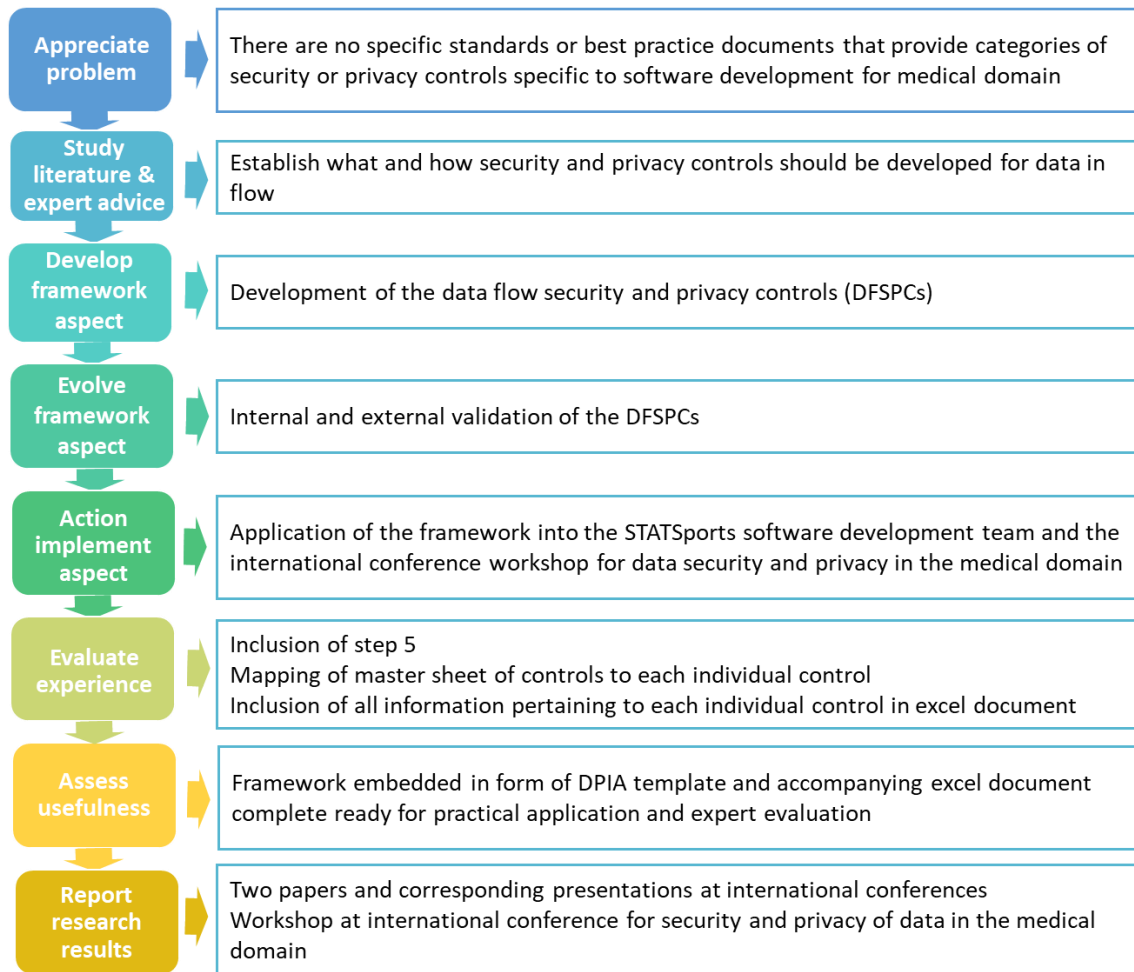


Figure 4.35 Cycle 4 summary

4.6.1 Appreciate the Problem

Figure 4.36 outlines what is discussed to appreciate the problem in cycle 4.

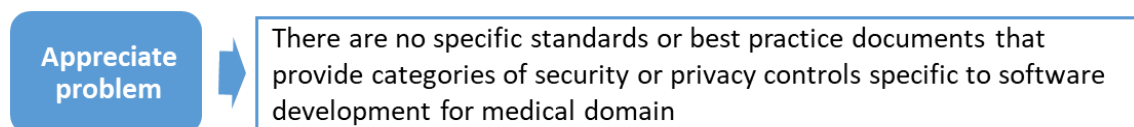


Figure 4.36 Cycle 4 appreciate the problem summary

Any security and privacy assessment methodology requires devising countermeasures and applying controls for protecting against threats (ISO/IEC 2010). The difficulty in the medical and generic software development domains, is there are specific standards and best practice documents that provide categories of security or privacy controls. However,

these are dispersed throughout various domains and are generally not specific to software development. Controls for security and privacy in the software development domain are derived from a variety of standards. This creates difficulty for developers and SMEs. Firstly, SMEs find it complicated to understand and find the appropriate standards or best practice that apply to security and privacy in the medical domain. Secondly, there is difficulty distinguishing the appropriate technical controls that apply to software development. The controls in the standards apply at both an organisational level and technical level. In addition, each standard has an individual classification approach for the controls. This can cause a lack of confidence and uncertainty for developers and SMEs on the appropriate approach to establish appropriate security and privacy controls for software development.

4.6.2 Study the Literature & Expert Advice

Figure 4.37 outlines what literature and expert advice was used in this cycle.

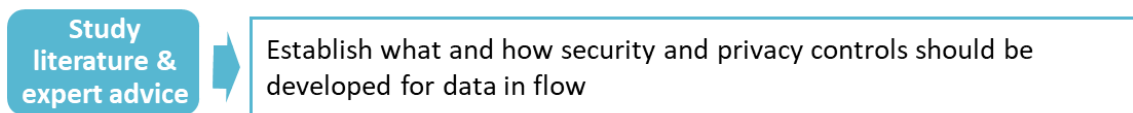


Figure 4.37 Cycle 4 literature studied and expert advice

Data was gathered from the standards in the domains of security and privacy in the medical device, network, and app development domains. There were no references to a list of applicable security and privacy controls from the app and network standards for software development. Each domain referenced a variety of standards to find controls. In addition, many of the controls were at organisational level implementation, not technical.

On conclusion of examination of the standards the development of the DFSPCs focused in the standards used for the development of IEC/TR 80001-2-8. IEC/TR 80001-2-8 identified over 300 security controls in a set of tables evaluated for their relevance in establishing the 19 security capabilities of IEC/TR 80001-2-2 (IEC 2012). These controls were developed using mappings to six international standards. Two of the standards were organisational and four were technical standards. The IEC/TR 80001-2-8 controls did not appropriately address the security and privacy properties identified for the framework due to the following reasons:

Chapter 4 Development of the Framework

- The IEC/TR 80001-2-8 controls are to manage risks to CIA and accountability of data and systems. The controls are related to product security capabilities; privacy is not largely considered;
- IEC/TR 80001-2-8 predominately focuses on controls at an organisational level and less on technical controls for software development. It should be considered as an approach for a foundation in security primarily at organisational level;
- The standard does not specifically consider data privacy.

On examination of the standards and in consultation with the experts, the DFSPCs were established from three of the technical standards used for the development of IEC/TR 80001-2-8:

- **NIST SP 800-53r5** Security and Privacy Controls for Information Systems and Organizations (NIST 2020). IEC/TR 80001-2-8 used Revision 4 of this standard.
- **ISO/IEC 15408-2:2008** Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components (ISO/IEC 2008a);
- **IEC 64223-3-3** Industrial Communication Networks - Network and System Security – Part 3-3: System security requirements and security levels (IEC 2013);

4.6.3 Develop Framework Aspect

Figure 4.38 presents the framework aspect developed in cycle 4.

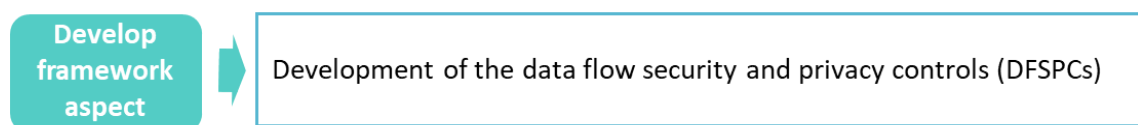


Figure 4.38 Cycle 4 framework aspect developed

Collectively the standards contain over 1200 controls in security and privacy at organisational and technical level. The key objectives for the development of the DFSPCs included:

- Establishment of a set of technical security controls most applicable for the security and privacy of data in flow of a software system;
- Offer a set of technical controls to assist developers in navigating the standards. to close the gap in lack of experience, knowledge and understanding in this area;
- To assist SMEs to demonstrate compliance with security and privacy requirements of regulations;

- To fill the vacuum of specific technical controls that could be applied in software development to address both security and privacy of data;

A criterion was developed with the support of the app and security experts for the extraction of the DFSPCs. This criterion included:

1. The DFSPCs should be based in technical security controls. This was supported out of IEC/TR 80001-2-8 with the division of the standards controls divided into technical security controls and operational/administrative security controls (IEC/TR 2016). The organisational/operational controls were policy based; the technical controls were based in software. The DFSPCs were developed explicitly extracting technical controls to support software development in line with the framework properties;
2. The technical controls for the DFSPCs should be based on the intent of security and privacy for data in flow. As outlined in the literature review the definition of data flow is:

“...movement of data through the active parts of a data processing system in the course of the performance of specific work” [SOURCE: ISO/IEC 2382:2015, 2121825 (ISO/IEC 2015a)].

In the context of this research, data flow is the path data takes through a system comprised of software, hardware or a combination of both, that includes all nodes through which the data travels, from its original source to its end users. It is the movement of data as it passes from one component to the next across networks, network infrastructure devices, between apps, individual systems, and devices, taking into consideration how it changes form during the process. A less detailed diagram from Figure 2.2 in section 2.1.2 of the literature review is presented in Figure 4.39 overleaf. This diagram outlines the possible data flow in the IoMT. During this flow the data can change from data to information and contrariwise.

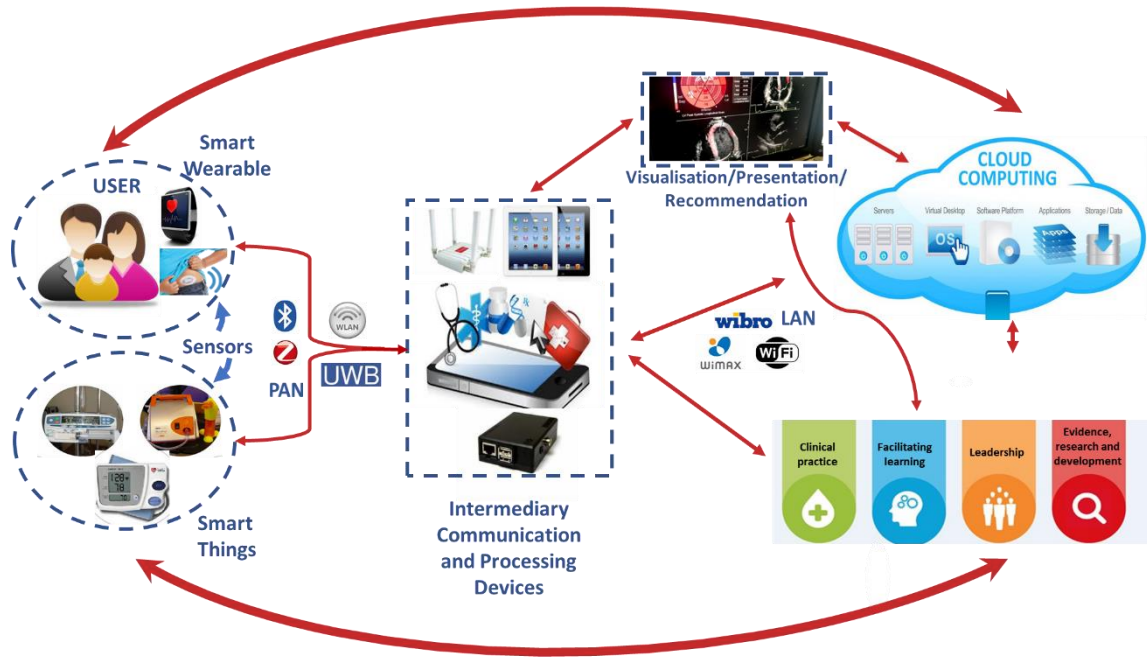


Figure 4.39 Potential data flow in the IoMT

The extraction of the DFSCs from the three technical standards was conducted by a keyword search (KWS). The keywords used for the search are listed in Table 4.6 below. The keywords were developed with the support of the app developer, the security experts and medical standards domain experts.

Table 4.6 List of keywords for search of three technical standards

• Authentication	• Undetectability
• Integrity	• Unobservability
• Repudiation	• Content awareness
• Non-repudiation	• Policy compliance
• Plausible deniability	• Consent
• Confidentiality	• Privacy
• Communication	• Identifiability
• Transport security	• Identifier
• Availability	• De-identification
• Access control	• Deniability
• Authorisation	• Disclosure of information
• Unlinkability	• Unawareness
• Anonymity	• Non-compliance
• Pseudonymity	• Sanitization

The controls from the KWS were evaluated against the criteria for the DFSPCs by the researcher. The controls that did not meet the criteria were not carried forward for validation. These results are provided in the Excel sheet labelled Appendix D. The KWS was completed twice for two reasons. The first KWS was completed when the privacy properties were not included in the framework. Secondly, NIST SP 800-53 was revised from revision 4 to revision 5. During the completion of the first controls extraction process on NIST SP 800-53r4, the internal and external validation had to consider which controls were relevant at organisational or technical level. This required extensive debate, consideration and was very time consuming. However, when NIST SP 800-53 was updated to revision 5, the standard had categorised the controls for organisational or security application.

As a result, categorising the technical controls from version 5 of NIST SP 800-53 standard was a simpler process. Some of the controls in NIST SP 800-53r5 were categorised as both organisational and security. These controls or control enhancements that can be implemented by an organisation, a system, or a combination of the two and are specified by an o/s. This is to alert the developers that can be implemented at an organisational or system level. These controls were included as they supported technical application in development. The second KWS included the privacy properties. This extended the framework properties from eight to fourteen and added the additional key words for the search. The added key words were: Undetectability, Unobservability, Content awareness, Plausible deniability, Consent, Identifiability, Identifier, De-identification, Deniability, Unlinkability, Unawareness, Pseudonymity and Sanitization. This expanded the initial controls extracted from 104 to 485. Many of the controls corresponded throughout the framework properties. The controls were categorised according to the framework properties by the researcher during the extraction process and validated during the internal and external validation.

4.6.4 Evolve the Method

Figure 4.40 outlines the DFSPCs progression in cycle 4.

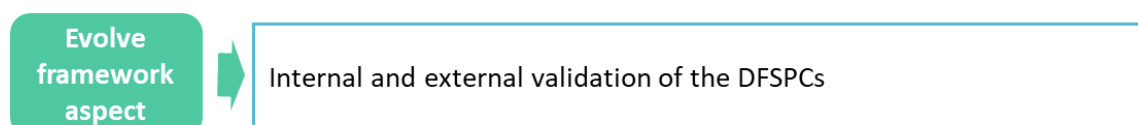


Figure 4.40 DFSPCs progression in cycle 4

Chapter 4 Development of the Framework

The controls determined by the researcher that met the criteria for the DFSPCs were carried forward for an internal and external validation. The internal validation process was completed by experts embedded in the Regulated Software Research Centre. The experts have diverse specialities within the domains of medical device standards, app development and security. The internal validation process also served as a “dress rehearsal” for the external validation process. It provided the opportunity to correct any lack of clarity and expectations in the security controls validation process. Each internal validator was provided in advance of a focus group:

- The carried forward controls per standard with links to a description of each of the controls;
- The DFSPCs criteria;
- The framework properties and threat types with definitions and descriptions, Table 4.2 provided in section 4.5.3 above.

The internal validators were tasked with pre-establishing the controls for inclusion and exclusion in the DFSPCs before the focus group. Each validator sent their conclusions to the researcher. The researcher assembled the individual conclusions for presentation at the focus group. The focus group firstly agreed on the controls that should be excluded and included as DFSPCs. Secondly, the focus group confirmed the framework properties each control would reside in. This information was collated by the researcher and sent to the external experts for validation.

The external validation was completed when the researcher met individually with the app developer and security experts and then the CTO and security champion of a medical device software development organisation. The external validators were sent the same information as the internal validators. They were also sent the collated results of the internal validation process. The researcher met with the experts individually to discuss their conclusions and confirm the DFSPCs choices and their categorisation into the framework properties. On conclusion the researcher distributed the final set of categorised controls to the external validators.

4.6.5 Action

Figure 4.41 outlines the action taken in cycle 4.

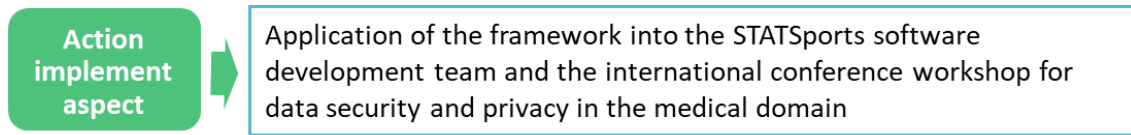


Figure 4.41 Application of the DFSPCs in cycle 4

The DFSPCs were introduced to the STATSports software development team. The introduction included a presentation to the software development team. The presentation was followed by a discussion session. The software development team understood the relationship of the threat types to the framework properties and the threat to attack types. There was discussion around the overlap of some of the threats to attacks and threats to framework properties. The conclusion was that it was important to consider all of the threat and framework properties overlaps because the threat mitigation for the individual framework properties may be different. The DFSPCs were added to the framework Excel document. The software team then applied the DFSPCs to the development project. The DFSPCs were also implemented as part of the framework in the 26th EuroSPI Conference Workshop *Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT*.

4.6.6 Evaluate Experience

Figure 4.42 outlines the evaluation in cycle 4.

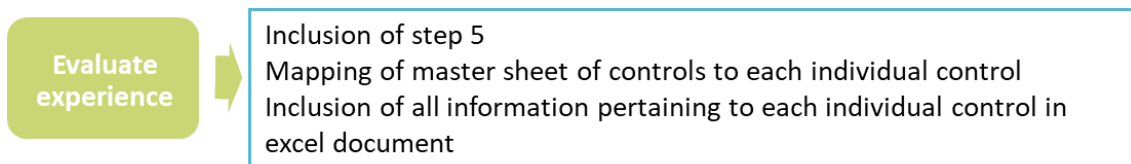


Figure 4.42 Evaluation supplied in cycle 4

The internal and software team evaluation of the Excel document and the DFSPCs resulted in a number of adjustments of the Excel document. The process of searching through the individual standards to find the selected control was deemed arduous and time consuming. Subsequently, the researcher provided an individual sheet for each DFSPC. In addition, the researcher provided a link from the master DFSPCs sheet to each individual control sheet. Also, within each DFSPC sheet, the researcher provided a corresponding link back to the master sheet. The researcher also provided links

throughout the Excel document back to the other applicable sheets. Adding the links assisted in the use of the Excel document.

The software team also, were not clear on how to map the attacks back to the framework properties. The researcher introduced step 5 to clarify mapping the attacks back to the threat type, back to the framework properties. This was completed as the DFSPCs are categorised to the framework's properties. The developers could then review the controls in the framework property category to identify a suitable control or controls to mitigate the threat in step 6. This mapping from attack to DFSCs process is presented in Figure 4.43. Step 5 was added to the documentation process in the master framework risk evaluation table in the Excel document.

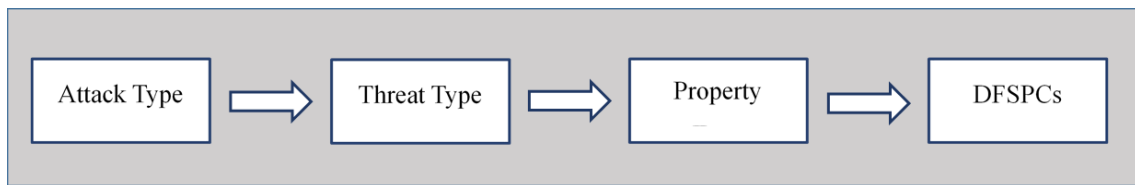


Figure 4.43 Mapping from attack to DFSCs

4.6.7 Assess Usefulness and Exit

Cycle 4 assessment of usefulness and exit is outlined in Figure 4.44.

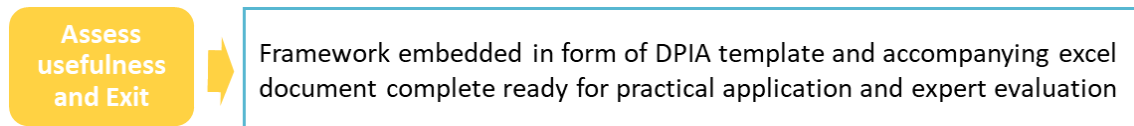


Figure 4.44 Cycle 4 assessed usefulness and exit

On completion of this research cycle the draft DPIA template and accompanying Excel document were assessed as ready for implementation into the software development project. The software team had a good understanding of the framework because of their interaction in its development. The framework in this form of the DPIA template and accompanying Excel document was prepared to send to the external expert for validation.

4.6.8 Report Research Results

The reported results from cycle 4 are presented in Figure 4.45.

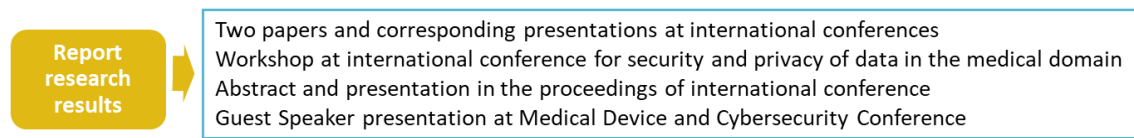


Figure 4.45 Reported results from cycle 4

The researcher presented papers at two international conferences.

- 1 Treacy, C., Loane, J. and McCaffery, F. (2020a). A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In: Messnarz, R. et al., eds. *Systems, Software and Services Process Improvement: 27th European Conference, EuroSPI 2020*. Springer Nature, pp.107–119.
- 2 Treacy, C., Loane, J. and McCaffery, F. (2020b). Developer driven framework for security and privacy in the IoMT. In: *ICSOFT 2020 - Proceedings of the 15th International Conference on Software Technologies*. Springer, pp.443–451.

The framework was developed as a workshop for the 26th EuroSPI Conference.

Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: *26th EuroSPI Conference*. Edinburgh: Springer.

The researcher was invited to deliver an abstract and present the research at the 4th International Clinical Engineering and Health Technology Management Congress. Treacy, C., Loane, J. and McCaffery, F. (2021). Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things. In: *4TH International Clinical Engineering and Health Technology Management Congress (ICEHTMC)*. Lake Buena Vista, FL: AAMI.

The researcher was also invited as a guest speaker to present the research at the Annual European Medical Device Cybersecurity Conference. Treacy, C. and McCaffery, F. (2021). Assisting Software Developers to Meet GDPR Data Protection and Privacy Requirements for their IoMT Products. In: *2021 European Medical Device Cybersecurity Virtual Conference*. TT Group.

4.7 Summary

This chapter presented the development of the framework, which relates to research sub-question 3 and research objective 4.

<p style="text-align: center;">RSQ. 3 What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?</p>	<p style="text-align: center;">RO. 4 Development of a security and privacy risk assessment framework to assist software developers to demonstrate compliance with the GDPR data protection requirements in the IoMT.</p>
---	--

The framework was created to meet the requirements of a DPIA. These requirements were established from the GDPR, ISO/IEC 29134:2017 and guidelines provided by the EU Article 29 Data Protection Working Party and the Irish Data Protection Commission. The information in the document provides extensive guidance and links to address the disparity of understanding and knowledge required to meet the requirements of a DPIA. In addition, the DPIA contains all of the components to assist inexperienced software developers implement a security and privacy risk assessment in software development to meet the GDPR data protection requirements.

The framework was developed over four research cycles. Cycle 1 defined the problem within the requirements of STATSports, through a literature review and with expert security developer participation. The findings from this cycle provided the basis for the development of the proposed framework. This cycle also established STATSports GDPR compliancy readiness, both organisationally and in their products. This cycle significantly contributed to the STATSports ISMS and obtaining their ISO 27001 certification.

The information gathered in cycle 2 was used to build on the basis of the GDPR data protection principles to provide the outline of the DPIA template. This included the development of the STATSports' privacy policy, collecting consent for use of personal data and the GDPR data protection requirements the framework must meet. This cycle was complete in collaboration with the STATSports solicitor firm, expert security developers and the STATSports software development team.

The information gathered in cycle 3 was used to develop the framework properties to defend the GDPR data protection principles. To meet the risk assessment requirement for a GDPR compliant DPIA, threat modeling was established as a suitable model for use in the software development process with the assistance of the security experts. The NIST

Chapter 4 Development of the Framework

SP 800-30 risk assessment scales and tables were applied in the framework. NIST SP 800-30 was used because it is endorsed by the FDA and the AAMI TIR 57 guidance for use in software development risk assessment. When the framework was implemented in the workshop during the 26th EuroSPI Conference the participants struggled to link the framework threat types to real world attack situations. This problem was corroborated by an additional literature review and feedback from the STATSports software team. In response, the researcher developed the threat to attack type resource library starter kit.

Cycle 4 included the development of the DFSPCs. The researcher developed the DFSPCs. The DFPCs were validated internally by experts within the RSRC and externally by the security experts and the CTO and software development security champion of a medical device software development organisation. The STATSports software team supported improving the process of mapping the appropriate DFSPC to threat and subsequent attack type in the framework Excel document. The framework development concluded in this cycle.

It should be noted that the research cycles were completed in parallel with each other. Various aspects developed in an individual research cycle, was influenced through the evaluation from other cycles. At this stage the framework is based upon the research conducted, the requirements for STATSports and expert input and is purely theoretical. Further validation of the framework was completed in two ways. The framework was implemented into a software development project within STATSports, which takes the framework from theoretical to the pragmatic. In addition, to increase confidence in the framework, validation from experts in the domains of software security and privacy would be beneficial. Consequently, an international expert in the field of security and privacy in software development was approached to review the framework. This validation is outlined and discussed in the next chapter.

5 Validation of the Framework

5.1 Introduction

This chapter describes the approach taken to validate the framework, how the approach was implemented and the results. The validation of the framework discussed in this section was used to address RSQ 4.

RSQ 4: To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?

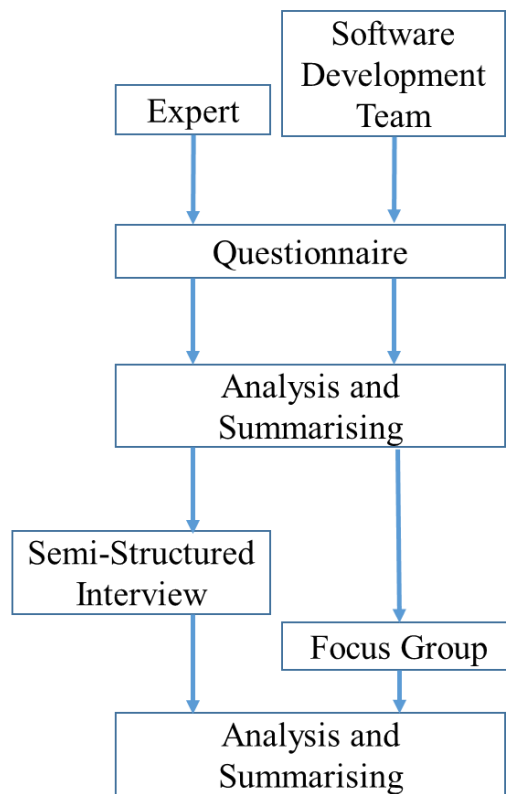


Figure 5.1 Steps of validation

The steps of the validation are presented in the diagram in Figure 5.1 above. The diagram shows that both the expert and software development team completed the questionnaire first. The researcher analysed and summarise the returned questionnaires. The semi-structured interview with the expert was completed and analysed before the focus group was conducted. The researcher used some of the feedback from the semi-structured interview with the expert to develop some of the questions for the focus group. On conclusion of the steps the researchers analysed and summarised the findings.

This validation stage was used to establish if the framework addresses the difficulties encountered by inexperienced software developers in SMEs inexperienced in implementing security and privacy for data in flow in the IoMT. The validation of RSQ. 4 was accomplished by completing RO. 5 and RO. 6, outlined in Figure 5.2 below.

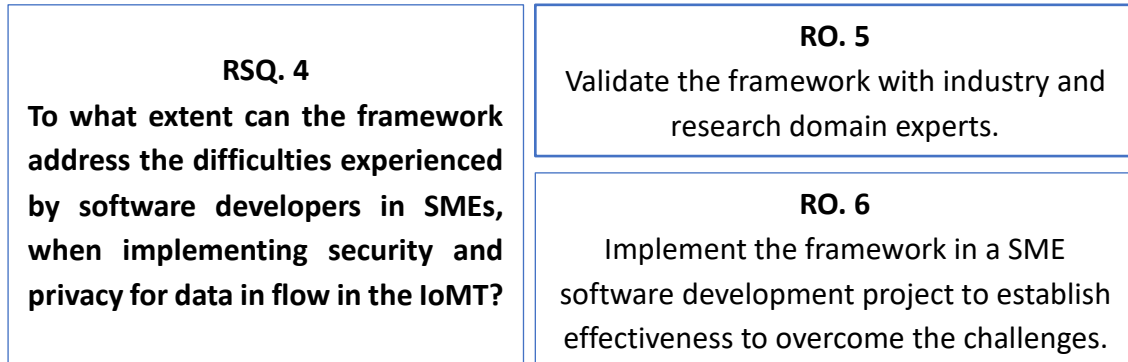


Figure 5.2 RSQ. 4 and RO. 5 and RO. 6 validated in chapter 6

To increase confidence in the framework, a review of the framework was performed by an international expert in the privacy threat model LINDDUN, (RO. 5). In order to validate the framework's effectiveness within its intended environment it was also implemented in a new software development project in STATSports (RO. 6). The implementation of the framework by the software development team is described in section 5.8 below. This implementation was overseen by the researcher and driven by the software architect within the STATSports software development team. While the validation presented in this section is used to address RSQ. 4 and its two related objectives, each stage of the development of the framework contributed towards the validation. At each stage of the development, the framework was updated, where appropriate, in line with the feedback received and prepared for the next stage of development and validation. This is in keeping with the AR approach used for the research. This is reflected in the development of the framework, as discussed in chapter 4. At this point in the validation, the software team were comfortable with the framework and providing feedback for validation. Data collection was completed through interviews guided by a questionnaire. Rabionet's (2011) six stages for the development of qualitative interviewing were followed for this research and are:

1. Selecting the type of interview;
2. Establishing ethical guidelines;
3. Creating the interview protocol;

Chapter 5 Validation of the Framework

4. Conducting and recording the interview;
5. Analysing and summarising the interview;
6. Reporting the findings.

This validation chapter will follow these stages and will be discussed in the following sections. The questionnaire presented in chapter 3 was used as the basis for conducting the interviews. The questionnaire sits within stage 3, creating the interview protocol. The questionnaire was developed in line with the questionnaire development process outlined in chapter 3 (section 3.8.1). Stages 4-6 will be discussed in the context of the SSI with the international expert and the focus group interviews with the STATSports software development team.

5.1 Stage 1: Selecting the Type of Interview

Selection of the type of interviews used for this study were outlined in chapter 3 (section 3.8.3). This section provides the motivations for choosing these types of interviews for this study.

5.1.1 Semi-structured Interview

The SSI was chosen to collect qualitative feedback data from the international expert to partially answer RSQ. 4 and fulfill RO. 5.

RO 5: Validate the framework with industry and research domain experts.
--

As discussed in chapter 4, the experts from industry provided validation of the components of the framework and the development of the DFSPCs. The aim of the SSI was to elicit feedback grounded in the experience of the research expert. The feedback related to the value, composition, and usability of the framework. A completely unstructured interview had the risk of not eliciting, the areas or issues more closely related to the research questions under consideration, from the expert. The SSI allowed the researcher to narrow down some areas and issues to ask the expert. Using the SSI allowed the researcher to make sure that they got answers to their research questions. To ensure the interview remained aligned with the aims of the research, a questionnaire was used to motivate the SSI discussion. Using the questionnaire in the SSI facilitated focus on the research by selecting questions to guide feedback on the value, composition, and usability of the framework. The SSI also facilitated a considerable degree of latitude for both the researcher and expert to answer questions and ask follow up questions. This facilitated

the inclusion of additional unscripted questions to probe for unforeseen information. Incorporating the questionnaire into the SSI assisted the researcher to prepare for the interview. The questionnaire also supported the international expert to prepare for the SSI, as it established the topic under study (Galletta 2013).

5.1.2 Focus Group Interviews

The focus group method was chosen to collect qualitative feedback data from the software development team to partially answer RSQ. 4. The focus group was also conducted to provide qualitative feedback data from the software developers on the implementation of the framework and answer RO. 6. The feedback was to review how the framework assisted with the challenges STATSports communicated and revealed through the literature review including: where to start, lack of knowledge of GDPR regulation and standards, difficulty applying standards to demonstrate compliance, lack of knowledge and experience in security and privacy risk management, application of controls to mitigate threats to security and privacy and what to include and how to demonstrate compliance in software systems to the GDPR data protection requirements, a DPIA.

RO 6: Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.

Focus groups were the ideal way to facilitate the members of the software development team to have an open discussion about the framework and its implementation. This approach is useful for the research because it is a fast and cooperative method to obtain experiences from the developers. In addition, it can deliver content rich, qualitative information and reveal insights that are difficult to obtain with other methods (Kontio et al. 2004). The aim of the focus groups was to gather feedback and usability experiences from the software development team in a group activity. The final focus group discussed in this chapter, concentrated on opinion and feedback on the framework's value, composition, and usability from the developers' perspective. This final focus group considered the feedback received from Dr. Kim Wuyts' expert review.

5.2 Stage 2: Establishing Ethical Guidelines

Stage two, establishing the ethical guidelines, was the same process for all the data collection methods of this study. As said by Dawson, *“As researchers we are unable to conduct our projects successfully if we do not receive the help of other people. If we*

Chapter 5 Validation of the Framework

expect them to give up their valuable time to help us, it follows that we should offer them something in return” (2009, p.149). This was an important consideration in this research, as conducting interviews intrudes both on people’s lives, and on the organisation. The researcher considered and provided the following ethical guidelines prior to starting the research project:

- Dundalk Institute of Technology mandates that all research requires approval by the ethics committee. The researcher completed Dundalk Institute of Technology’s Ethical Application Form and the project obtained ethical approval. The ethical approval covered the participant informed consent and information form, and the themes to guide the SSI and focus groups.
- The researcher is embedded in the organisation and because of such personal involvement it was important to consider the risks and particular ethical issues associated with this. The researcher presented the organisation with the following conditions and guarantees:
 - The researcher would keep STATSports up to date throughout the project;
 - All information to be published will be approved by STATSports. STATSports may decide they have revealed more about their organisation than they are prepared to share publicly;
 - STATSports will receive a copy of the final report;
 - All participants will remain de-identified;
 - All information will be treated with the strictest confidentiality;
 - STATSports have a stake in the improvement, development and implementation of the framework and are encouraged to shape and form the work;
 - The software team participants will have the opportunity to verify statements when the research is in draft form.
- The international expert was provided with an expert review pack that included:
 - The framework and accompanying Excel document (version on completion of the development process discussed in chapter 4);
 - Participant information leaflet;
 - Participant consent form;
 - Questionnaire;

- Copy of the standards used for the development of the DFSPCs.
- The expert was also provided with a copy of their statements used when the research was in draft form to provide them the opportunity to verify their statements.

5.3 Creating the Interview Protocol

The researcher used the interview protocol refinement (IPR) framework presented by Castillo-Montoya (2016) to create the interview guide. The IPR provides a systematic framework for developing and refining interview protocols (Castillo-Montoya 2016). This approach was used to strengthen the reliability of the interview protocol for this study. This approach ensured the interviews were anchored in the purpose and aims of the research (Jones et al. 2014). This in turn ensured the interviews provided quality feedback to accomplish RSQ. 4 and research objectives 5 and 6. The IPR consists of a four-phase process, which includes:

1. Ensuring interview questions align with research questions;
2. Constructing an inquiry-based conversation;
3. Receiving feedback on interview protocols;
4. Piloting the interview protocol (Castillo-Montoya 2016).

5.3.1 Ensuring Interview Questions Align with Research Questions

This phase concentrates on *the alignment between interview questions and research questions* (Castillo-Montoya 2016, p.812). The researcher used a questionnaire to guide the interviews. The questionnaire enabled intentional and necessary interview questions to ensure the interview questions aligned with the research question and objectives. Even though there are some specific areas that the researcher would like covered, at the same time I wanted to hear the expert's opinions and feedback.

This approach was shaped by Seidman who stated:

“The purpose of in-depth interviewing is not to get answers to questions... At the root of in-depth interviewing is an interest in understanding the lived experiences of other people and the meaning they make of that experience.... At the heart of interviewing research is an interest in other individuals' stories because they are of worth.” (2006, p.9)

The questionnaire was developed in line with the questionnaire development process outlined in chapter 3 (section 3.8.1). The questionnaire with the review information leaflet is available in Appendix A The researcher used a question protocol matrix that

encompassed the RSQs. The matrix mapped and aligned the questionnaire questions to the RSQs. This was completed to ensure that the questions aligned with the research aims. A sample of this matrix is presented in Table 5.1 below. The full mapping is available in Appendix B

The questionnaire incorporated both more theoretically driven and open-ended key questions and was a starting point for the development of the interview protocol. This ensured the researcher asked questions to gain specific information related to the aims of the research (Patton 2015). The questions were designed to provide feedback on specific areas related to the framework. These areas were chosen as they had been identified as challenges that the framework would need to address. These areas provided the source for the overall research question and research sub questions.

Table 5.1 Sample matrix for mapping the steps and components of the framework to the research questions

Questionnaire Question	RSQ 1	RSQ 2	RSQ 3	RSQ 4
Value				
In your opinion is there a gap for a specific individual implementation process for both security and privacy for SMEs and inexperienced developers in this domain?	X			
In your opinion is there a gap in explicit guidance for inexperienced SMEs and developers in the application of both security and privacy in software development within regulatory requirements?	X	X		

5.3.2 Constructing an Inquiry-Based Conversation

Castillo-Montoya (2016) refers to an inquiry-based conversation in interviewing, which is the need for balance between inquiry and conversation. An inquiry-based conversation for this SII was appropriate because it allowed the interviewer to gather more detailed and relevant information from Dr. Wuyts. It facilitated asking open-ended questions that could encourage Dr. Wuyts to share her experiences and reveal her knowledge, skills, and attitudes and apply these to the framework. In emails to coordinate the SSI with Dr. Wuyts, she suggested she would provide comments on the framework as she worked through her review. The researcher agreed, as this would provide additional content for an inquiry-based conversation directly from the experience and knowledge of the expert. There was no need to ease into the interview process as the researcher and expert had developed a rapport. When designing the questionnaire, the researcher took this into

Chapter 5 Validation of the Framework

consideration. The initial section of the questionnaire gathered information about the expert to profile her experience. This was to demonstrate her expertise in this domain to substantiate her inclusion.

It was not necessary for the researcher to build a rapport with the software team because they had been working closely over the development and implementation of the framework. Therefore, the initial section of the questionnaire gathered information about the participants of the focus group to provide the background of the focus group. The questions for the software development team focus group were developed by the researcher:

- From identified categories of the challenges found by the researcher through the literature review and understanding the needs for STATSports. These categories are listed in Table 5.2, overleaf. There were numerous themes within each category;
- To target and encourage discussion on certain aspects to answer the research questions and objectives;
- To target certain key aspects guided from the expert review;
- From the completed and returned original questionnaires from the software development team, before the final focus group took place.

Table 5.2 Questionnaire categories developed to themes for developing interview protocol

Questionnaire Categories	Themes	Code
Value	Challenges with security and privacy Security and Privacy in software development Guidance Needs Regulatory knowledge Regulatory requirements Risk assessment Risk assessment practices	Se/Pr Gu Reg V-RAs
Composition	Composition Obstacles Threats and attacks in security and privacy Threats understanding and knowledge Risk assessment Security and privacy controls	C-Ob Th C-RAs CTRL
Usability	Usability for SME software developers inexperienced Generalisability of framework Usability obstacles <i>How To/Improvements</i> <i>Benefits</i> <i>Developers Insights</i>	Use Gb U-Ob <i>HT/Im</i> <i>Ben</i> <i>Devs</i>

The researcher used the question protocol matrix that included the RSQs and aligned them to the questionnaire categories to develop further interview questions. This is the sample matrix mapping presented in Table 5.2, with the full mapping available in Appendix B. The researcher constructed questions in each of the topic areas as well as taking into consideration the answers from the returned questionnaires. The questions were kept open ended and short to encourage an inquiry-based conversation. The interview process moved through the questions in the questionnaire mapped to the research aims. The researcher aimed to promote an inquiry-based conversation based on the answers to the questions. The researcher listened to replies to ask follow-up questions based on the categories and identified themes. The researcher returned to the questionnaire to ensure the conversation was kept in alignment with the research aims.

5.3.3 Receiving feedback on interview protocols

The interview protocol was reviewed by two members of the RSRC and an academic researcher outside the RSRC. The RSRC members have extensive experience and expertise in software development, research and in developing interview protocols. The reviewer outside the RSRC is an academic researcher with extensive experience and expertise in research and in developing interview protocols. Each of the reviewers were provided with a draft copy of the:

- Participant information leaflet;
- Consent form;
- Questionnaire;
- Proposal on the distribution and timeframes for conducting the interviews.

The reviewers were asked to comment on how well the interview protocol fulfilled its purpose and to ensure that it did not contain ambiguity. There were two discussion meetings with the reviewers. The first provided initial feedback and the second agreed that all requested changes had been completed. The first session included discussion on grammatical corrections, the purpose of the questions and if they achieve their purpose. This led to the researcher reworking of some questions. The second session discussed the changes and after this session through a general consensus, it was agreed that it was not necessary to make any further changes.

5.3.4 Piloting the Interview Protocol

The interview protocol was piloted with a RSRC researcher with software development experience. The RSRC researcher was provided with the interview pack, which included:

- Research acknowledgement and questionnaire;
- DPIA template;
- DPIA accompanying Excel document;
- Three international standards – used for the DFSPCs:
 - NIST SP 800-53 r5;
 - ISO/IEC 15408-2;
 - IEC 62443-3-3.

The reviewer was asked to return the questionnaire before the discussion meeting with any comments. The pilot interview and discussion were conducted on Teams. The interview was completed without any misunderstandings, difficulties, or confusion. There were some formatting differences due to different versions of word between the researcher and the reviewer. The time to complete the questionnaire and pilot interview was approximately one hour. However, the time allowed for the interviews was extended to 90 mins. This time extension allowed time for discussion.

5.4 Conducting and Recording the Interview and Focus Group

All interviews were conducted over Teams and recorded. All participants had agreed to the recording prior to the commencement of the interviews. The interview participants were supplied with the questionnaire before the interviews took place. The participants agreed to the return the questionnaire two days before the interviews were scheduled. The returned questionnaire would include feedback, opinions, and areas they consider need further discussion. This was done to:

- Provide the researcher the opportunity to review the feedback before the interviews and to consider any follow up questions;
- Provide the opportunity for the expert to familiarise herself with the framework before taking part in the interview;
- Familiarise the participants with the requirements of the questionnaire before taking part in the interviews;
- Provide participants time to consider their opinions and feedback;
- Provide time for the participants to consider areas for further discussion;

- Enable participants to provide their follow up questions if they chose before the interviews.

During the interviews the researcher also made notes. In the case of the expert the comments were added to the commented word framework template returned from the expert. The researcher and expert had agreed to begin the review of the framework by moving through her comments in the document. The researcher considered that many of the questionnaire questions would be addressed in completing the review this way. This approach provided additional content for an inquiry-based conversation. On completion of reviewing the comments the researcher and expert examined the questionnaire. This was to ensure all the research aims were included in the expert review.

This chapter also details the final focus group on implementation of the framework. Previous focus groups which took place during the framework development and implementation, are discussed in chapter 4. These focus groups were to establish an understanding of the framework and how to implement it. At this stage of the validation the software team were very familiar with the components of the framework. The software team were provided the interview pack. It was agreed that the questionnaire would be completed by the software development team before the final focus group, and these would be returned to the researcher. This would give the researcher time to analyse their feedback and develop any further follow up questions. The researcher took notes during this focus group.

5.5 Analysing and Summarising the Interview

The researcher considered that the time involved and method chosen for analysing the interviews depended heavily on the number of people interviewed and the number of topics addressed (Adams 2015). Therefore, the approach to the SSI and the focus group was different. The analysis and summarisation of the SSI with the international expert was not complicated. The SSI analysis was completed by moving through the expert's commented document while listening to the recorded interview. The researcher pulled out and analysed comments from the expert whilst transcribing the interview. These comments were aligned to the categories of the questionnaire, value, composition, and usability. Many of the comments overlapped the categories and the researcher grouped the comments into the appropriate category when writing up the review. The researcher made notes alongside the expert's comments to categorise them. Additionally, at the end of the SSI the researcher and expert examined the questionnaire to consider any gaps in

the areas the researcher wanted to discuss. This provided an informal mapping back to the questions in the questionnaire. This helped the researcher to analyse and summarise with focus on this specific study (Barbour 2008).

Analysing and summarising the focus group interview included transcribing the interview. This resulted in large amounts of data with similar ideas in different locations of the text and contained content unrelated to the study. Qualitative content analysis (Mayring 2000), was used to structure the interview data so it could be analysed and summarised. It was completed to reduce the material to help gain meaningful conclusions. The main procedure was the formulation “*of a criterion of definition, derived from theoretical background and research question*” (Mayring 2000, p.162). As outlined in section 5.3.2 above, the categories came from the objectives of the research.

As described in section 5.3.1, the questionnaire questions were mapped to the RSQs. The researcher continued this mapping for the focus group follow up questions to produce an interview protocol matrix. The interview protocol matrix questions were mapped to the RSQs and the ROs. The interview matrix protocol is available in Appendix E. During the analysis some new themes emerged, which were How To/Improvements (HT/Im), Benefits (ben) and Developer’s Insights (Devs). HT/Im was as a result of the expert review, which will be discussed in section 5.6.2.3. The other two themes and codes emerged from the focus group text itself. This is supported by Cohen et al. (2005), where they state to be true to the data, codes themselves should arise from the data rather than being absolutely decided in advance. These new themes are presented in italics in Table 5.2. The new themes were added as a means to obtain rich feedback from the developers on how best the framework could be presented to meet their needs. As the focus group generated considerable data that crossed the categories, the themes were coded and labelled to allow the grouping of several statements under one idea so as to limit the number of codes (Flick 2008). The researcher used the codes over iterative readings of the transcript of the focus group interview to help with grouping statements into themes for analysis. These codes are presented in Table 5.2 above. The transcript was annotated on each reading with the codes until no new text for coding emerged. The key findings from the software development team were formed from this procedure.

5.6 International Expert Review

This section describes the findings of the expert review with Dr. Wuyts. It also reports on the modifications made as a result of performing this review process. The expert review was performed as part of the validation to complete RO. 5.

RO 5: Validate the framework with industry and research domain experts.

The validation was a part of the action taking and evaluating stages of this action research to address RSQ 3 and RSQ 4, outlined in Figure 5.3.



Figure 5.3 Validation as part of action taking and evaluating stages of this action research

Three weeks before the interview was scheduled Dr. Wuyts was provided with the expert review pack, itemised in section 5.2. This lead time provided ample time for Dr. Wuyts to review the framework, accompanying documents and to complete the questionnaire. The agreement stated that the questionnaire would be sent back to the researcher two days before the scheduled interview. This provided the researcher sufficient time to analyse the completed questionnaire and to derive further questions from the responses. The transcript for the expert review SSI is in Appendix F. The quotes used in this discussion section are highlighted yellow in the appendix transcript.

5.6.1 International Expert Biography

Dr. Wuyts was instrumental in the development and extension of the privacy-by-design framework LINDDUN. LINDDUN was developed and empirically validated during her PhD. LINDDUN was the privacy threat model adapted by the framework. Dr. Wuyts has more than 10 years' experience in security and privacy in software engineering and her specialties include: threat modeling, privacy engineering, security engineering and data protection. She has published extensively on threat modeling and its adoption for privacy-by-design and security when developing software. Dr. Wuyts is currently a postdoctoral researcher at the Department of Computer Science of the Katholieke Universiteit Leuven,

Belgium. She is a member of the Security: Development processes And Middleware taskforce of the DistriNet Research Group and the working group of the Threat Modeling Manifesto. Dr. Wuyts was program co-chair of the 2021 International Workshop on Privacy Engineering – IWPE’21.

5.6.2 Findings

The questionnaire was returned to the researcher two days before the interview. Dr. Wuyts had also made notes on the framework template document during her review. The commented version was emailed to the researcher just before the commencement of the interview. The researcher decided that the first part of the interview would involve a review of the commented document. This approach was used since the researcher in reviewing the comments, recognised that many of the comments related to the questions found in the questionnaire. The researcher grouped the review findings according to the categories of the questionnaire, value, composition, and usability. The review findings overlapped through these categories.

5.6.2.1 Findings – Value

The SSI questions sought to establish if the expert saw if the framework added value to the domain. Questions 1.1-1.4 from the first part of the questionnaire focuses on the expert’s opinion on the gap for a tailored process for developers inexperienced in security and privacy, meeting the GDPR data protection requirements. The questions take into consideration the challenges this presents and how the framework does and does not meet the challenges. These questions were based on addressing the RSQs. 1 and 2 and ROs. 1, 2 and 3 defined in Figure 5.4. The RSQs. mapping to the questionnaire is presented in Appendix B

<p>RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?</p>	<p>RO. 1 Investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs when implementing the requirements.</p>	<p>RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.</p>
<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>RO. 2 Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.</p>	

Figure 5.4 RSQs and ROs mapped to questionnaire questions 1.1 – 1.3 analysed in value

Chapter 5 Validation of the Framework

Questions 1.4-1.8 focus on the benefits of the guidance and processes provided in the framework for developers inexperienced in security and privacy meeting GDPR regulatory requirements. The questions consider in depth the adequacy of the framework processes and what improvements or changes the expert would recommend. These questions were based on addressing the RSQs. 2, 3 and 4 and ROs. 2, 3 and 6 outlined in Figure 5.5 below.

<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>RO. 2 Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.</p>	<p>RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.</p>
<hr style="border-top: 1px dashed #000;"/>		
<p>RSQ. 3 What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?</p>		
<hr style="border-top: 1px dashed #000;"/>		
<p>RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?</p>	<p>RO. 6 Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.</p>	

Figure 5.5 RSQs and ROs mapped to questionnaire questions 1.4 - 1.8 analysed in value

The collection of an extensive amount of information into the single framework template was considered valuable by the expert. Dr. Wuyts saw it as a valuable resource for organisations and developers that have no knowledge and experience in the field. The distinction of the framework is that it is focused on the needs of the software development team in SMEs. This domain lacks subject matter expertise, experience and knowledge in the areas referred by the framework. Dr. Wuyts also identified value in having all of this information collected and documented in one place. The advantage being that the information is documented and can be reused or simply referenced again. Dr Wuyts noted *“We have that discussion with some people from industry too that they say, well, documenting this would be such an overhead, and then, but, but you can reuse it.”* For software development projects much of the information in the framework can be transferred knowledge through to other projects.

In addition, the researcher and expert discussed the value for new developers joining the team having this information available to them. It would provide both a reference to the process for security and privacy in development but also as an instructive

tool. Having this framework information documented also lessens the impact of people leaving and moving on. Dr. Wuyts noted *“people move all the time and then the experts leave, and you’re left with nothing”*.

A value to the framework is creating a situation where both privacy and security are addressed on an equal basis. However, Dr. Wuyts emphasised *“so, when I talk about security and privacy, I always say, like, it’s, you can do threat modeling for both and it’s very much the same, but it requires a different mind-set. So, for security, you need the valuable assets for the organisation and for privacy, you need to think of the perspective of the individual, the data subject”*. Part of the discussion focused on this mind-set and ensuring that it is obvious for the framework user. The researcher agreed the importance of this mind-set and added a sentence to the framework to underscore the difference required in approaches for security and privacy for the user. Dr. Wuyts also referred to *“Potential to have a privacy champion as well as a security champion. Now, I’m thinking from the company perspective, and now, I’m thinking more like if I was a data subject, would I be okay with all these things happening? You are trying to protect, like, all data is valuable because, well, we need it for the company but from, for privacy, it might be different data that is really valuable to the data subject, not that valuable to the company but requires a lot of privacy attention because it’s so valuable to the data subject”*.

The threat to attack type starter kit library was seen as a strength for this type of approach. Dr. Wuyts suggested it was a particular strength *“especially for people new to it”*. The depth *“is all that background information”*. The literature, experience with academia through a workshop and feedback from developers, has revealed that there is a deficiency in mapping a threat category to a particular attack that exploits a vulnerability. This lack of understanding and knowledge hinders the ability to think systematically and complete threat modeling. Dr. Wuyts noted that the threat to attack type starter kit library provides strength for the user *“because, well, you can say now, think about it systematically if you don’t know what to think about’, and you’re lost”*.

When considering the approach of the framework in combining security and privacy Dr. Wuyts reasoned that privacy is currently being done because it is now legally required. Her opinion is that privacy is therefore, managed more *“by the legal people and then somehow push those requirements to the developers”*. Dr. Wuyts maintains that for security it is coming more from development and so the developers. In addition, she contends the companies still want all of the data they can get. *“Companies are not ready to, to say, like, well, maybe we don’t need that data unnecessarily and it’s okay”*. In Dr.

Wuyts' opinion, this appears that the companies are *“doing compliance and not doing privacy because, well, they want to do the bare minimum to not get fined and not do privacy because that's something they should be doing”*. This framework approach brings both privacy and security to the developer.

In step 2 of the framework, Table 9 provides for the documentation of the already known decisions or constraints in relation to security and privacy in development. As discussed in the literature review and chapter 4, these decisions or constraints would be due to common issues for SMEs. Issues such as talent and skills capability within the team and platforms or software the organisation is already tied to. Dr. Wuyts saw value in step 2 Table 9 that documents already known decisions or constraints for the software development team. This discussion arose due to her confusion on the value of the table, outlined in section 5.6.2.2 below. With further clarification around the purpose of the table Dr. Wuyts responded *“it's already maybe sometimes also solutions that are already in place and that can influence the outcome, okay. Yeah, that makes sense”*. Where the developers have either had previous experience they can reuse, or there are already known security or privacy solutions with the tools, platforms or software being used that can be applied. Also, simply understanding that there are security and privacy solutions available to draw from with the tools, platforms or software being used, is an advantage to developers and SMEs.

One of the advantages applied by the researcher for using the per-interaction approach was that it was perceived as less time consuming. Dr. Wuyts stressed *“It is incorrect to say that it is less time consuming, as you will be looking at the same components”*. Dr. Wuyts is a colleague of Laurens Sion one of the authors referenced for the researcher's claim. Dr. Wuyts discussed my assertion with Laurens Sion, and he noted that it would be incorrect to assert that per-interaction is less time consuming. In the discussion with the researcher, Dr Wuyts concluded *“Well, there are advantages definitely of per-interaction because it's, it's more intuitive, definitely, but I'm not sure whether it will be less time consuming and exhaustive”*. The researcher agreed to modify her assertion that using per-interaction is less time consuming. The researcher instead considered Dhillon's (2011) and Shostack's (2014a) experience. Dhillon noted about their early experience using STRIDE that the developers found analysing each individual element in the DFD *“time-consuming and redundant and began focusing instead on analysing interactions”* (Dhillon 2011, p.43). Shostack (2014a, p.80) maintained that per-interaction is a *“simplified approach to identifying threats, designed to be easily*

understood by the beginner". The motive for using per-interaction after discussion with Dr. Wuyts and considering the experiences of Dhillon and Shostack, is this approach is more intuitive for inexperienced developers to complete TM.

Additional value noted by Dr. Wuyts were the links into the security and privacy standards based in both these wider domains but also previously applied in the medical domain. The framework has collected all of this information, which helps SMEs and developers with little to no experience or knowledge. They will not have this steep learning curve because this aspect has been provided by the framework.

5.6.2.2 Findings – Composition

The questions in this section sought to establish the expert's opinion on the composition of the framework. The questions based in this section of the questionnaire were developed to determine the expert's opinion on the framework steps, processes, documentation, and guidance. The researcher wanted to determine if these framework aspects were suitable for the purpose of the framework and the domain. The questions are driven to consider how the framework does and does not meet the tasks. These questions were based on addressing all RSQs. and ROs. 3, 6 and 5, defined in Figure 5.6 overleaf. The RSQs. mapping to the questionnaire is presented in Appendix B .

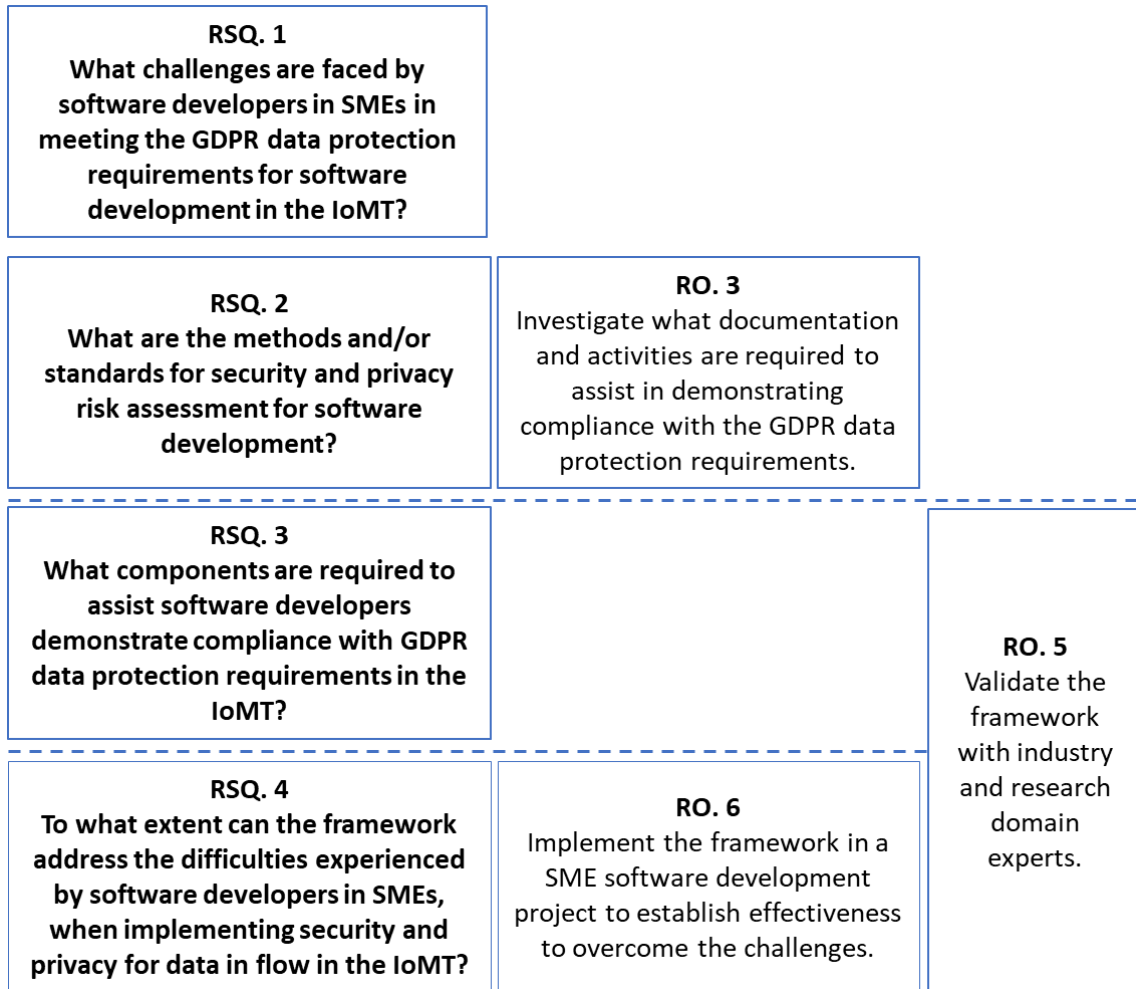


Figure 5.6 RSQs and ROs mapped to questionnaire questions analysed in composition

Overall, the composition of the framework was deemed acceptable as it is based in established threat models and risk assessment processes. There were recommendations on the structure and wording for parts of the framework.

In step 1 Dr. Wuyts recommended clarity in relation to the development of the privacy policy. Dr. Wuyts expressed that drafting a privacy policy in one of the first steps seems like you are doing it too soon. This is because the project would still be in the design phase, and *“you are still trying to specify what you are doing and how you will be doing it”*. The question Dr. Wuyts asked at this point was *“Shouldn’t the processing actions and purposes be specified first?”* This would mean the policy is drafted too soon and would have to be revised later on. The researcher reasoned that the introduction on the development of the privacy policy at this stage, was to make sure the developers were thinking about privacy as a concern from beginning the implementation of the framework. The aim is to have privacy as a concern from the beginning, in the design

part. The researcher discussed that the developers need to be concerned about what information is going to be collected. Also, how they will obtain the data subject's consent for processing and where and how you will get the consent. Even before you are looking at your architecture. Dr. Wuyts agreed this was useful, *"because by thinking about it, you are thinking about the general privacy strategy, and you will implement it within the design probably"*.

However, the clarification was needed because to Dr. Wuyts *"it felt to me like this was like the policy you would give out to the user"*. This is not the case as the privacy policy is a process that is continued through the product and data lifecycle. Dr. Wuyts recommended adding a sentence to clarify that it is the beginning and will need to be updated until the product goes live. It would also follow the product and data lifecycle to ensure any changes made in processing the gathered data or collecting new data would trigger a new consent request.

Making GDPR legal requirements, such as data register and processing more explicit in step 1 was discussed. A data register is the documentation of what personal data is being gathered for use in a system and the processes to the data. Dr. Wuyts was not aware of these requirements being included in the framework. She noted *"shouldn't this mean the data register and processes to this data should be more explicit. We have collaborated with a legal department and from what I remember you need a data register. With an overview of what data is being used in the system and what processes and activities belong to the data. These are things I did not get from your document"*. The GDPR legal requirements concerning data registration and processing is included in step 1 of the framework through Table 7 'Lawful processing'. This table was misinterpreted by Dr. Wuyts as concentrating on the technical part and consent. She believed that it did not relate to the legal requirements, *"It felt like an overview of the GDPR articles more for information"*. This table is one of the most important aspects of the framework for the legal requirement of the GDPR. With further discussion about the information required documenting in the table, Dr. Wuyts acknowledged *"that it is definitely related to purpose and the legal stuff I talked about before. I think that this felt like information on GDPR articles. But I think it's the middle column that you want people to do and think about"*.

The conclusion was in step 1 Table 7 'Lawful processing' required elevation in line with its importance for the framework and the requirements of a DPIA from the GDPR. Dr. Wuyts expressed that a DFD would not contain all of the information required for the

legal part of the GDPR. However, having the information captured in Table 7 ‘Lawful processing’ could provide the legal requirements. Dr Wuyts considered the information would need to be confirmed from a legal perspective to ensure it aligned with the GDPR requirements. In addition, the legal regard would have to continue throughout the development project and the data lifecycle taking into consideration any changes in data collection or use. There is validity later in the framework in the documenting of the per-interaction processes because step one will give an overview of what it is, the purposes for gathering the information. The GDPR and privacy requirements will have to be considered in each of the per-interaction processes to make sure that the project is complying with what was outlined and that it all lines up. Dr. Wuyts suggested there would need to be more reference to “*purpose specification and compatibility checks*”. This is a legal requirement to make sure you have all the purposes specified up front for collection and you only process data items for that specific purpose. There could be a per-interaction process appraisal so you can prove that the process complied with the purpose the data was collected for. Dr. Wuyts stated this could be done through a compatibility assessment. The researcher agreed this would need to be defined in the framework. The developers are ensuring the development is in line with the purpose specification.

There were two composition enquiries on the threat categories of the framework. The first related to the merging of the threat categories in the framework. Dr. Wuyts could understand why this is desirable but expressed the necessity that the threats need to be examined from both the security and privacy perspective. A useful standpoint agreed upon was the concept of encouraging both security and privacy champions from members of the software development team. A security or privacy champion would concentrate on their specific area to ensure that it is promoted in the software development process. The concept of encouraging both security and privacy champions for the framework implementation was to be introduced into the template.

In particular Dr. Wuyts could see why repudiation and non-repudiation would be combined. However, she questioned “*I see why you would combine it because it’s the same thing but on the other hand, it’s like the complete opposite. So, I was just wondering, like, why did you combine them and not have non-repudiation...as a different item?*” The argument from the researcher was to make the process as compact and simple as possible. A similar position that supports Dr. Wuyts’ point of view was expressed by a reviewer of a paper submitted by the researcher to Joint 15th International Conference on Software

and System Processes (ICSSP) and 16th ACM/IEEE International Conference on Global Software Engineering (ICGSE) Conference. Dr. Wuyts stressed that *“from a security perspective, you need it. From a privacy perspective, you don’t want it or might not want it.”* Both parties discussed the importance to consider at that point which is the most important aspect, security, or privacy, and what are you trying to do.

However, Dr. Wuyts has never *“came across a situation so far that there is actually a conflict”* between repudiation and non-repudiation. An example provided by Dr. Wuyts was with voting, *“voting when you want plausible deniability about who you voted for. That is completely fine with having non-repudiation about the fact that you voted.”* So, the discussion in the voting example was that you have both, but they don’t conflict *“because they are at different, different data items, different types of information or flows or, or properties.”* Dr. Wuyts further specified that if there was a conflict between the two then, *“you need to revise the entire focus of the project.”* This is *“because I think if you need both, something with strong repudiation and strong non-repudiation features for the same property”*, then there is something missing in the project. The researcher agreed on conclusion of the discussion that repudiation and non-repudiation should be distinct categories. This adjustment would be made through to the categorisation of the data flow security and privacy controls (DFSPCs).

One of the threat categories Dr. Wuyts was undecided about was insecure communication, *“I’m not sure why you need it as a different thing. Isn’t it part of information disclosure because if you look at per-interaction, you have sender, receiver and the flow?”* The researcher described that insecure communication was directly related to the process of the flow of your data. This threat directly relates to how information is communicated over networks and through the software system. This threat specifically considers communication protocols and interoperability of these protocols across different software and Operating System (OS) components and networks of a system. Where information disclosure or disclosure of information considers the potential threat of information being leaked, exposed in every component of a system. Given the framework is focused on security and privacy of data in flow in the IoMT, the researcher reasoned the distinction is needed due to the different vulnerabilities and attacks each threat could present. Dr. Wuyts suggested seeking support for the need for this category from Adam Shostack. The researcher accepted that his opinion would be valuable particularly in shaping the threat category insecure communication to prevent the violation of the security property communication or transport security.

In Step 2 Table 9 was confusing for Dr. Wuyts. The purpose of this table was not clear. The researcher discussed her experience with the SME software development team. They had already known decisions about the development of a new project, due to several factors which included the talent and skills within the team, what the development team had done previously and platforms and tools they are already tied to. This experience also correlated with the literature review. Dr. Wuyts related this to what they would call assumptions. These assumptions would include solutions already in place that can influence the outcome. With particular platforms or software there will be known security and privacy solutions. This could all tie back together potentially into the threat model. Dr. Wuyts saw this as something very interesting, *“but probably out of scope here.”* The researcher agreed that this would be interesting research but, was out of scope for this study. However, the idea is to encourage the developers to draw on the established resources already available to them. The researcher decided to replace the already known description for this table to assumptions and add a sentence to clarify the purpose and motivation for the table.

5.6.2.3 Findings – Usability

The questions in this section sought to establish the expert’s opinion on the usability of the framework. The researcher sought to obtain the expert’s opinion not only because of her experience in application of security and privacy in industry but also her experience in developing the LINDDUN framework. The researcher’s objective was to establish if in the expert’s view, the framework is appropriate and adequate for the research domain. These questions were based in addressing all the RSQs. and ROs. 3, 5 and 6, defined in Figure 5.7, overleaf. The RSQs. mapping to the questions of the questionnaire is presented in Appendix B

<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.</p>	
<p>RSQ. 3 What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?</p>		<p>RO. 5 Validate the framework with industry and research domain experts.</p>
<p>RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?</p>	<p>RO. 6 Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.</p>	

Figure 5.7 RSQs and ROs mapped to questionnaire questions analysed in usability

Dr. Wuyts remarked that the current document is too complicated but argues it's a typical academic issue. She noted that they *“have been struggling with that comment for 10 years for LINDDUN because when we first created it, it was an academic work and now people want to use it and there's, kind of, a difference.”* Her recommendation is to have a summarised version of the current academic document or a quick guide on how to use the framework. Dr. Wuyts suggested a plan along the lines of *“This is the framework, these are the six steps, and from a high-level perspective, this is what they are, and this is why you should do that. This would make it easier to use.”* Dr. Wuyts rationalised her argument by saying *“well, with, if SMEs have to go through this, they might get a bit lost.”* She suggested to distil the current document into a high-level manual. Dr. Wuyts remarked, the content is there, *“I think it's, like, making it more polished as an instruction or as a manual...or a technical report which is the manual.”*

The finalised high-level version would be supported by links to the more detailed document that provides the academic background and support for use of the standards and components of the framework. Dr. Wuyts commented, *“when I read through it, sometimes it felt like this is an instruction to do, and then you have a lot of information like, this is why I think you should do it, and references to academic work, and I think*

from an academic perspective that's useful. From a practical perspective, that's mostly just a footnote or I'm not that interested." This advice came directly from Dr. Wuyts' experience in her development of LINDDUN for her PhD research. She commented that many developers or SMEs would look at the current version and think *"How should I tackle this giant beast of a document to look for those things that are useful for me? It would be easier if the useful things have been already emphasised or available."* Dr. Wuyts noted that the manual would provide an easier *"This is how you use it, because now it's just a big list, kind of, a block of information and how should you approach this."*

The discussion recommendation can be summarised in Dr. Wuyts' comment *"making it more user friendly or...Soften the blow of, like, this is a big framework because, well, you need it basically but, but now, here is how to, to get familiar with it and, and this is in general what you will do, and then you can go into more detail."* Dr. Wuyts also suggested the potential of the development of a workshop around the implementation of the framework. This would include working examples through the framework to make the steps and processes more practical and realistic.

Dr. Wuyts noted the usability of the DFSPCs would be challenging, however she noted, *"I don't think you necessarily need to do a lot of things about that categorisation...and, as such because it's a great overview but maybe that's also going back to the manual."* Dr. Wuyts indicated the manual would better serve the use of the DFSPCs with a more concise "how to" use the categorisation. Step 5 of the framework was also an aspect of this discussion. Dr. Wuyts was perplexed about step 5, she asserted *"it was just such a small portion of the document that I was thinking, like, does it make sense, but, no, it's okay."* In discussion around the step, it became clearer to Dr. Wuyts why this would be a separate step. The framework is moving from the problem space into the solution space. So, we're thinking about requirements and solutions.

The use of examples throughout the framework was also recommended by Dr. Wuyts. She commented *"it would make it much easier, just a simple example of each key element was provided. For e.g., this is a threat, this is the attack, and this is the security property it violates."* On reviewing at the end of the interview Dr. Wuyts was asked again about the usability of the framework. She noted *"I think it's just cosmetics. Or it might be a visual thing."* On reading through the framework, she expected to get a high-level overview and the dive into the details. However, the framework was already in the details and that "confused" her. Dr. Wuyts noted that figure one *"is a really overwhelming picture"* which *"is great for academia...But for the developer, it's like, wow, this is*

complex.” Again, the solution involves supplying from the current version a concise less academic technical document. To “*extract the useful content, the instructions from your manuscript and put it into something more practical, a manual, an overview, a quick guide, getting started.*” The researcher discussed the implementation of the framework and Dr. Wuyts suggested using this aspect to extract the useful information for the developers.

5.6.2.4 Summary of Expert Review Framework Amendments

This section summarises changes to the framework on completion of the expert review. Table 7 ‘Lawful processing’ was elevated in the framework to convey its importance. This table is one of the most important GDPR legal aspects of the framework. It collects significant requirements necessary for a DPIA and evidence that consideration of the legal processing has been considered and addressed.

The researcher agreed that repudiation and non-repudiation should be distinct categories. This adjustment would be made through to the categorisation of the data flow security and privacy controls (DFSPCs).

The researcher agreed the importance of the different mind-set required when threat modeling security and privacy. The researcher agreed that it was important to point this out in the framework and bring it to the attention of the user. There will be a short addition to the framework in step 3 to communicate the different mind-sets required when threat modeling security and privacy. This also drew on the discussion encouraging both a security and privacy champion among the software development team and this was written into the framework. The concept of encouraging both security and privacy champions for the framework implementation was to be introduced into the template.

The framework would need a requirement for a compatibility assessment. A compatibility assessment is to make sure all the purposes specified up front for collection of the data are the only processes on the data items. It also includes assessing that the data collected is only used for that specific purpose. The compatibility assessment process would run through the per-interaction process. The developers would assess if the processes being developed are compliant with the conditions for the original stated purpose and received consent for processing the personal data. If the compatibility assessment reveals gaps, the project will have to address these to continue being compliant. Step 2 Table 9, the researcher replaced the already know description for this

table to assumptions. The researcher also added a sentence to clarify the purpose and motivation for the table.

The researcher added a sentence to step 1 to clarify the privacy policy is a process that is continuous throughout the product development and the data lifecycles. This was not clear to the expert reviewer. Dr. Wuyts questioned “*Shouldn’t the processing actions and purposes be specified first?*” before the privacy policy was finalised. The researcher added a sentence to stress the importance around ensuring that the development of the privacy policy stayed in line with the development of the system. The privacy policy would not be concluded until the system development was completed. There was a wording correction in section 3.3, per-element replaced with per-interaction.

The future work for the framework will include a summarised version of the current academic document. This will include a quick guide on how to use the framework or an implementation manual for use by developers. The current document is too complicated and academically biased. The finalised plain version for developers should also include examples. In addition, an implementation manual or high-level overview could be developed out of the implementation of the framework within STATSports as suggested by Dr. Wuyts. The researcher could investigate with the development team from STATSports what a high-level technical or “How To” manual should contain. The suggestion is to extract from the development team what they would consider would make the reading and implementation of the framework less academic, more appealing to developers. The development of a high-level technical or “How To” manual is seen as future work with the framework.

5.7 Final Focus Group

This section describes the findings of the final focus group with the STATSports software development team. This focus group was performed to collect qualitative feedback data to partially answer RQ. 4 and fulfill RO. 6.

RO 6: Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.

The validation was part of the action taking and evaluating stages of the adopted action research approach to address RSQ 3 and RSQ 4, outlined in Figure 5.8 overleaf.

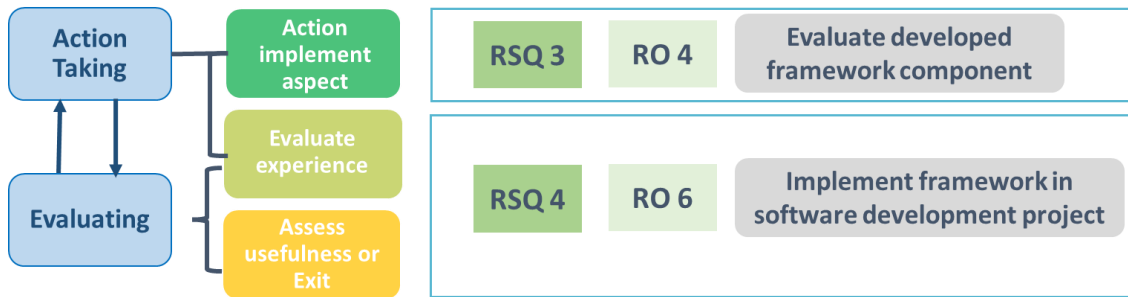


Figure 5.8 Validation as part of action taking and evaluating stages of this action research

Two weeks before the focus group was scheduled the software development team was provided with the questionnaire. This lead time provided ample time for the software team to review and complete the questionnaire. The questionnaire was emailed back to the researcher two days before the focus group was scheduled to take place. This allowed the researcher time to analyse the completed questionnaire and to derive any further questions from the responses. The focus group questions evolved from the questionnaire to ensure the questions linked back to the research sub-questions. The focus group questions were mapped to the research sub-questions and objectives. The focus group questions matrix is available in Appendix E, along with the open-ended questions from the focus group. Some of the focus group questions were developed from the replies in the returned questionnaire from the STATSports software development team. Questions for the focus group were also motivated to target certain key aspects established from the expert review. This included understanding if the developers recognised the importance of the GDPR legal requirements in step 1, which are:

- Table 7 Lawful processing;
- Screening statements process 1.5;
- Classification of data;
- Requirement of consent for collection of data; and
- Informing the data subject on data being collected and its use.

Other questions developed from the expert for the focus group included; bringing the overview diagram through to each step, understanding the language in the framework and what a technical or “How To” version of the current document would include to make it less intimidating or more developer friendly.

The questions prompted from the expert review are marked with an asterisk * in the interview protocol matrix in Appendix E. The researcher developed the focus group questions to encourage discussion and target certain components to enable the research

question and sub-questions to be answered. The transcript for the focus group is provided in Appendix G. The quotes used in this discussion section are highlighted yellow in the focus group transcript.

5.7.1.1 Software System Description

The STATSports software system the framework was applied to is called Sonra cloud. The Sonra cloud offering is an extension to the existing Sonra desktop analysis platform. This is the first STATSports product developed for and available in the cloud. The Sonra cloud allows users to share player data seamlessly through a bi-directional data sync process with other users anywhere in the world. It also enables users to tap into brand-new features that will be developed on the Sonra cloud, which will make use of the massive computational power provided by Microsoft Azure. This will allow STATSports to provide access to features never possible with the Sonra desktop solution due to the computing constraints of local machines.

The Sonra cloud is built on a fully serverless architecture, utilising some of the core serverless services provided by the Azure cloud including Azure Functions, Azure BLOB Storage, and Azure SQL Database. Each client deployed as a cloud tenant, receives their own set of dedicated resources, including compute and storage. This approach was used to ensure a high-security standard and keeping individual client's data segregated during processing and storage.

5.7.1.2 Software Development Team Profiles - Focus Group

Each of the participants completed sections B of the Research Information Leaflet and Questionnaire document, presented in Appendix A. Section B of this document collects the participants experience and domain knowledge. All of the participants answered yes that data security and privacy are important for their domain. The profiles of the software team focus group participants included their position in the development team and what part of the development they held responsibility for.

STATSports Chief Software Architect (CSA), started as a developer with STATSports in 2014 and is now the chief software architect. The CSA designed the Sonra cloud architecture as a new optional feature for the existing Sonra product. His role also involved oversight of the development of the cloud feature. CSA has 1-3 years of experience in applying both security and privacy in development. He had no experience in implementing the STRIDE or LINDDUN models before implementing the framework.

The CSA rates his level of experience in implementing controls as good for security and excellent for privacy in the software development process. His experience in implementing security controls includes following best practices for transmission and storage of personal and confidential data. For privacy the CSA has experience implementing security and privacy practices for transmission and storage of personal identifiable data using field level database encryption, encryption at REST and transmission over secure protocols such as HTTPS.

STATSports Software Developer One (SD1) is a software developer with STATSports since 2017. He was involved with building and implementing the cloud into the Sonra product. SD1 has 1-3 years of experience in applying both security and privacy in development. He had no experience in implementing the STRIDE or LINDDUN models before implementing the framework. SD1 rates his level of experience as fair for implementing controls for both security and privacy in the software development process. SD1 has experience implementing controls and best practices for transmission and storage of personal and confidential data and following software principles of security practices for stored data, encryption of data and transmission of data using rest HTTP calls. He has a software engineering degree and is an AWS certified DevOps Engineer.

STATSports Software Developer two (SD2) began as a software developer in 2018 when he joined STATSports, coming from a software engineering degree. He was involved with building and implementing the solution for the cloud, for both the local and remote features of Sonra. SD2 also has 1-3 years of experience in applying both security and privacy in development. He had no experience in implementing the STRIDE or LINDDUN models before implementing the framework. SD2 rates his level of experience as fair for implementing controls for both security and privacy in the software development process. He has experience implementing controls and best practices for transmission and storage of personal and confidential data. For privacy SD2's experience includes implementation of privacy practices for transmitting and storing of personal identifiable data, using field level database encryption, encryption at REST and transmission over secure protocols such as HTTPS.

5.7.2 Focus Group Findings

The researcher reviewed the returned questionnaire and assessed the returned answers to the questions that had been developed for the focus group. The returned questionnaire and focus group findings were analysed according to the categories and codes found in

Table 5.2. The discussion around the findings will follow the categories and codes. However, like the expert review, many of the focus group findings crossed categories. The focus group questions are mapped to the RSQs and ROs, which is available in full in Appendix E. Both the questionnaire and focus group were completed when the development team had fully implemented the framework.

5.7.2.1 Findings – Value

The discussion in this set of questions follows part one of the questionnaire and relates to the value the framework brings to developers. Value is measured for this part of the validation on how the framework provides knowledge, understanding, processes and legal needs to meet the GDPR data protection requirements for developers. The focus group questions sought to establish if the framework added value for the software development team and what they would recommend to add value.

Questions 1.1-1.4 of the questionnaire concentrate on the developers’ opinion on the gap for a specific individual implementation process for SME developers inexperienced in security and privacy meeting GDPR regulatory requirements. The focus group questions consider the challenges this presents and how the framework does and does not meet the challenges for the developers. These questions were addressing RSQs. 1 and 2 and ROs. 1, 2 and 3 defined in Figure 5.9. The RSQs. mapping to the questions of the questionnaire is presented in Appendix B The extended mapping for the focus group questions is available Appendix E.

<p>RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements for software development in the IoMT?</p>	<p>RO. 1 Investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs when implementing the requirements.</p>	<p>RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.</p>
<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>RO. 2 Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.</p>	

Figure 5.9 RSQs and ROs mapped to questionnaire and focus group analysed in value

Questions 1.4-1.8 focus on the benefits of the guidance and processes provided in the framework for developers inexperienced in security and privacy meeting GDPR regulatory requirements. The focus group questions consider in depth the adequacy of the

framework processes and what the improvements or changes the developers would recommend. These questions were based on addressing the RSQs. 2, 3 and 4 and ROs. 2, 3 and 6 defined in Figure 5.10.

<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>RO. 2 Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.</p>	<p>RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.</p>
<p>RSQ. 3 What components are required to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?</p>		
<p>RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?</p>	<p>RO. 6 Implement the framework in a SME software development project to establish effectiveness to overcome the challenges.</p>	

Figure 5.10 RSQs and ROs mapped to questionnaire and focus group analysed in value

When answering question 1.1 of the questionnaire, the development team confirmed that they find a gap in the guidance provided for developers. This gap was established in the literature review and supported by Dr. Wuyts’ opinion provided in the SSI section. This was one of the key challenges that prompted the organisation to approach the research centre for assistance, discussed in chapter 4. The organisation recognised the need to get support to meet the GDPR security and privacy requirements in their products and for the wider organisation. The development team questionnaire answer asserted **there is no one destination for developers to find a framework that can be used in the development of their applications for security and privacy to meet the GDPR requirements.** The developers revealed that security and privacy in development was not a priority until the introduction of the GDPR regulation. The CSA stated, *“It’s only really in the last three years when this started to be more important because of the GDPR...when we began to take it more seriously.”* The first follow-up focus group question was prompted from the expert review. It asked if the framework provided a tailored process that covers the needs for applying security and privacy of data in the individual software development project. The development team strongly agreed with this question. In the discussion the CSA said, *“I found, and the other developers also found...that the framework provided everything that was needed.”* This in part

answered RSQ. 1, the development team identified the gap and stated in their opinion the framework addresses this gap.

The team acknowledged that the framework did provide a *“tailored process”*. However, they also agreed that *“narrowing down the current approach would improve the framework”*, which they believed would improve the potential for implementation. The software team offered recommendations on narrowing down the approach.

The team suggested it would help to *“apply different layers of filtering”* to various components of the framework. One suggestion was adding filtering to the threats because the *“threats included everything.”* Which in their opinion *“is an excellent resource”* but, this made finding and distinguishing the threats for the specific type of development awkward and time consuming. The initial type of filtering suggested was filtering threat types into *“specifically hardware related, software related or network related threats.”*

The team advanced on this concept to further filter the type of threats to the type of development. They used software development as the example, where the threats could be filtered to specifically target *“web app development...versus the threats specific to developing a mobile app.”* However, they did also say *“that it was very easy to pull up all the specific threats that could happen within a particular process or boundary.”* This was a key intention of the framework because as revealed in the literature review attackers focus at entry and/or exit points and boundaries for vulnerabilities to breach security and privacy. The researcher recognises that filtering threats would simplify this aspect of the framework. This in turn could benefit and simplify the framework implementation. As seen in the literature review and discussion with the team, developer’s time is valuable. Developer time constraints was also one of the challenges identified for this domain. Simplifying the processes in the framework to their requirements could improve adoption of the framework. This is an improvement for future work with the framework.

The discussion moved on to examining if the framework provided adequate information on the GDPR regulatory requirements and the risk assessment process for the development team. This analysis included understanding if the framework stressed the importance of the processes essential to meet the GDPR regulatory requirements. In addition, it considered if the security and privacy and the risk assessment process was seen as equal. These questions were asked to investigate how well the framework accomplished RSQ.2 and ROs. 2 and 3. The team agreed that implementing the framework resulted in a better knowledge and understanding of the GDPR regulatory requirements. They also agreed that their confidence in understanding the GDPR

regulatory requirements and how to apply them in software development was better. The CSA pointed out for the team *“everyone is aware of the GDPR...but actually having a framework to go through, and it lays it out, we feel it definitely helps a lot.”* The team affirmed that the steps and each process and component of the framework *“were sufficient to get you through it.”* The team did not find they were unable to complete any of the steps or processes of the framework. They did acknowledge that they had access to and assistance from the researcher. However, they were confident that they could have completed all steps and processes independently, it may have taken longer.

In response to a discussion during the expert review the researcher questioned if the software team considered there was too little focus or importance on the GDPR legal requirements in the framework. Dr. Wuyts questioned if there was enough prominence on the GDPR legal requirements in the framework. This related to RO. 3 of the research. Consequently, the focus group questions were directed at the key GDPR legal aspects of the framework in step 1 of the framework:

- Table 7 Lawful processing;
- Screening statements process 1.5;
- Classification of data;
- Requirement of consent for collection of data; and
- Informing the data subject on data being collected and its use.

The team agreed they had assumed that all aspects of the framework were important and accepted that all steps and processes had to be completed. They didn't question the importance of one over the next. The CSA answered for the team on Table 7 by saying, *“we don't really have any kind of specific feedback that we misunderstood it was quite clear to us.”* However, the team did point out that this was already familiar to them and was done with the researcher during one of the introduction sessions. They had the same answer with regards to the screening questions and data classification. All of these concerns were familiar to the developers. They did state that it could be beneficial to highlight their importance from a GDPR regulatory requirement position. However, they saw all of the steps and components as necessary of equal importance stating, *“we were treating all processes of equal importance.”* With regards to consent and informing the data subjects about their data, the developers had already experience with this. With the introduction of the GDPR in 2018 they had to retrospectively apply this requirement to established products. In addition, the team had since the introduction of the GDPR

developed a consumer product and had built the consent requirement for any processing of personal data. The team noted that from their experience, the information provided in the framework was more than adequate to meet these requirements. They saw the draft privacy policy as a particularly valuable asset for developers. However, the team did accept that much of this was done with the researcher. SD1 stressed *“what we were not sure of, we would have you, go through with us.”* They did recommend an interactive example to help complete the privacy policy. They indicated this would really benefit people with no or little experience with this process. The CSA pointed out the team completed this component *“with you and that really helped us understand and complete it...and having an interactive draft policy potentially might be very beneficial to people.”* The researcher views this as part of future work for the evolution of the framework to improve its future potential implementation.

The team had a similar attitude to security and privacy in the framework. They believed that both aspects were equally important and did not sense that one was promoted over the other. The CSA commented for the team that they *“didn't feel like one weighted above another...everything was on par.”* This was one of the aims of the framework, to bring together security and privacy into one tailored process and have each aspect on an equal footing in order to meet the GDPR data protection requirements. The team agreed they *“didn't feel like one was favoured over the other.”* When asked if they previously would have considered privacy or did the framework really enforce it, the team had a number of thoughts. As already discussed, privacy only became important to the developers with the introduction of the GDPR. They said that *“the framework, forces you to look at two specific things, security, and privacy, at consider each of your processes and your process boundaries.”* SD2 expanded on this and said that the framework *“puts the GDPR into the mind-set of thinking about it the whole way through development.”* The team stated they did not encounter any difficulty with implementing both security and privacy at the same time. The CSA stated, *“there was no conflict between security and privacy, or that we couldn't apply something.”*

As noted in the literature review and in the review with Dr. Wuyts there is great value in having all of the information regarding a development project collected and documented in one place. Dr. Wuyts believed the advantage with this is that the information can be reused or simply referenced again. The development team articulated this experience, *“the way the architecture of the system is, a lot of our processes and services are developed the same way under the same patterns. So, there was a lot of like*

repetition.” This meant that for much of the software development project *we really only had to...dig deep into one of the services and then that could be applied across the board.*” This is where much of the information in the framework can be transferred knowledge throughout a project. The CSA agreed *“that very much followed through because a lot of the services,”* they employ, *“are the same”* for the majority of their systems. In addition, the development team understood that the work completed for this project would cross to other projects, as much of their products and systems *“follow the same architectural pattern. So, a lot of these principles would apply across the board.”* The team also considered this would be of value for new developers joining the team. Having this information available to them would provide both a reference to the process for security and privacy in development but also as an instructive tool.

The collection of an extensive amount of information into a single framework template was considered valuable by the developers. SD2 stated and the team agreed, *“there are a lot of links in there to bring you to additional information, and so I think that was very helpful that you have put those in the framework.”* This was also agreed by Dr. Wuyts in her value assessment of the framework. The software team saw this aspect of the framework as a valuable resource for developers that have no knowledge and experience in the field. They also thought it would be beneficial for developers looking to expand their knowledge. The developers agreed the information in the framework expanded the capability for further information because it *“provided a lot of links to more information, so they were sufficient enough, for anything that we feel we needed more information on.”* When asked to consider if the links would be of value and the software team would trust the linked information, the CSA responded by stating *“if we are trusting the framework, we’ll trust the links.”*

The researcher was satisfied that the feedback from this section determined the fulfilment of RSQ. 4. The feedback determined that the framework provided sufficient information and guidance for the developers. This developed their confidence in understanding and addressing the GDPR requirements. The feedback also recognised the risk assessment process was practicable for the developers. In addition, it was found the developers would also use the framework as a building block for future application to other projects. They recognised the work completed during this implementation would carry through to other projects.

5.7.2.2 Findings – Composition

These questions were based in addressing all the RSQs. and ROs. 3, 5 and 6, see Figure 5.11. The RSQs. mapping to the questions of the questionnaire is presented in Appendix B The extended mapping for the focus group questions is available Appendix E.

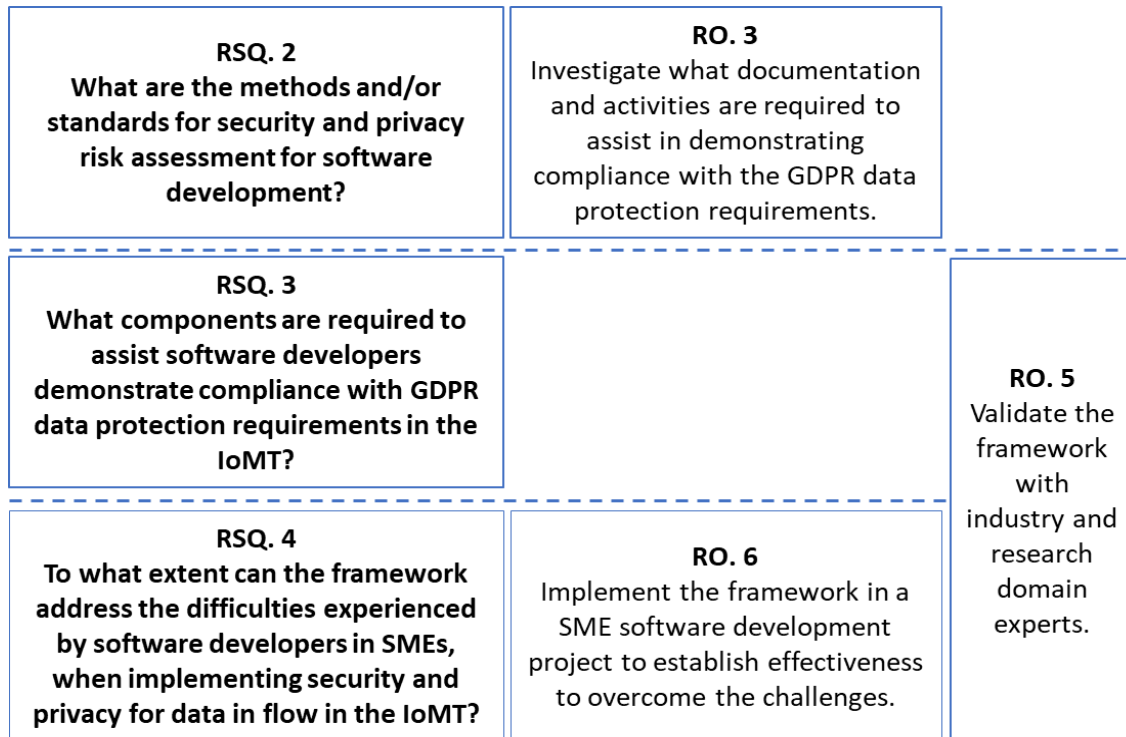


Figure 5.11 RSQs and ROs mapped to questionnaire and focus group analysed in composition

Overall, the composition of the framework was considered appropriate by the development team. With the focus group questions the researcher went through all of the steps and processes of the steps with the developers. This was in an effort to uncover any aspects of the framework the developers may deem unnecessary, excessive, and unclear or they had difficulty understanding. The software team provided valuable feedback and recommendations on the composition of the framework.

One of the key composition aspects of the framework recommended by the software team was filtering for threat elicitation in step 3. This step included the threat to attack starter kit. The development of the threat to attack starter kit was in response to a conference workshop and was discussed in chapter 4. During the workshop the implementation of the framework practically came to a stop when the participants came to threat elicitation. Threat elicitation was revealed as a challenge for developers. The researcher developed the threat to attack library starter kit to address this challenge and assist implementation of the framework. This is one of the components of the framework

that was deemed essential by the software team. They were asked to consider if the threat to attack starter kit was seen more as background guidance or as a necessity for developers in SMEs to kick start threat elicitation. The CSA stated, *“the threat to attack library starter kit is really a necessity to get the kick start, people could probably figure it out, but it would be a difficult task. Particularly with when you don't have experience threats or finding or thinking about the threats for a specific aspect.”* SD2 expanded on its importance by saying *“even if you didn't have the threat to attack library, you might miss a few, so having the library there makes you see all the possibilities rather than be single minded and only pick out a few. Rather, this puts it all in front of you and many of the potentials.”* The team agreed that the threat to attack library starter kit did encourage them to look outside of the library table and find other potential areas.

The software team also looked further into the OWASP top 10 and the CWE and threats. They appreciated the links to these other sources and agreed the threat to attack starter kit made it easier for them to find threats. The CSA commenced the discussion by saying *“picking out the threats, was more time consuming, but having the library helped. If the starter kit wasn't there, you'd have to go look it up yourself and then it would be where do you start with that.”* This was the primary reason for the development and inclusion of the threat to attack starter library in the framework. However, as seen from the comment the software team did find the process for threat elicitation in the framework difficult to navigate because of the structure. The team suggested filtering to help streamline the process.

Filtering was also provided as a solution by the team when they answered question 2.11 in the questionnaire. They were asked to describe any deficiency they have observed in the framework. The team wrote, *“the framework should add the ability to filter the framework on a number of different levels to allow the user to narrow down the threats specific to their domain.”* For the software team the time to search through all of the provided threats in the starter kit was frustrating. They saw this as a shortcoming of the starter kit. They provided examples of two levels of filtering they considered would greatly assist in threat elicitation, presented in Table 5.3, overleaf.

Table 5.3 Software team recommendations for filter level categories for threat elicitation

Environment	Software Domain
- Hardware	- Web App
- Software	- Database
	- API's

In the focus group discussion, the software team supported their answer in the questionnaire and expanded on it stating, “*we believe adding multiple layers of filtering will help improve the framework.*” Currently, all possible threats are included but these can cover a wide array of domains. Having the ability to allow developers filter threats to be more specific to their domain will improve the overall ease of use of and adoption of the framework. The CSA expanded on this in the focus group discussion, he said “*it just took a bit of work...because all the threats and attacks were listed.*” This meant that the developers had to investigate all of the attacks to see if they were relevant to the threat in the development they were completing. They indicated that “*when you click in for more info on the attacks, they may not have been directly linked or correlated to whatever your threat was.*” This resulted in the developers having “*to look through all of the attacks in the threat category they were listed in.*” The software team focus group discussion also encouraged applying filters to fit the software that is being developed. The examples provided by the team included having hardware, software and network related, filtered threats, and breaking this down even further to the type of software development such as, “*web app there's specific types of threats that would be applicable versus a mobile app.*”

The software team also recommended the filtering should extend as much as possible to the controls. The researcher can see the difficulty with having all the potential threats, types of development and controls collected without filtering and acknowledges that filtering could make this process more streamlined and less time consuming. Section 5.7.2.3 discusses how this difficulty impacted the usability of the framework. SD2 also suggested “*if there was a way of being able to link between, say, the interaction you are working on and the threats that you do have in your interaction and between that starter kit it would be make things a lot easier.*” The researcher understands this as another level of capability for filtering and separating the risk assessment within the framework. The developers would be able to link right across the framework from a per-interaction assessment to threats to attacks to controls. The researcher determines this as future

improvement work for the framework to increase uptake and ease implementation. In summary, the software team accepted the guidance provided in step 3 was sufficient for developers inexperienced in threat elicitation. However, they did point out that it was overwhelming and was not easy to navigate. SD1 summarised their thoughts by saying, *“it was probably a bit of a learning curve to understand what exactly was needed. But, once you get your head around it, it was pretty straight forward. I kind of felt a little overwhelmed at times with it. I thought it was kind of a bombardment of information.”* This is also discussed further in section 5.7.2.3, on the usability of the threat to attack starter kit and threat elicitation.

The software team did not have any difficulties with the composition of the risk assessment process in step 4. They believed there was nothing further required to assist them identify security and privacy risks or to make it more understandable. When questioned on the risk assessment process the team acknowledged they *“wouldn't have done a risk assessment like this.”* They would have previously considered security but, would not have had a formal approach or documented the process. The CSA acknowledged with the introduction of the GDPR regulation they would have paid more attention to security and privacy. However, he said *“this was worked on...with yourself, verifying the privacy and security requirements from the GDPR.”* But this would not have been documented and would not be in one place. It would have been recorded through different tools and systems used to develop the software. The information would not be in a collective single place to reference. When asked if implementing the framework assisted with the developer's confidence in completing risk assessment. Both SD1 and SD2 acknowledged that they would have more confidence. When asked if they would be happy to put a new developer through the risk assessment process, SD1 answered *“I would like to do a bit more studying on it to refresh my mind but yeah.”* The software team did not encounter any confusion on which threats they needed to prioritise whether it was privacy or security. They were sure that they did not view one having *“priority over the other.”* They further specified that with security and privacy they did not think *“that one was easier or more difficult than the other to implement or having a priority over the other one whenever we were implementing it. There wasn't an emphasis on one over the other.”*

The researcher discussed the necessity of step 5 with the developers because of the feedback from the expert review. Step 5 is mapping the attacks back to the threats and then back to the framework properties. This step is to link the threats back to the

framework properties because, the DFSPCs are categorised to the framework properties. Dr Wuyts was not clear why step 5 would be a step in itself as it was such a simple step. The software team were positive about step 5 being a separate step. They appreciated that this was a separate step to bring everything full circle back to the framework properties. The team did acknowledge *“whenever we did it, we did the whole process...rather than breaking it up as step five or six, we combined them.”* However, they did not see any value in bringing this step into step 6. SD1 noted that they *“liked it separated out because you've got that extra granularity, it breaks it down that wee bit more.”* They agreed that having it as a separate step helped draw them into the composition of the framework. The CSA agreed, *“the smaller the steps the better. It's better to have more small steps than do large steps in my opinion as well.”* The team discussed that the step prevented them from getting lost in the framework. The researcher took the recommendation of the developers and will keep step 5. SD1 summarised for the software team by saying, *“I like things broken down and the layman terms really kinda breaking it into chunks nearly to make it just really understandable and clear.”*

Similarly, the software team did not believe there was anything missing in step 6 and the controls provided to mitigate the threats. The difficulty in this step is in relation to the usability and filtering across the framework. This is discussed further in section 5.7.2.3.

The researcher wished to get feedback on the language in the framework and if it was understandable for developers. Dr Wuyts suggested that the framework was very academically oriented. The software team were asked in the focus group what they thought of the language and if it was difficult or a deterrent for implementation. The CSA began the discussion by stating *“this is probably where some more Googling came but, it's the first time seeing a framework like this so typical of the language I would expect and I don't have any kind of feedback on how to water it down, for us, I think there is terminology that you probably have to use, and it's just about making sure that the definitions are there so that people can easily understand it.”* The software team were in particular asked about the terminology of the GDPR data protection requirements and the framework properties. The team did admit that *“there probably was a bit of Googling on the side to...to fully get up to speed with the more obscure properties to do with privacy. But I think generally it kind of gave a good outline of them all.”* SD2 said he had difficulty at the beginning as it was such a steep *“learning curve, for me it was a big step up.”* When asked what made it manageable, SD1 and SD2, the less experienced developers of

the team, agreed that *“as soon as you got further in, and into the processes and going through each one like. The language started to make sense and you knew how to work your way around and understand the whole framework a lot better.”* They also expressed that the meetings with the researcher and having the CSA involved, who has more experience in the domain, really helped. SD1 said, *“the time spent going through the steps in each of the meetings as SD2 touched on helped...the CSA was a big help to us explaining it as well.”* The researcher inquired how they would have managed if the team didn't have somebody with the CSA's knowledge and experience, did they think it would have been more of a struggle. SD1 said, *“I think we would have got there eventually just the getting started would have been a struggle.”* SD2 agreed by saying *“I would say yes initially in getting started it would have been difficult.”* The team suggested that having interactive guidance in the form of an example would really help to understand the language and terminology in the framework.

5.7.2.3 Findings – Usability

The questions in this section sought to establish the developer's opinion on the usability of the framework. The researcher sought to extract from the development team what issues they had when implementing the framework. Another objective was to find out what the team would suggest for the framework to make it less academic and more appealing to developers. These questions were based in addressing RSQs. 2, 3 and 4 and ROs. 3, 5 and 6, defined in Figure 5.12 overleaf. The RSQs. mapping to the questions of the questionnaire is presented in Appendix B The extended mapping for the focus group questions is available Appendix E.

The discussion in this section will begin with a summary of feedback on usability. The remainder of the section will follow the steps of the framework for ease of reading and discussion. The discussion around each step will include the themes for this category presented in Table 5.2, which are:

- Usability for inexperienced SME software developers;
- Usability obstacles;
- Generalisability of framework;
- How To/Improvements;
- Benefits;
- Developers Insights.

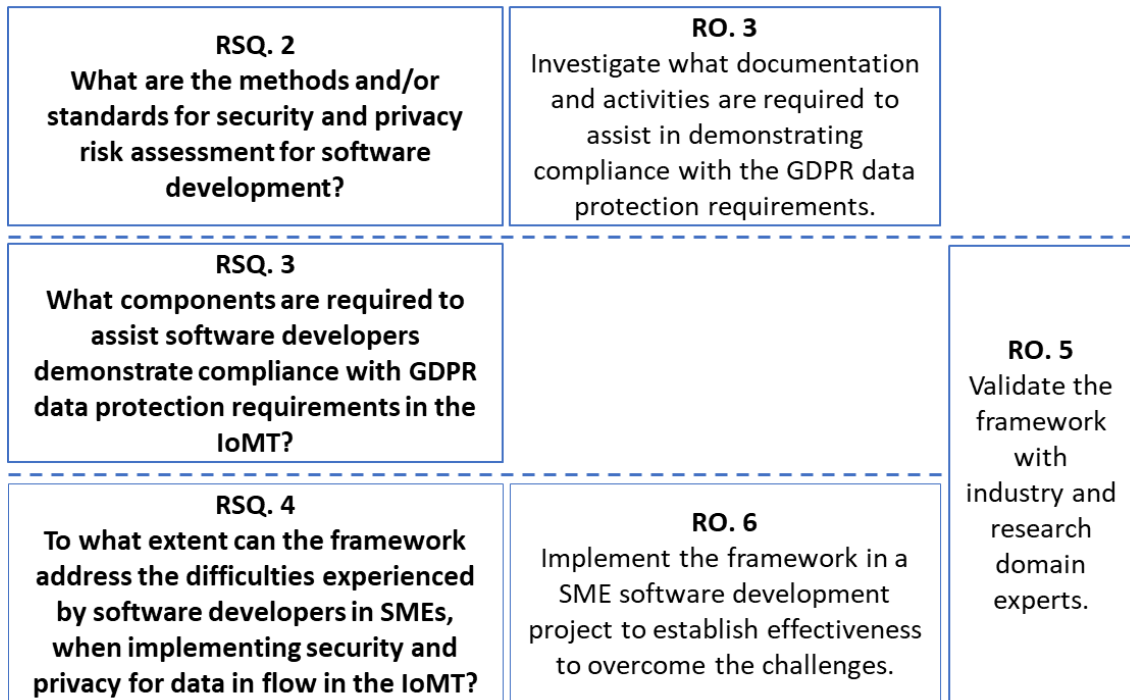


Figure 5.12 RSQs and ROs mapped to questionnaire and focus group analysed in usability

The researcher reviewed with the developers the usability of each step, process, and guidance part of the framework and the framework as a whole. The software development team provided very valuable feedback on the processes, recommendations on the structure, and ways to streamline components of the framework.

Overall, the usability of the framework was considered acceptable by the development team. The answer in the questionnaire from the team was Yes, the framework is easy to understand once the user goes through it at least once or twice and for more experienced users who have used similar frameworks. The CSA expanded on this answer in the focus group and said, “once you go through and get used to the framework then I think it's much easier. I think we probably struggled a bit just at the start. And then once we went through it once or twice it became very easy. It took a couple of reads and working through it to get the hang of it. Once you get your head around that then it's OK.” However, they did also state, “for developers completely new, following a framework like this could be quite daunting.” This correlates with feedback received from Dr. Wuyts in the expert review and discussed in section 5.7.2.4. Dr. Wuyts suggested the framework could be daunting to developers inexperienced in this domain. She proposed an implementation manual or high-level overview could be developed. She recommended investigating this idea with the development team and what a high level technical or ‘How To’ manual should contain. The development team had considered

aspects to help with the usability of the framework with the answers they provided in the questionnaire. This feedback helped to partially answer RSQ. 4.

This feedback to help in relation to the usability of the framework, was one of the key pieces of opinion from the developers that came from the questionnaire and focus group. The recommendation from the questionnaire was the framework is easy to understand once the user goes through it at least once or twice and for more experienced users who have used similar frameworks. For developers completely new to following a framework like this is could be quite daunting so an interactive demo would help with the steep learning curve. An interactive process was previously suggested in the previous section 5.7.2.1, when the developers suggested an interactive draft policy to help complete this process. They also suggested an interactive demo in section 5.7.2.2 when discussing composition of the risk assessment process. As suggested by Dr. Wuyts, the researcher used the focus group to obtain detailed feedback from the developers to make the reading and implementation of the framework less academic and more appealing to developers. The discussion included providing an interactive demo, the software team discussed *“going through each step and explaining each step”* would be very helpful. They recommended using an example product or system and applying this example through the entire framework, each step and process. The discussion evolved into breaking an interactive demo into a series of bite size videos, the CSA thought that *“one overall video might actually be quite long and maybe people might click off it. So maybe the smaller video on each step is better.”*

The researcher introduced the idea of a technical ‘How To’ document discussed in the SSI expert review. The current form of the framework is broadly academic, which is necessary for the completion of the action research project. However, this academic style may be intimidating to developers. All of the developers thought that a technical document could be useful to bridge the overwhelming aspect of framework. SD2 summarised the developers’ thoughts by saying *“I think a technical document would be a lot easier to get into since we wouldn't feel as overwhelmed compared to the academic document and then combine that with a series of small videos based in each step. And I think it would be all that I'd need really to be able to do this confidently.”* SD1 agreed. However, the CSA supported keeping the academic document also to have it as background information that could be referenced for further information. The team agreed but, as they theorised, the more supporting information you have the better it is.

Chapter 5 Validation of the Framework

The CSA summarised the discussion by saying *“I don’t know if this is the right answer to say because I think it’s good to have it all there.”*

The conclusion of this discussion was the academic document is necessary. It was concluded that the academic version has all of the information that a developer would need to understand all the aspects of the framework and all of the links to further information. SD1 summarised the explanation for having the academic and technical document by saying *“Let’s say the first one or two times you go through this there should also be an academic document that could be used, to get more familiar with it, then maybe having just the technical stuff. You know it’s just a cleaner approach.”* However, all of the development team agreed that there should be an interactive support, through videos that would guide you through the whole framework and then you always have your technical document which you could reference with the videos. *“It’s from the videos and then use that going forward as you go to and then you’d also have your academic information if you need more information or links on any particular subject that’s there as well.”* The conclusion of this discussion provided a clear plan for the future evolution of the framework for the researcher. The developers provided feedback to make the framework more compatible and attractive to developers’ requirements.

The developers had no usability issue with the summary rationale or diagram presenting the framework. They were satisfied it provided a clear overview of the framework. SD1 noted, *it is easy to understand once you get used to it or go through it once or twice.* The developers did not see a problem with the summary or the diagram. When asked if it should be continued through each step to improve usability the developers did not think it was necessary. This was a point raised in the expert review, Dr. Wuyts believed it would be potentially beneficial for developers to have the diagram carried through to each step of the framework.

Likewise, there was nothing specific in step 1 that the development team emphasised as unnecessary or that required changing. The software team were asked to consider the appropriateness and explanation of the approach the framework had taken and described in step 1. The approach connecting the GDPR data protection principles to the security and privacy properties that were linked to the threat categories that were linked to categorised controls. The contextual knowledge of step 1 *“helped with the overview of the thing.”* The CSA noted they grasped the approach, and it makes sense to the developers *“as you have to link it back to the GDPR through the properties and then link it to the threat and then show you have you know like put a control in...it kind of puts*

the GDPR into like the mind-set of thinking about it the whole way through.” As highlighted previously in section 5.7.2.1, the development team did not consider the important legal aspects of the GDPR requirements screening, privacy policy and lawful processing required elevation in importance in the step. The developers stated they just understood everything had to be completed. The CSA said *“it would be no harm in pointing it out, but I mean, to us it's all kind of part of the one process you know. So, we were kind of treating them all of equal importance.”* The fact that the development team did not see these crucial processes as superfluous or laborious and just as necessary was one of the aims of the framework and answers RSQ. 4. However, as addressed in section 5.7.2.1, the developers did acknowledge that much of this was done with input from the researcher. This is a consideration for the usability of the framework without the presence of the researcher and the guidance provided. The development team did state that an interactive example would make this process less overwhelming and easier to understand as previously discussed.

The developers claimed that the process of listing already known security and privacy decisions or constraints in step 2 was useful. The team would *“use basically the best practices provided by those technologies.”* However, they did not think it was useful because they were a SME. They said it was useful *“probably more due to the technology let's say, more so than a SME.”* The developers were questioned that if there was a need to go outside the technologies they have been using, implementing the framework would take longer as they would have to realise the best practices provided by the new technologies. They agreed *“because it would be outside the skill set of the team.”* The researcher considers this relates back to the challenges for developers in SMEs and the constraints due to skill level in the development team from RSQ. 1. It was then proposed to the team, if they needed to adopt a new technology within a project that this process would help in establishing bringing the technologies security and privacy best practices into the project. The team agreed that this process would be useful for that purpose and also for applying the technologies best practices for security and privacy into the development cycle. The conclusion being that the process of listing already known security and privacy decisions or constraints in step 2 was useful for the software development team. The software team understand that technologies provide guidance and recommendations in relation to data security and privacy. Using these resources could reduce the learning curve and time for developers. In addition, having the already known

security and privacy decisions or constraints listed, facilitates the organisation's ability to inform their clients if they request, on the technologies used in the system.

The guidance on constructing DFDs and the security and privacy annotations were determined as simple to use and effective. The development team observed *"because of the particular format...particular style of DFDs, it was useful to have the complete table of explanations there. Also, everyone worked off the same template so all of DFDs would have the same format."* Again, the lack of understanding and consistency in DFD construction for the decomposition of the system was one of the challenges defined from RSQ. 1. For developers inexperienced in TM and system deconstruction, creating a DFD was a challenge. Bringing a consistent set of symbols and procedures made the process stress free for the development team. The team agreed for DFD construction *"all of the examples were clear, and having it all there to use, made it easier and keep it the same all the way through.* It meant also that the team *worked off the same template so you know all of DFDs would have the same format."* This indicates that for every iteration of the system decomposition the DFDs will be consistent.

The addition of the annotations to the DFDs in the framework for both security and privacy were to make the DFDs more visual for both requirements. The objective was to increase visualisation of the security and privacy of data in the DFDs to inspire developers to be more aware of these requirements. The developers stated adding the annotations to the DFDs *wasn't that challenging.* However, it seems that the addition of the annotations achieved their objective. The developers said, *"it's more just putting a lot of thought into it and going through each one, it was just explicit of where we had to do the risk analysis and concentrate on threats. We had already established where the data was, the type of data it was, it was just highlighting it in the DFDs...It was much more visual...you could look at the DFD and see where you had to look at privacy and security."* The team also appreciated the different colours for different boundaries because it was more visual and made it clear which boundaries were external and internal. The CSA remarked, *"It just makes it clearer when you're looking at it, and it makes it easier when you are putting the DFDs together you have to think about what type of boundary it is. This will make a difference to the security, privacy level or how you think about them."* In summary, step 2 of the framework provided everything necessary for the developers to make the first part of the TM process, system decomposition, clear and straight forward.

Step 3 of the framework includes threat elicitation. As realised from the literature review, this is one of the most difficult aspects for developers to comprehend. Threat

elicitation was one of the key areas the software team considered could be refined for usability. The software team clearly supported the threat to attack library from the answer they provided to question 2.7 in the questionnaire. They answered that the threat to attack library *“Provides the user with a jump start on getting started using the framework. Ideal for inexperienced developers with none or very little exposure to similar frameworks.”* This support for the threat to attack starter kit continued in the focus group, when asked if it made the process to find threats easier all of the developers agreed, *“absolutely, without a doubt.”*

However, it did bring challenges for the usability of the framework. The threat to attack starter kit and the security and privacy controls in the implemented version of the framework are presented in Excel. The developers found *“there was a lot of jumping around the place”* when using the Excel document. SD2 said it was *“tedious at times because of the like the jumping back and forth to try and find out which risk you were dealing.”* Essentially the issue was it was an annoyance to navigate. Suggestions included linking each individual threat to attacks to individual controls in dropdown menus with links. The software teams’ answer to question 3.4 *“Do you have any suggestions to improve the framework usability”*, summarised their recommendation on the usability of the framework. They wrote, *“Excel is a great tool for prototyping the framework as it provides infinite possibilities as the framework extends, however doesn’t always provide the best user experience. Develop the framework into an easy-to-use software tool would greatly improve usability.”* This usability difficulty extended to step 6 where the developers would select the controls to mitigate the extracted threats. As previously discussed, the developers suggested applying filters across the framework linking the threat to attack to controls.

The software team did not have any other difficult usability issues with step 3. They found the per-interaction approach very useful in establishing what data is where in the system. SD2 suggested that in addition to the filtering already discussed in section 5.7.2.2, that there is scope for filtering for a specific interaction process in the system. All of the filtering for the framework would be considered as future work for evolving the framework.

Step 4 did not present any usability issues for the software team. The team agreed the risk assessment approach was very clear and straight forward. However, again they did suggest an interactive example. They stated it was very useful for their team that before they completed a step in the framework the researcher would present the step and

the processes in the step. They did note that the tables provided for the risk assessment were good because they were simple with examples and the colours made them *easy to read*. This supports the application of the NIST SP 800-30 risk assessment tables into the framework and RSQ. 3. They stated, *“the more kind of visual stuff definitely helps.”* The team were asked if the security and privacy risk assessment of the framework was achievable for developers inexperienced in this practice. All of the developers agreed, and SD2 expanded in his agreement by affirming *“Absolutely. You know I like that there is a set structure in place to go through and actually put your products against before you even start developing them, before you begin, I wouldn’t even have a clue where to start with this without the framework.”*

The team had no usability issues with step 5. The researcher did consider the necessity of step 5 with the developers because of the feedback from the expert review, discussed in section 5.7.2.2. Additionally, the software team did not have any concerns with the flow of the framework. They considered each step was in the correct order and they did not find any process that was superfluous in any of part of the framework, *“we think it flows naturally enough.”*

5.7.2.4 Summary of Focus Group Findings

The software development team synopsised their general opinion on the framework in the questionnaire stating, *“it gives developers and SMEs a single destination and framework to apply in the SDLC.”* The software team stated in the questionnaire *“The framework has allowed us to systematically go through each process and identify possible threats to each boundary. Having used the framework on the multiples of identified boundaries it becomes very easy to understand and follow.”* In summarising the software teams’ understanding and usability of the framework SD1 said *“it’s a whole lot clearer from whenever we first started...I kind of felt overwhelmed. I thought there’s a lot of stuff in here. But yeah, once you sort of get a step-by-step picture and how things are meant to work your understanding and confidence increases.”* SD2 agreed that it was daunting in the beginning and identified when it became clearer for him. He stated, *“I agree with that whenever we started...identifying different boundaries and that sort of thing, whenever we start doing that, everything started making sense.* The software team did reveal their difficulties in using the framework in its current format. They provided feedback they believed would make the implementation easier for developers and increase the likelihood for uptake and implementation. This included considering several

levels of filtering within the framework. The software team suggested filtering according to the type of development, e.g., API, web app or network. They also suggested filtering the attacks in the threat types to link according to the type of development. They also suggested providing a technical document that could be used once they had built confidence with use of the academic document. In addition, the software team proposed providing a worked example of applying the framework. They recommended putting the worked example into bite size videos that would work through each part of the DPIA and framework steps.

5.8 STATSports Implementation of the Framework

The implemented framework results for STATSports project are provided in Appendix I. This section presents the implementation of the framework and provides a summary of the results and examples of completed tasks.

The software development project applied to this research was the extension of a current STATSports' standalone software product into the cloud. This was the first time the organisation and software development team had brought their product on to the cloud. The development was completed over 20 months, there were 11 Sprint planning meetings and associated retrospectives. The software team had daily stand-up meetings to outline what they had done, what they were doing today and highlight any obstruction to completing their tasks. The researcher presented each aspect of the framework to the software development team before it was implemented. In addition, the researcher was available to the software development team to assist with any difficulties they had in understanding or implementing the tasks of the framework. The implementation of the framework was set in the software development SOP previously outlined in section 4.3.3.

In the planning stages of the project the software development team implemented the backdrop components part of the framework. This implementation took place before the software development process began. It was in the product development stage for STATSports. During this stage the software development team completed the tasks outlined in Table 1 Executive, of the framework. This included defining the scope of the DPIA and what is out of scope of the DPIA. A redacted version of the scope is:

The boundaries of this DPIA are within the data processing cycle of the...System, which includes software and hardware. This is inclusive of both the...desktop application and the cloud storage component that allows for the centralisation and free flowing movement of data within a client's tenant. What is out of scope of this DPIA is the security

and privacy measures the users have on the endpoint technologies. STATSports provide a Minimum-Security Standards Policy guiding the minimal security and privacy requirements to run the software.

The DPIA then required a description of the system and documentation of the stakeholders completing the DPIA and their roles. This task allowed the software team to provide a clear distinction of each persons' role in the project. The final task of this part required the documentation of the information in relation to data and countries associated with the system in Table 2. This enabled the software team to identify the location of the data subjects, the data hosting locations and the associated international data transfer arrangements and grounds for transfer, if any. Links to these documents were included in the DPIA. The software team documented 29 separate locations. This task enabled the software team to gather this information in one place for the first time.

This part also required linking any consultations from the data protection officer in relation to the data being processed and other experts. For example, STATSports documented the consultancy services of an external company to complete pen testing in this section and provided links to previous service level agreements. Any documents that are relevant to the DPIA were also documented. In this item the software team linked the organisational policies relevant to the DPIA, an example being the Systems Access Policy. Other example documents include the technical and organisational design documents and data protection agreements between STATSports and their service providers. The software team completed this part of the framework without any support from the researcher.

Step 1 Contextual Knowledge of the framework includes many of the legal requirements of meeting the GDPR requirements such as the rationale for a DPIA, categorisation of the data being gathered and processed by the system, and administration of privacy through a privacy policy, content awareness and consent compliance, lawful processing. The implementation of this step required support from the researcher. The software development team needed assistance with understanding the privacy and regulatory terminology and determining what they were asked to provide. One of the key results from step 1 was an appreciation on the lawful processing requirements of the GDPR. The framework provides Table 7 Lawful processing to guide compliancy through developed questions to meet GDPR requirements such as; consent, transparency, data minimisation and subject access request. The software team requested a meeting with the researcher to complete this task. A key result for the software development project was a

clear understanding where consent would be obtained and communicating this with the user through the privacy policy. Table 5.4 below provides an example of a requirement addressed by STATSports. Contracts with the clients contains the need for inclusion in a player contract for consent to process their data.

Table 5.4 Example GDPR lawful processing requirements

GDPR Requirement		Notes/Measures
<p>Lawfulness of processing GDPR Article.6 (1) Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</p>	<p>Consent: If you will be relying on consent, will it be given by a confirmation or action by the individual? Where and how is consent attained? How will this be recorded?</p>	<p>Consent is provided through the client/customer Client contract with player</p>

System decomposition in step 2 of the framework was driven by the software architect. The development of the DFDs were completed through specifically scheduled meeting of the software development team and included the product owner. The researcher was not required during this step of the framework. This step resulted in decomposition of the system to Level 2. This include a high Level 1 DFD, with Level 2 providing annotation for both privacy and security in relation to the assets in the software system. The Level 1 DFD contained one boundary, nine processes, three storages and provided the flow of data through the system. In contrast, the Level 2 DFD contained 11 processes, three types of boundaries 12 annotations for security and 10 annotations for privacy. The development of the DFDs was started during the software development planning stage of the SOP using the user stories. Refinement of the DFDs were done in the software requirements analysis stage and the architectural design and software detailed design stage of the software development process. requirements analysis stage of the.

Step 3 threat elicitation was completed after the software requirements analysis stage and the architectural design and software detailed design stage. This process was completed in specific meetings of the software development team and the product owner. This was an added time burden to the software development team. They built time into

the Sprint cycles to facilitate threat elicitation, analysis and prioritisation for an identified process that included personal or health data in the Sprint. The team included defined goals at the start of each sprint for data security and privacy. Anything with regards to data security and privacy would have been planned into the development. The requirements were assessed for risk and checked for consistency, clarity, testability, and traceability. User acceptance criteria and system acceptance test cases were defined and linked to each requirement in Confluence and TestRail. Jira tasks for implementation are created once the product owner signs off the requirements. All of documentation and management of the requirements was done through Confluence. All the tasks that needed to be done would be in put into the backlog. The capacity of the team at the that time was 60 story points. The team decided what task they can bring into the Sprint that make up the sixty story points. The team would talk through each story and break that down into the subtasks. The fact that a security or privacy requirement was part of the Sprint did not impact the number of story points.

The threat elicitation began with the listing the processes of the system that were included in the Sprint cycle. This step included examination of per-interaction processes on the DFDs for potential threats to the system. Each of the processes were documented in the Excel sheet. During the development the software system the software team recorded 10 processes using personal and health data. For each of these processes threat analysis was completed through each of the framework threat categories. Potential attacks that the system could be exposed to due to the threat were accessed by the software team using the threat to attack library. The software team did criticise that the Excel document for this process was poor. They also noted the lack of filtering on the category of attack to the type of development consumed too much of their time.

Chapter 5 Validation of the Framework

The software team noted that without the threat to attack library they would have struggled to complete this task. Table 5.5 presents an example of one process and its threat elicitation in accordance to per-interaction recommended approach to the framework threat categories. The process was given a distinct ID and name, the asset type is outlined and the interaction description is documented. The process was then applied to the framework threat categories. The software team identified potential attacks in within each of the threat categories using the threat to attack library, presented in the table.

Table 5.5 Example threat elicitation

ID	Name	Asset Type	Interaction Description	Origin	Data Flow	Destination	Spoofing	Tampering
43	Machine Boundary - Local Sync Service to Cloud API	- PII Data - System data	Requests to transfer data from the local data to the remote database	Local Sync Service	Local service to remote service	Cloud API	- Relay Attack - Man-In-The Middle Spoofing a file	- Command Injection - Application API Message Manipulation via Man-in-the-Middle
Reputation	Non-Repudiation	Information Disclosure	Insecure Communication	Denial of Service	Elevation of Privilege	Linkability	Identifiability	Detectability
- Insertion of sensitive data into log file - Insufficient logging - Audit logging	- Impersonation authentication	- Sensitive data exposure - Uncontrolled resource consumption - Missing encryption of sensitive - Direct API interaction	- Eavesdropping - Information exposure through query strings in url	- HTTP flood attack - Buffer overflow attack - Slowloris attack - Zero-day attack	- SQL injection - Command injection - Masquerading attack	- Exposure of sensitive information	- Brute force attack	- Eavesdropping - Jamming attack

Step 4 risk analysis and prioritisation were completed within the boundaries of the extracted threat encompassed in the task. Each threat was prioritised for mitigation according to the assessment criteria in this step. The software team would then complete step 5 which was to map the threat back to the security or privacy property through the threat category. The controls to mitigate the identified threat was chosen from the data security and privacy controls.

Table 5.6 provides an example of the results of the risk analysis and prioritisation in relation to the threat and attack presented in Table 5.5 above. This table also provides a list of controls the software team implemented to mitigate the risk. This risk was prioritised as 1, which is the highest level. Therefore, the application of controls within this subtask of development would be completed first.

Table 5.6 Example risk analysis results

ID	Name	Asset Type	Interaction Description	Origin	Data Flow	Destination	Threat	Vulnerability
43	Machine Boundary - Local Sync Service to Cloud API	- PII Data - System Data	Requests to transfer data from the local data to the remote database	Local Sync Service	Local service to remote service	Cloud API	Relay Attack	Access to data packets contain identifiable data that could be tied to a specific athlete
Security	Privacy	Likelihood	Impact	Overall Risk	Mitigation	Priority	Framework Property	DFSPC
Y	Y	Very High	Very High	Very High	Modify Risk	1	Authentication	- 800-53r5 - SC-8 - SC-8(1) - SC-8(2) - SC-8(4) - 15408-2 - FDP_DAU.1.1

The software team extracted 17 vulnerabilities to the personal and health data within this analysis of the system. In total, to mitigate these vulnerabilities there were 28 controls applied to the software system.

The learning curve for the software team included understanding regulatory language and applying it to their software system. The assistance of the researcher impacted their ability to complete this task of the framework. The threat elicitation was not a time-consuming task however, the lack of filters in the threat to attack library did make the identification of potential attacks and vulnerabilities task more time consuming. The development of the DFD including the annotation and boundaries. But the developers appreciated the end result because it was very visual.

5.9 Summary

This chapter describes the approach taken to validate the framework. Additionally, it reports on the findings and modifications made as a result of the expert review. It also

reports on the recommendations made from the software development team that implemented the framework.

The validation is performed as part of the Action Taking, Evaluating and Specific Learning stages of this action research project, presented in Figure 5.13.

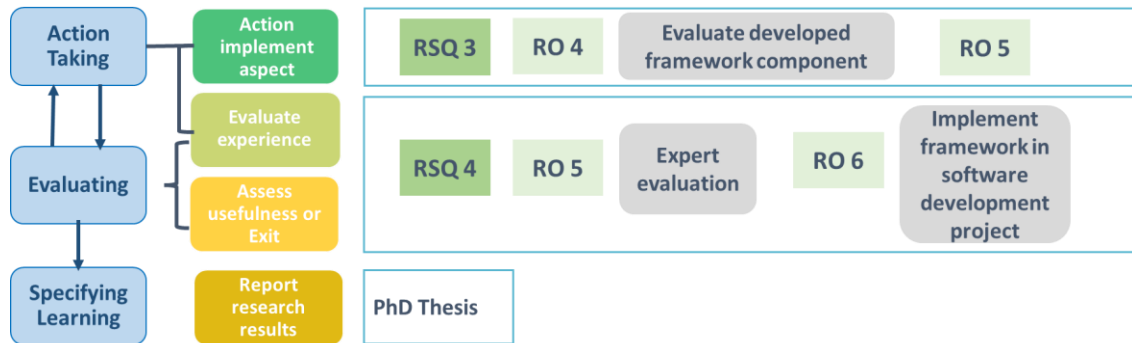


Figure 5.13 Validation as part of action research project

The aim of Action Taking in validation was completed in two parts. The first part was in the development of the framework, which included initial validation with experts and the organisation, discussed in chapter 4. The second part, discussed in this chapter, included validation through expert review, discussed in section 5.6. The aim of Evaluation is to demonstrate the benefit of the framework to solve one or more instances of the challenges established in the literature review and from STATSports. The Evaluation validation was also in two parts. The initial validation was completed by an expert review. The objective was to obtain feedback from an expert on the capability of the framework to meet the requirements of the domain. The second Evaluation validation was accomplished through implementing the framework into a software development project in the organisation. The implementation of the model involved an assessment of the capability of the framework to answer the challenges presented by the organisation. Another validation objective was also to assess the appropriateness of the framework for developers and implementation into a software development environment.

The validation determined that the framework provided ample information and guidance on meeting the GDPR data protection principles. All of the information provided could be applied in software development. Both Dr. Wuyts and the STATSports' software development team commended the depth of the information provided. They also commented that the additional links to further guidance and information provided were an excellent resource. They agreed this would develop confidence in understanding and addressing the GDPR data protection requirements. Dr.

Chapter 5 Validation of the Framework

Wuyts recommended elevating the importance of the legal GDPR requirements in step 1. The software development team did not see the need for this as they assumed it was all important but, acknowledged it would not undermine the framework.

Both Dr. Wuyts and the software development team recognised the framework provided a systematic approach for developers inexperienced in data security and privacy application in development to meet the GDPR data protection requirements. The framework gathered and presented from the disseminated standards, guidance, and best practice an approach feasible for SME developers. Both validations agreed that the risk assessment process was reasonable and achievable for developers inexperienced in this domain.

Dr. Wuyts and the software development team recognised the work completed in implementing the framework could be used to begin to build a data security and privacy library of knowledge, experience about threats, attacks, and mitigation controls.

On conclusion of the validation with Dr. Wuyts, the researcher would examine the application of a compatibility assessment within the framework. This would be built into verifying all the purposes specified up front for collection of the data are the only processes on the data items. The compatibility assessment process would prompt the developers to assess if the processes being developed are compliant with the conditions for the original stated purpose and received consent for processing the personal data.

The researcher agreed the importance of the different mind-set required when threat modeling security and privacy indicated by Dr. Wuyts. The researcher granted that it was important to point this out in the framework and bring it to the attention of the user. The software development team also agreed that a different mind-set is needed. However, they did not find that it was necessary to address the different mind-set requirement in the framework. The software development team maintained that once they understood the personal data collected and where it is in the system that privacy was addressed as this would be treated differently throughout development. The software team saw security as more of an ongoing concern and privacy less so. This reflects the difference Dr. Wuyts discussed, privacy like security is an ongoing concern that requires constant preservation. The researcher clarified this mindset position in the framework.

The future work for the framework will include a technical version of the current academic document. This will also incorporate a quick guide on how to use the framework or an implementation manual for use by developers. There will be an example system implementation with bite size recordings for each step and process to complement

Chapter 5 Validation of the Framework

both the academic and the technical “How To” document. Development of the framework into an interactive product proposed by the software development team, is potential future work project from this research.

The final part of this chapter provided a description on how the framework was implemented within the STATSports software development process. It provided examples of results from the implemented framework. This section also highlighted the difficulties the software development team encounter in implementing the framework.

Part 4 Summary and Conclusions

Part 4 of this thesis contains one chapter as shown in Figure 0.5. Chapter 6 presents a summary of the thesis. The summary revisits the Research Questions and Objectives, the contributions made by the research and their impact on the field and outlines areas of future research. The chapter ends with a conclusion.

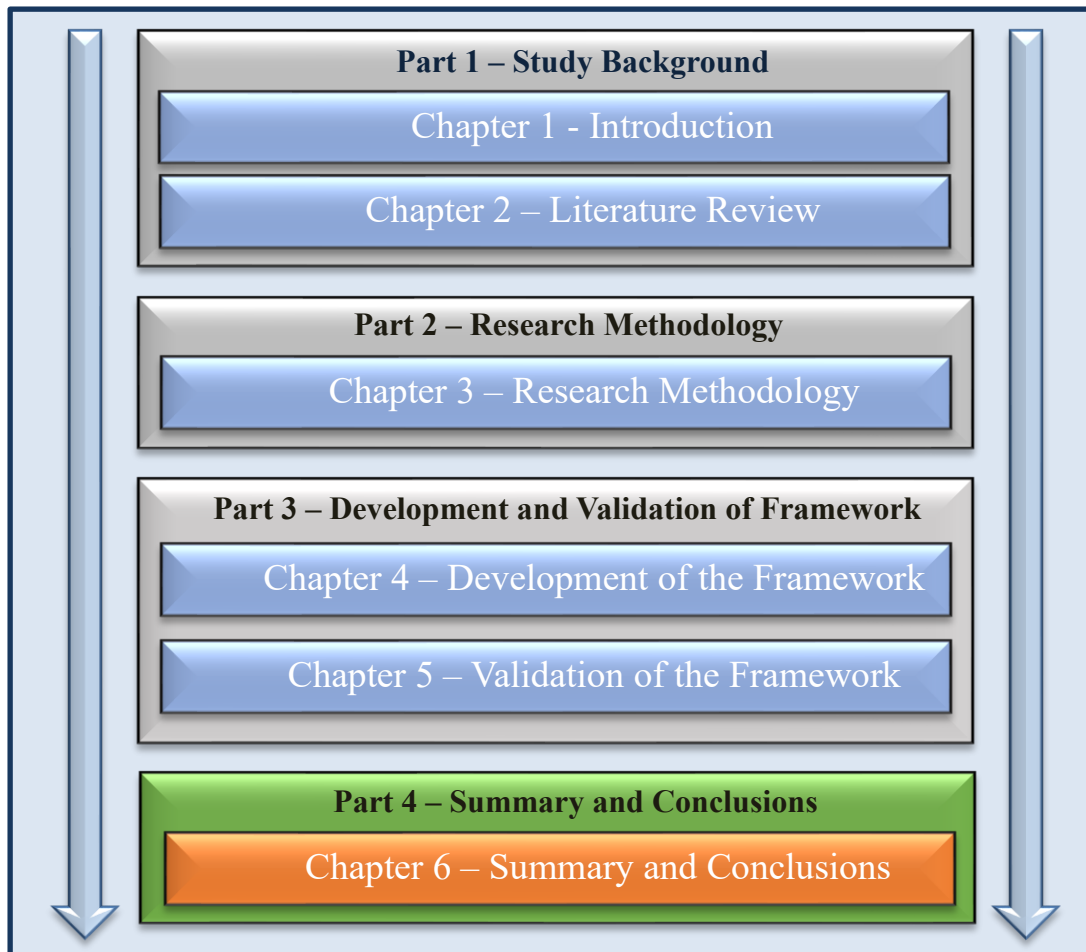


Figure 0.5 Map of the Thesis - Part 4

6 Summary and Conclusion

Chapter six begins by providing a summary of the research project. The chapter then reviews the findings of this study by revisiting the research questions and objectives. The contributions and impact of this research to the domain are examined in the following section. The next section includes an outline of the impact on the field, research limitations and research validity. Finally, the chapter concludes by highlighting some recommendations for areas of future research.

6.1 Summary

The Internet of Medical Things (IoMT) is a fast-growing domain. This growth has been accelerated with the transition of structured healthcare services into care in the community, remote healthcare. There are many advantages to the IoMT such as improved patient care, and access to fuller and more accurate patient information through remote healthcare monitoring in real-time (Al Shorman et al. 2020). However, with remote healthcare the personal and health data associated with the IoMT can potentially flow through a diversity of apps, systems, devices and technologies, and public and open networks. This exposes data in the IoMT to additional attack surfaces, which requires the hardening of the security and privacy of the data. Consequently, as the IoMT grows, cybersecurity risks have risen (Brien et al. 2018; Papageorgiou et al. 2018). In order to mitigate cybersecurity risks both security and privacy of data should be considered from the outset of any software project that processes personal and health data.

Appropriately, personal and health data is bound by regulatory safety, security, and privacy requirements. The EU law on data protection and privacy is the General Data Protection Regulation 2016/679 (GDPR). Any organisation that processes personal data and offer goods and services to, or monitor the behaviour of, EU residents have to comply with the GDPR. With the introduction of the GDPR, privacy has been propelled to an equal status and requirement with security. One of the key GDPR regulation requirements is Article 25 and *data protection by design and by default* (2016, p.23), the GDPR data protection requirements. Article 24(1) of the GDPR (2016, p.22), places the responsibility for the management of data protection by design and by default on the organisation by asserting that *“the controller shall implement appropriate technical and organizational measures to ensure and demonstrate compliance with the Regulation”* and document a

data protection impact assessment (DPIA) (EU General Data Protection Regulation (GDPR) 2016).

The initial phase of the literature review was conducted to gain an understanding of the challenges which are faced by developers in implementing the GDPR data protection, security, and privacy requirements into their software development projects. This initial part of the review revealed that in SMEs the responsibility for implementing data protection requirements frequently falls to the software development team (ENISA 2017). It also showed that applying the regulatory data protection requirements is a struggle for developers due to a variety of diverse challenges (ENISA 2021). The review also uncovered that security and privacy in the healthcare domain is lacking in maturity (Ponemon Institute 2018). These findings were supported in consultations with the STATSports software development team. STATSports recognised the challenges they faced in addressing the GDPR and client data protection requirements and demonstrating compliance.

To address demonstration of compliance, the literature review, then examined the GDPR data protection and DPIA requirements. The review also investigated standards and methods that could potentially assist in demonstrating compliance. The aim of this part of the literature review was to establish what was necessary for and what could demonstrate compliance to the GDPR requirements. It was noted during this part of the literature review that the standards, methods, and guidelines in the medical, security and privacy domains were diverse (ENISA 2021). This added to the challenge for SME developers because establishing the appropriate approach was complicated. Consequently, this research set out with the objective to develop a framework for developers in SMEs, to assist in meeting regulatory requirements for security and privacy of data in flow in the IoMT.

The framework was developed on the principles of the GDPR data protection requirements since the organisation and their clients requesting compliance demonstration were based in the EU. From the literature review it was determined that the framework should be a systematic process targeted at software developers (Dhillon 2011). Many of the standards and current frameworks were at organisational level and not technical development level. Furthermore, the researcher translated the language and requirements of the GDPR data protection principles into language and processes appropriate for software development. From this review, the structure of security and privacy properties were established as a suitable approach for software development. The

framework was structured to demonstrate that the preservation of the properties would determine compliance with the GDPR data protection principles. The decision to take this focus was based on methods for security and privacy risk management in software development identified in the literature review. Threat modeling (TM) was established as the most appropriate software engineering technique to help identify threats, attacks, and vulnerabilities. Additionally, TM facilitates shaping the software system's design to meet an organisations security and privacy objectives and reduce risk (Appari and Johnson 2010). It, therefore, can align with the STATSports ISO 27001 obligations. In order to account for compliance, the framework included a set of categorised technical security and privacy controls to mitigate identified threats. The systemic approach was mapped into the other key GDPR requirement, a DPIA. The requirements for a DPIA were established in the initial part of the literature review.

The framework was developed in a collaborative manner with the software development team from STATSports. During the development of the various components of the framework, validation was performed with two security experts in software development, legal guidance from STATSports' solicitors and RSRC standards experts in the medical domain. Once developed the framework was validated by an expert review and implemented in a STATSports software project. Feedback which was gathered during the validation process has been incorporated into the latest versions of the framework.

6.2 Revisiting the Research Objectives

The aim of this research was to investigate the overall Research Question "*How can the development of a security and privacy risk assessment framework for data in flow in the IoMT assist software developers in SMEs demonstrate compliance with the GDPR data protection requirements in their software products?*"

To meet this aim there were four research sub-questions developed. To answer these research sub-questions there were six research objectives developed. The research objectives will be discussed first as they address the research sub-questions. The research questions and research sub-questions are discussed in section 6.3. The relationship between the research objectives and research questions is shown in Figure 6.1 overleaf.

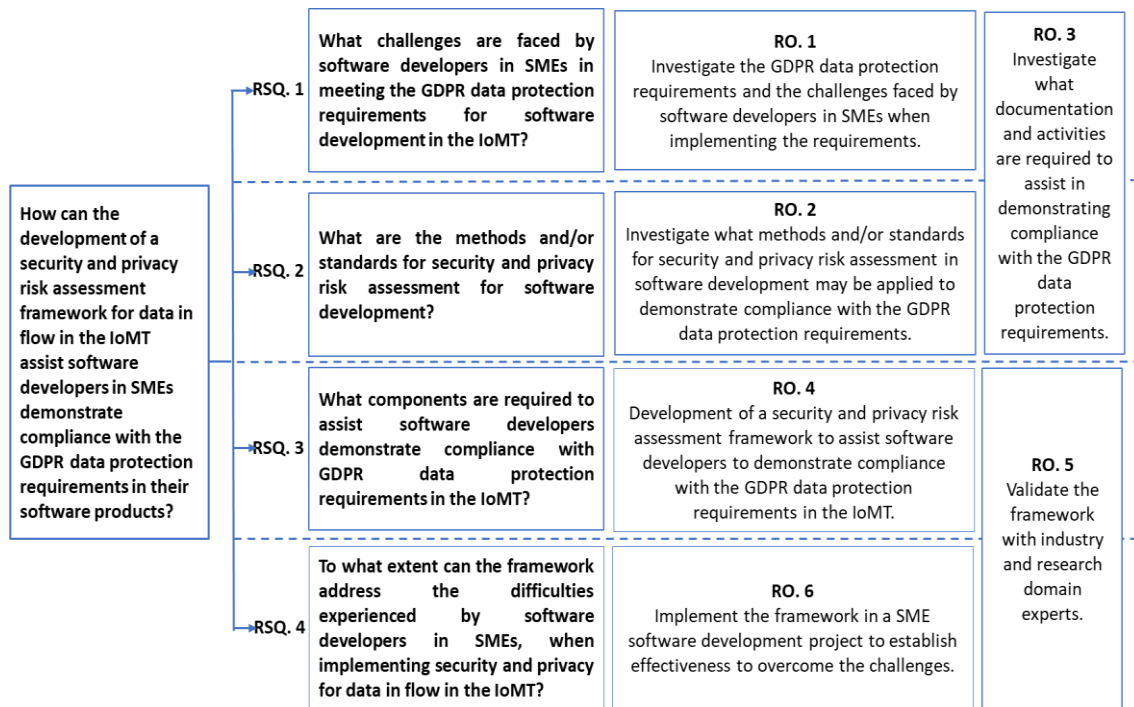


Figure 6.1 Relationship between Research Questions and Objectives

The following Research Objectives were addressed:

RO. 1 Investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs in meeting the requirements.

RO. 2. Investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

RO. 3 Investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

RO. 4 Development of a security and privacy risk assessment framework to assist software developers to demonstrate compliance with the GDPR data protection requirements in the IoMT.

RO. 5 Validate the framework with industry and research domain experts.

RO. 6 Implement the framework into a SME software development project to establish appropriateness to overcome the challenges.

6.2.1 Research Objective 1

The first objective was to investigate the GDPR data protection requirements and the challenges faced by software developers in SMEs in meeting the requirements.

Chapter 6 Summary and Conclusion

To address this objective a review of the literature and the GDPR regulation was completed to investigate:

- The requirements for security and privacy of data in the IoMT;
- The challenges for developers implementing security and privacy in the IoMT;
- The GDPR data protection principles;
- DPIA requirements.

The purpose of the investigation of the requirements for security and privacy of data in the IoMT was to establish the position of each of these aspects as they relate to software development. The literature revealed that both security and privacy requirements for data processing are led by regional regulatory requirements (Horgan et al. 2018). The findings positioned privacy as a fundamental human right that has been placed in the hands of the data subject through the enactment of the GDPR in the EU. The challenge with privacy is, there is no agreement on a set of privacy properties (Pfitzmann and Hansen 2010). Similarly, the findings for security revealed that the traditional CIA properties, although they remain fundamental for security, are no longer adequate in the constantly changing environment of the IoMT (Yaacoub et al. 2020). The challenge for developers, is identifying security and privacy properties sufficient for the IoMT (Hatzivasilis et al. 2019), that will satisfy regulatory requirements. The findings also showed that both security and privacy should be integrated from the inception of a development project security, and privacy by design (Galvez and Gurses 2018). An additional challenge is that both security and privacy models are implemented independently in the current standards and guidance. There is no process that addresses both security and privacy for developers in the software development context.

This objective also aims to understand the challenges faced by SME medical software developers in meeting the GDPR data protection requirements not only in research but also in practice. The literature revealed that while the GDPR embodies data protection, the regulation does not provide guidance on how to demonstrate compliance (Ataei et al. 2020). The literature review investigated the GDPR data protection principles and the DPIA requirements. The literature review revealed that there was no systematic method in existence to assist developers demonstrate compliance to the GDPR data protection requirements. It also revealed there was no framework to assist developers in structuring and using a DPIA.

6.2.2 Research Objective 2

The second objective outlined was to investigate what methods and/or standards for security and privacy risk assessment in software development may be applied to demonstrate compliance with the GDPR data protection requirements.

This section of the literature review examined the standards, guidance, and models for risk assessment from the medical, security and privacy domains. The findings from this part of the literature review shaped the structure of the framework. It also informed the development of the framework properties as a means to demonstrate compliance to the GDPR data protection principles.

The review revealed that there are many different frameworks for assessing security risks at an organisational level. The translation of these high-level organisational risk assessments into the software development domain was not established and caused a significant challenge. In addition, the majority of the risk assessment frameworks focused primarily on security and had deficiencies when used to analyse privacy. The review revealed the AAMI TIR 57 guidance is the risk management framework recommended for information security risk management in software development. However, AAMI TIR 57 only provides guidance on methods to perform information security risk management. This guidance specifically targets the medical device domain as the assessment is based in the context of the safety risk management process ISO 14971. Therefore, AAMI TIR 57 was employed in this research to provide the structure of the research framework. It was chosen because the structure is systematic, is consistent with the risk management processes in other standards and guidelines and it aligns with ISO 14971.

AAMI TIR 57 provides the risk management framework but does not provide the processes to assess the risks to the software system. The review then considered how privacy could be incorporated along with security into a risk management framework. The review revealed TM as the most widely used process in software development to identify potential threats to a system. STRIDE is a well-established systematic security TM. LINDDUN follows the same systematic approach to model privacy threats. Both implement an information flow-oriented model of a system with DFDs. On conclusion of this review, the STRIDE and LINDDUN TMs were determined as appropriate approaches to incorporate into the framework for threat assessment in software development. As TM provides a systematic approach it was established as a suitable

approach to build the risk assessment process upon. The review also indicated a prioritisation for risk mitigation was needed to mitigate the most critical threats. A prioritisation process was included in the framework.

This part of the review also contributed to the establishment of the security and privacy properties to demonstrate compliance with the GDPR data protection principles. The review presented the expansion of the confidentiality, integrity, and availability security properties through review of network security standards. The framework privacy properties were confirmed through a review of the standards and the LINDDUN TM. The security and privacy properties were blended for the framework. The preservation of the framework properties would demonstrate the organisation has implemented a risk assessment process to comply with the GDPR data protection principles. The literature review for this research objective overlapped with Research Objective 3.

6.2.3 Research Objective 3

The third objective was to investigate what documentation and activities are required to assist in demonstrating compliance with the GDPR data protection requirements.

This part of the literature review identified what activities are required for software developers to demonstrate compliance with the GDPR data protection requirements. This included the legal requirements of the GDPR in addition to the data protection requirements. This objective incorporated aspects from all parts of the literature review. This examination promoted the development of the six stepped systematic approach of the framework. Each step of the framework process has activities at key parts of the development process to address the GDPR data protection and legal requirements. The GDPR data protection requirements are addressed by the protection of the framework properties. The TM approach extracts potential threats that could violate the properties and the risk assessment processes determines if risk mitigation is required and prioritise the mitigation of the pertinent threats. The six stepped framework is built into the GDPR legal requirements of a DPIA. This facilitates the provision of evidence that data protection by design and default has been applied to the software development project.

The structure of the DPIA was established through the review of the GDPR requirements, government, and regulatory guidance. This included the necessity to provide evidence on why your product requires a DPIA. The review also revealed the legal aspects of the GDPR data protection principles. These include lawfulness, fairness and transparency, and the lawful processing analysis for personal data. It is a requirement

to determine whether data processed by an IT system is personal data or not. There is also the need to consider if the data being processed can become personal data as the result of such processing. These items were identified as required for inclusion in the framework to address the key GDPR legal requirements.

One of the key aspects of the GDPR found through the review, was risk assessment (ENISA 2017) and therefore, inclusion was needed in a DPIA. It is required that all data protection risks, and applicable safeguards should be identified at a high level for any system processing personal data. The risk assessment would demonstrate that all risks to the rights of the data subjects have been considered before processing any personal data. As noted in the previous section, the risk approach brought into the framework was TM. However, whilst TM provides the method to establish the threats to a system, the review revealed that a risk assessment approach was also needed to evaluate and prioritise the extracted threats for mitigation. To establish the appropriate risk assessment approach for software developers the review looked at the current frameworks. This review revealed the current frameworks were pitched at the organisational level. The AAMI TIR 57 guidance recommended the NIST SP 800-30 guidance for conducting risk assessments. This guidance provides a variety of approaches and because the framework is for developers inexperienced in security and privacy the approach considered most suitable was the qualitative approach.

6.2.4 Research Objective 4

The fourth objective outlined was the development of a security and privacy risk assessment framework to assist software developers demonstrate compliance with the GDPR data protection requirements in the IoMT.

The framework was developed in response to the challenges identified through research objectives 1, 2, and 3. The framework was developed using an action research (AR) approach. The AR approach places the emphasis on an interactive investigation process that balances problem-solving actions implemented in a collaborative context with research. The researcher collaborated with the STATSports software team, software security experts and a SME IoMT organisation to develop the framework to solve the problems identified through the literature review and in STATSports. The AR approach facilitated the incorporation of feedback from expert reviewers and feedback gathered during the implementation of the framework. This ensured that the developed artifact, the framework, is suited for use in the software development environment. Focus groups

were used extensively during the research process. This ensured that the perspectives of various stakeholders were considered in the development and validation of the framework.

6.2.5 Research Objective 5

The fifth objective outlined was to validate the framework with industry and research domain experts.

One part of the validation of the framework was conducted through the use of expert review. Industry expert reviewers were used during the development of the framework and an expert review was completed on the developed framework. The industry experts were chosen to review specific parts of the framework during the development stage. These experts had over 10 years' experience working in implementing security in IT systems. Two software security experts an IoMT organisation and senior members of the RSRC validated the DFSPCs. On reflection much of the validation was completed by experts specific to security. Therefore, an expert review was completed of the developed framework by Dr. Wuyts the developer of the LINDDUN TM for privacy. The focus of this phase of the expert review process was to ensure that the framework: was consistent with the requirements of the data protection principles, addressed the requirements for security and privacy in the IoMT and was suited for use in a software development context.

6.2.6 Research Objective 6

The sixth objective outlined was to implement the framework into a SME software development project to establish its effectiveness to overcome the challenges identified through the literature review and at STATSports.

While the achievement of research objective 5 validated that the framework components fulfilled security and privacy requirements in the IoMT research objective 6 focuses on ensuring that the framework is applicable for use in a software development environment. In order to achieve this, the framework was implemented in a STATSports software development project. The implementation highlighted a number of obstacles in applying the framework from the software team.

The software team revealed the amount of information presented in the framework was initially overwhelming. However, with feedback from the researcher and completing the individual components of the framework the software team's understanding and

confidence increased. The software team provided feedback they believed would make the implementation easier for developers. This feedback included considering several levels of filtering within the framework. They proposed filtering according to the type of development, e.g., API, web app or network and extending this filtering to the attack types. They indicated this would improve the usability of the framework and potentially increase the uptake in implementation.

Another recommendation provided by the software team was the development of a technical document that could be used once they had built confidence with use of the academic document. The software team appreciated the broad information and links in the academic document and suggested maintaining this document. However, they suggested as their confidence and experience increased a less information intense technical document would be more useable and sufficient. An additional recommendation also proposed was a working example in applying the framework with accompanying bite size videos working through each part of the DPIA and framework steps.

The feedback was received from participants through a focus group. Much of the feedback from this focus group would be applied to future work with the framework.

6.3 Revisiting the Research Questions

The focus of this research was to address the overall research question:

How can the development of a security and privacy risk assessment framework for data in flow in the IoMT assist software developers in SMEs demonstrate compliance with the GDPR data protection requirements in their software products?

In order to address the overall research question there were four research sub-questions developed at a lower level. The four research sub-questions are:

RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements in software development in the IoMT?

RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?

RSQ. 3 What components should be in a framework to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?

RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?

The following sections present how each research sub-question has been addressed. The research sub-questions have been addressed through the achievement of the research objectives discussed in section 6.2.

6.3.1 Research Sub-Question 1

Research sub-question 1, presented in Figure 6.2, has been addressed through the achievement of research objectives 1 and 3.

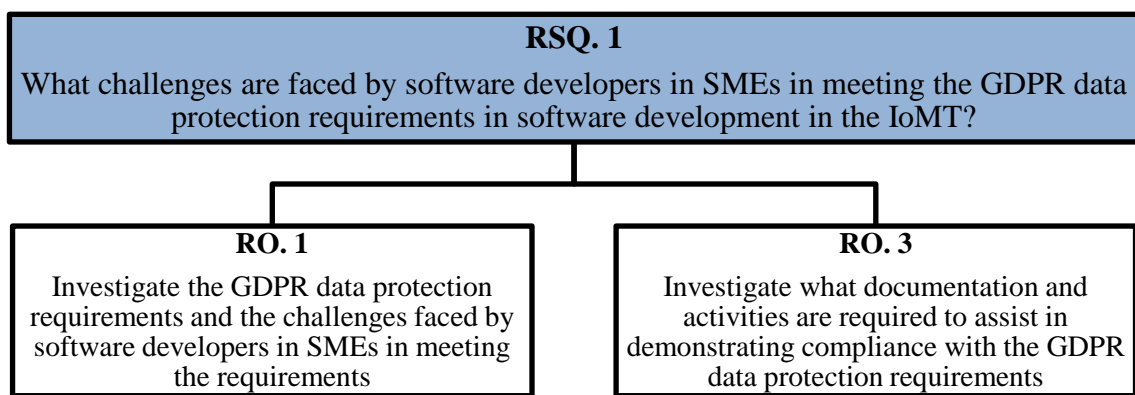


Figure 6.2 RSQ. 1 addressed by RO. 1 and 3

This research sub-question was defined to identify the challenges that are experienced by developers of SMEs in demonstrating security and privacy of data in flow in the IoMT. This question was also posed to identify the challenges that are experienced for developers in demonstrating compliance with the GDPR data protection requirements.

The literature review revealed the challenges experienced by software developers in SMEs. The literature review, also revealed the challenges experienced in addressing and demonstrating compliance with the GDPR data protection requirements. In addressing these challenges, developers need to incorporate many considerations ranging from observing to GDPR legal requirements, security and privacy risk management, threat identification and mitigation. The findings of the challenges showed that there is not a single systematic approach for developers to assist them in addressing the challenges. The identified challenges are consistent with addressing security and privacy in software development and meeting the GDPR data protection requirements communicated by STATSports. The research focused on answering the following challenges:

- The lack of knowledge in SME software development teams on how to build GDPR compliant products and meet the GDPR data protection principles. The GDPR data protection principles were mapped to security and privacy properties that require preservation. The research also established the requirements of a DPIA;
- Understanding the appropriate standards and guidance to implement and meet the requirements for data security and privacy risk management in software development and in the IoMT. Assembling the appropriate standards and guidance for software developers in SMEs to demonstrate the security and privacy of the data in their software products. The research established the domains and possible standards and methods that could be applied to meet the GDPR data protection requirements in software development;
- Establishing a systematic approach for SME software developers to apply both security and privacy simultaneously in software development to meet GDPR data protection requirements. The research established a risk assessment approach which included threat modeling to adapt the process to software development.

Research sub-question 1 was addressed by the investigation carried out during Research Objectives 1 and 3.

6.3.2 Research Sub-Question 2

Research Sub-Question 2 presented in Figure 6.3, is addressed by research objectives 2 and 3 and builds on the findings of research objective 1 and research sub-question 1.

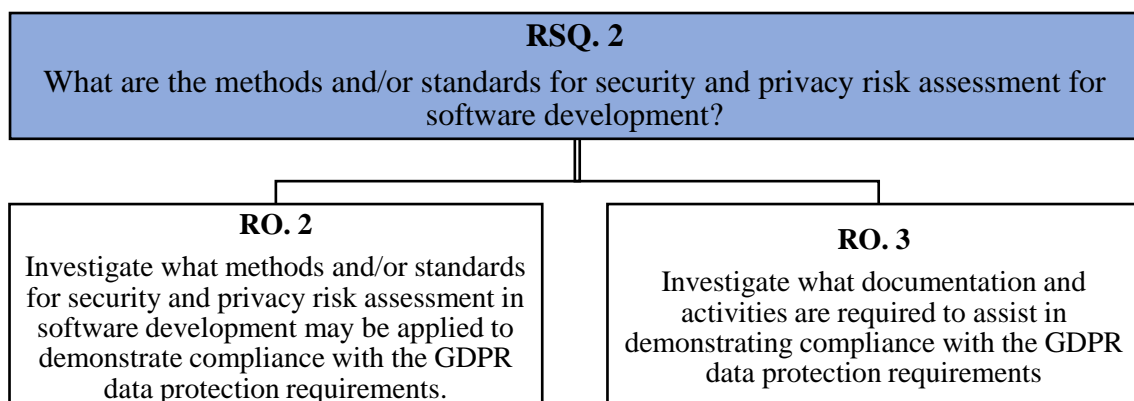


Figure 6.3 RSQ. 2 addressed by RO. 2 and 3

To demonstrate consideration of security and privacy in software products and systems, research objective 2 examined the standards and methods for security and privacy risk

Chapter 6 Summary and Conclusion

assessment during software development. This was to align with the GDPR requirement of security and privacy by design and by default. It was determined in order to demonstrate compliance with the GDPR data protection requirements the legal and technical necessities of the regulation would need to be addressed. In addition, one of the key requirements for a DPIA is a risk assessment. These requirements have been reviewed in the discussion on research objective 3 in section 6.2.3 above. The legal aspects of the GDPR data protection principles included; developing rationale for a DPIA, developing a privacy policy, ensuring consent for processing personal data, categorisation of the collected personal data and upholding the processing of the collected personal data particular to the consent obtained for the collection and processing of the personal data. It was determined that a multifaceted approach was needed to address the research sub-question. The literature determined there was no one approach to address security and privacy risk assessment in software development at the same time.

To manage risk assessment, the research framework adopts all phases of AMMI TIR57. AMMI TIR 57 was chosen because it provides guidance on methods for security risk management for a medical device. It focuses the risk assessment on the identification, analysis, and evaluation of all potential security aspects. It is also based and operates in tandem with the medical safety risk management process required by ISO 14971. The framework expands the scope of AAMI TIR 57 to include both security and privacy. Figure 6.4 overleaf, presents the framework steps mapped to the AAMI TIR 57 recommended security risk management framework with privacy integrated.

To analyse a system's architecture to identify the assets requiring protection and uncover potential risks to the assets, the framework used TM. TM is about identifying potential threats to the system being developed and by understanding the threats it is possible to determine its vulnerabilities. Again, security and privacy were treated individually in TM. The framework combined the TMs STRIDE, used for security, and LINDDUN, used for privacy. This combining was completed through the framework properties where each threat correspondent to the threat types of the TMs. The risk assessment approaches adopted to the framework were from NIST SP 800-30. A qualitative risk assessment approach was used because it was seen as more appropriate for threat analysis and suitable for developers inexperienced in risk assessment.

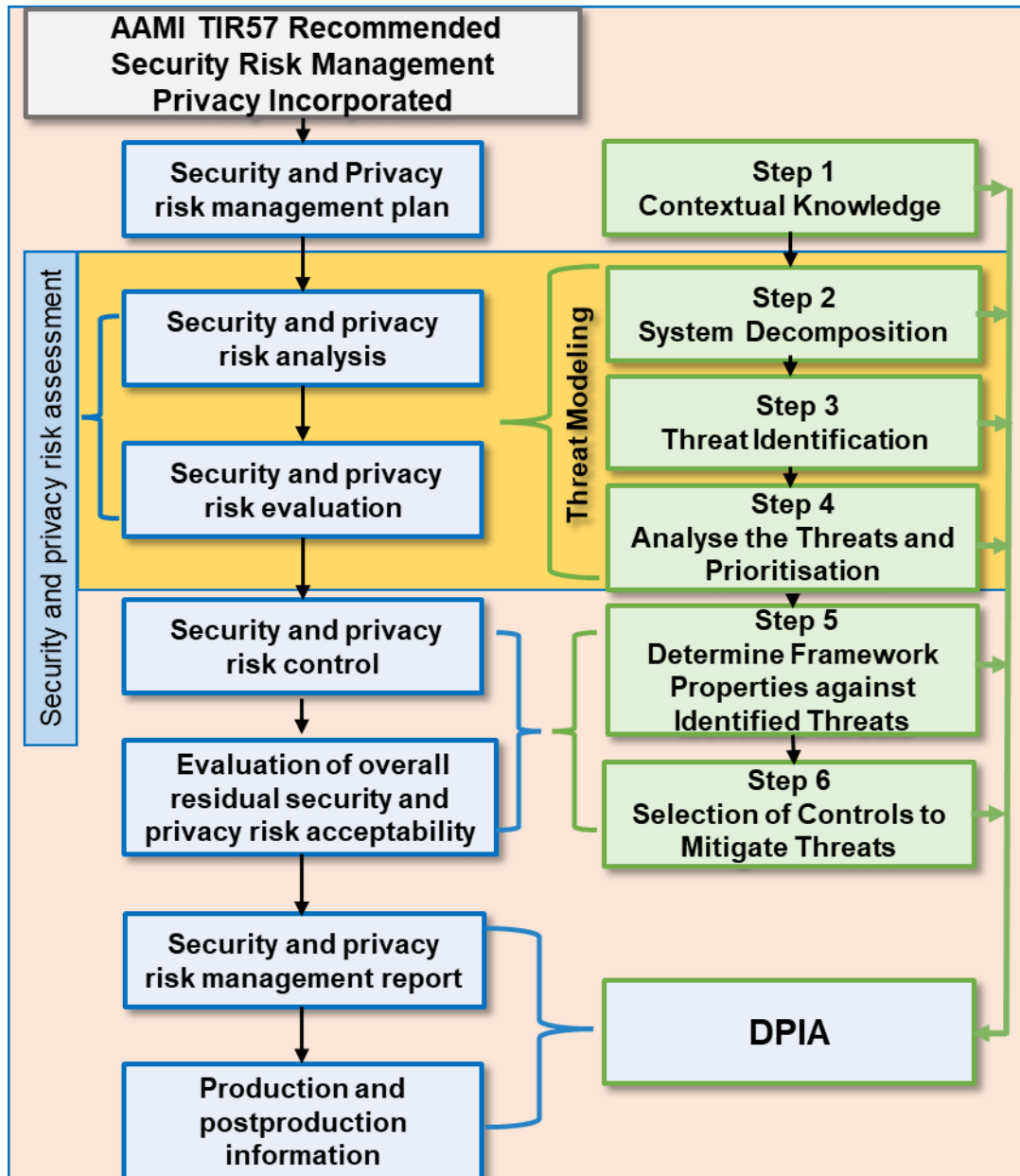


Figure 6.4 Framework steps mapped to the AAMI TIR 57 recommended security risk management framework with privacy integrated

6.3.3 Research Sub-Question 3

Research sub-question 3, presented in Figure 6.5, is addressed by research objectives 4 and 5. This RSQ builds on the findings of research objectives 2 and 3 and research sub-question 2.

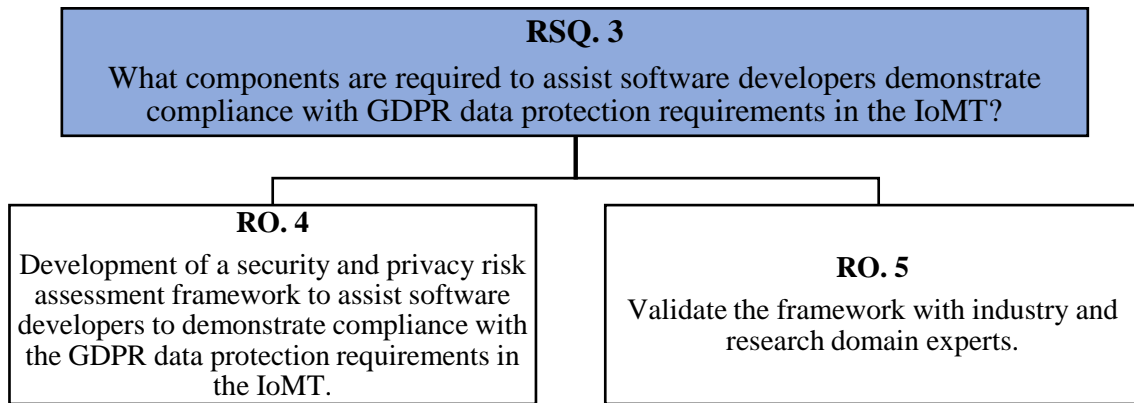


Figure 6.5 RSQ. 3 addressed by RO. 4 and 5

As a consequence of research sub-question 3, a systematic approach for the performance of a risk assessment that includes both security and privacy was developed. The approach incorporated addressing the GDPR data protection principles within the development process providing demonstration of the regulatory requirements. One of the objectives of this research was to apply the GDPR data protection principles to the software development process through a framework that can be used by developers. The development of the framework components was completed with STATSports and two software security experts. For the development of the security and privacy controls component of the framework validation was completed at this point. This validation was completed by internal experts from the RSRC, the security developers and by a medical app software development organisation. Having determined what, the framework should contain, research objectives 4 and 5 were concerned with the development and validation of the components of the framework.

The framework is documented in a DPIA in the form of a word document and an accompanying Excel document. The DPIA is the academic document that provides the information required to complete the different steps. The DPIA documents the background information for the GDPR legal requirements of the software development project. The accompanying Excel document provides the tables to document the steps of the framework, the DFSPCs, and the threat to attack starter kit library. The framework is provided in Appendix H.

6.3.4 Research Sub-Question 4

Research sub-question 4, presented in Figure 6.6, is addressed by research objectives 5 and 6 which consisted of an expert review and the implementation of the framework in a software development project.

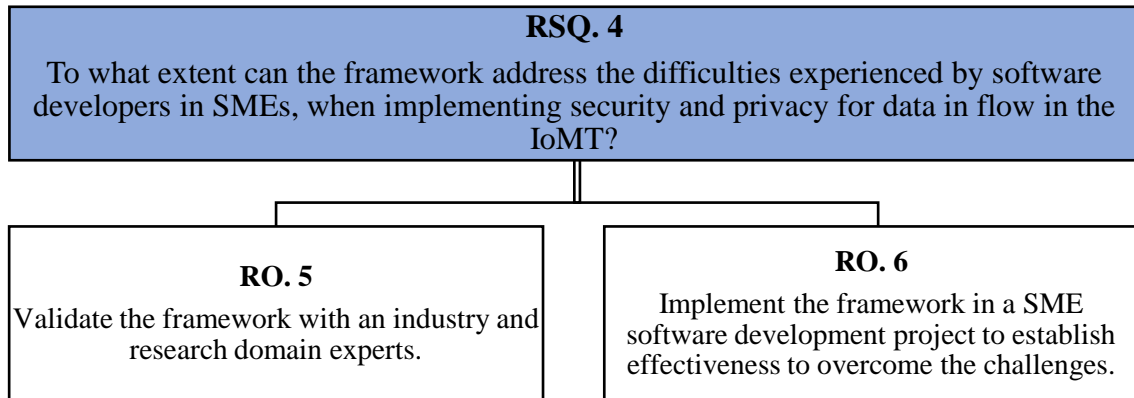


Figure 6.6 RSQ. 4 addressed by RO. 5 and 6

The development of the framework included experts from the security domain. To ensure the framework addressed the privacy requirements a second stage validation of the framework was performed in RO. 5 to fully address research sub-question 4. The privacy expert developed the LINDDUN privacy TM incorporated into the framework. This validation revealed shortcomings in the overall framework. Several recommendations were made to address these shortcomings. It was not possible to implement all of the recommendations in the course of this study, some were identified as future research which are discussed in section 6.8. The recommendations implemented during this study included:

- The GDPR legal features of the framework were elevated in the framework to assert their importance in the components table at the beginning of step 1;
- The different mind-set required when threat modeling security and privacy. Dr. Wuyts stated it is important to specify this difference in the framework and highlight it to the user. A short addition was added to step 3 of the framework to convey the different mind-set required when threat modeling security and privacy;
- Adding a sentence to step 1 to clarify the privacy policy is a process that is continued through the product and data lifecycle.

In addition, the researcher conducted a final focus group based on the questionnaire with the STATSports software development team to evaluate RO. 6 and to part answer

RSQ. 4. The software team summarised their opinion on the framework in the questionnaire stating, “*it gives developers and SMEs a single destination and framework to apply in the SDLC.*” Their feedback was predominantly on the usability of the framework and making the framework implementation easier for developers. The software team’s feedback was focused on increasing the likelihood for uptake and implementation. It was not possible to implement their recommendations in the course of this study and they were identified as future research, discussed in section 6.8. The software team did express their difficulties in using the framework in its current format in their feedback. These difficulties included having too much information to get through to find the pertinent piece. They recommended considering several levels of filtering within the framework. The filtering proposed included using the type of development, e.g., API, web app or network. They also suggested filtering the attacks in the threat types to link according to the type of development. Other recommendations included providing a technical document and a worked example applying each step of the framework with accompanying bite size videos.

6.3.5 Overall Research Question

An overall research question was posed at the beginning of this research as follows:

How can the development of a security and privacy risk assessment framework for data in flow in the IoMT assist software developers in SMEs demonstrate compliance with the GDPR data protection requirements in their software products?

The research objectives and questions discussed have contributed to addressing this overall research question. In order to answer the overall research question, an investigation was completed on the challenges faced by developers in SMEs demonstrating data security and privacy implementation within their IoMT products to meet GDPR data protection requirements.

This investigation revealed that developers in SMEs have many challenges to implement and demonstrate security and privacy in their software products to meet GDPR data protection requirements. The research conducted showed that to address the challenges, many components have to be considered. Furthermore, because developers of SMEs generally are less experienced and have limited resources, consideration must

be provided to the steep learning curve required in understanding, applying, and delivering evidence of compliance with the GDPR data protection requirements.

The research concluded that the approach required had to meet the GDPR legal and data protection requirements. The research showed the approach should be designed for developers, standardised, and systematic to support implementation. This identified the need for a framework that could be used by developers to establish the software project or product has applied security and privacy controls to meet the GDPR data protection requirements. For the development of the framework, processes and activities were established through the research positioned specifically for developers. The approach was documented as a DPIA to meet the GDPR requirements for processing personal data. The development of the framework was completed in collaboration with the STATSports software development team.

The framework was implemented into a STATSports software project to develop a new cloud feature to a current product. The framework was also reviewed by an international expert in privacy Dr. Wuyts. Dr. Wuyts has more than 10 years' experience in security and privacy in software engineering and threat modeling, privacy engineering, security engineering and data protection. Dr. Wuyts developed the LINDDUN™ as part of her research. On conclusion of the implementation and expert review the framework was understood as a valuable resource for SME development teams with limited to no knowledge in demonstrating compliancy with the GDPR data protection principles and their requirements. The STATSports software development team stated that they *“liked that there is a set structure in place to go through and actually put your products against before you even start developing them, ...we wouldn't have a clue where to start with this without the framework.”* The implemented framework results for the STATSports project are provided in Appendix I

6.4 Research Contributions

This research has made several contributions in a number of areas. This section will discuss the contributions of this research to the:

- Literature and research community;
- To the knowledge of the application of security and privacy risk assessment in software development;
- To the knowledge of demonstrating compliance to the GDPR data protection principles to the SME software development community.

6.4.1 Literature and Research Community

This research through a literature review and feedback provided by STATSports, identified many challenges for SMEs and their developers in demonstrating compliance to GDPR data protection requirements. Additionally, this research has defined the challenges organisations encounter when implementing data security and privacy in their IoMT software products. This research provided a validated framework to address some of the challenges. This framework aims to assist SME developers to overcome the challenges of understanding the GDPR data protection requirements, what procedures are needed to demonstrate compliance and how to implement these procedures. Overcoming these challenges will improve SME organisations compliance with the data protection regulatory requirements. The final activity of the action research process is specifying learning. This has been achieved in this research through the reporting of the research results. The research has been published in international conference proceedings and in two international journals. The research was also presented at an international thematic workshop, in Edinburgh, Scotland. The researcher also presented the research as a guest speaker at 2021 European Medical Device Cybersecurity Conference. The resulting publications and mapping to the research-sub questions are presented in Figure 6.7 overleaf.

<p>RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements in software development in the IoMT?</p>	<p>Treacy, C., McCaffery, F. and Finnegan, A. (2015). Mobile Health & Medical Apps: Possible Impediments to Healthcare Adoption. In: eTELEMED, The Seventh International Conference on eHealth, Telemedicine, and Social Medicine. Lisbon, Portugal: IARIA, 2015, pp.8–11.</p> <p>Treacy, C. and McCaffery, F. (2016b). Medical Mobile Apps Data Security Overview. In: SOFTENG: The Second International Conference on Advances and Trends in Software Engineering. Lisbon, Portugal, pp.123–128.</p> <p>Treacy, C. and McCaffery, F. (2016a). Data Security Overview for Medical Mobile Apps Assuring. <i>International Journal on Advances in Security</i>, 9(3 & 4), pp.146–157.</p>
<p>RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?</p>	<p>McCaffery, F., Özcan-Top, Ö., Treacy, C., Paul, P., Loane, J., Crilly, J. and Mahon, A.M. (2018). A Process Framework Combining Safety and Security in Practice. In: <i>Communications in Computer and Information Science</i>.</p>
<p>RSQ. 3 What components should be in a framework to assist software developers demonstrate compliance with GDPR data protection requirements?</p>	<p>Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: <i>26th EuroSPI Conference</i>. Edinburgh: Springer Links. Available from: https://2020.eurospi.net/index.php/workshop#.</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2020a). A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In: Messnarz, R. et al., eds. <i>Systems, Software and Services Process Improvement: 27th European Conference, EuroSPI 2020</i>. Springer Nature, pp.107–119.</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2020b). Developer driven framework for security and privacy in the IoMT. In: <i>ICSOFT 2020 - Proceedings of the 15th International Conference on Software Technologies</i>. Springer, pp.443–451.</p>
<p>RSQ. 4 To what extent can the framework address the difficulties experienced by SME medical software developers when implementing security and privacy for data in flow in the IoMT?</p>	<p>PhD Thesis</p> <p>Treacy, C., Loane, J. and McCaffery, F. (2021). Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things. In: <i>4TH International Clinical Engineering and Health Technology Management Congress (ICEHTMC)</i>. Lake Buena Vista, FL: AAMI.</p> <p>Treacy, C. and McCaffery, F. (2021). Assisting Software Developers to Meet GDPR Data Protection and Privacy Requirements for their IoMT Products. In: <i>2021 European Medical Device Cybersecurity Virtual Conference</i>. Available from: https://www.medtechcybersecurity.com/</p>

Figure 6.7 Publishing of research results

These contributions are important for both software development and cybersecurity practitioners and the IoMT research community. This section discusses the contributions of this research in the following areas:

- To the knowledge of the application of security and privacy risk assessment in software development in SMEs;
- To the knowledge of demonstrating compliance to the GDPR data protection principles to the software development community.

6.4.2 To the Knowledge of the Application of Security and Privacy Risk Assessment in Software Development

The literature review placed the use of health data within the overall context of the internet of things, the Internet of Medical Things (IoMT). This enabled the challenges which have been associated with the application and demonstration of security and privacy of data in the IoMT to be placed in the context of the SME software developer. The literature review with feedback from STATSports, revealed the need for a method intended for software developers to assist in demonstrating the application of security and privacy of the data in their IoMT software systems or products to meet the GDPR data protection principles. The framework provides a systematic approach developed from established standards and best practice to apply a security and privacy risk assessment for potential threats to data in flow in the IoMT.

The literature review revealed a multitude of standards and best practices related with data security and privacy dispersed through several domains. One of the challenges for developers and SMEs is identifying the applicable standards and best practices to follow. Secondly, the standards and best practice are difficult to understand and arduous. Moreover, while the literature review identified numerous standards and approaches for risk assessment it revealed many operate at an organisational level. One of the challenges for developers is translating these risk assessment standards to software development practice. Additionally, many of the risk assessment standards are generic and do not provide directed approaches and processes to apply to software development. All of these add to the challenge for developers inexperienced in security and privacy in SMEs who have limited knowledge and resources. There is not a single approach identified in the literature review that provides an approach to implement both a security and privacy risk assessment for software development at the same time. In the existing frameworks, privacy protection and threats are not emphasised. This framework emphasises the

Chapter 6 Summary and Conclusion

requirement to address privacy alongside security. Frameworks such as PASTA do not highlight the necessity for addressing threats to privacy. PASTA focuses on the business objectives. This framework is focused on the software developer and supporting those that are inexperienced. PASTA can be expensive and time-consuming to implement, especially for smaller organisations or those with limited security resources. This framework is built on regulation, standards and well-established models.

A significant contribution of the framework is in bringing together the dispersed standards, best practice, and guidelines into a standardised systematic approach specifically for software developers. The framework has interpreted the language of the standards, best practice and guidelines into a single approach that is applied at software development level. A further significant contribution provided by the framework is the development of an approach to consider both security and privacy data protection. The framework has been developed in accordance to the AAMI TIR 57 risk assessment guidance. AAMI TIR 57 provides guidance on methods to perform information security risk management for a medical device. The framework applies the AAMI TIR 57 risk assessment approach to incorporate both security and privacy. This research has provided a systematic approach to address the gap of a simultaneous security and privacy risk assessment for software development.

Furthermore, the research has compiled the best practice for security and privacy risk assessment during system decomposition. The framework provides a clear set of components, symbols, and boundary identification for data flow diagrams. This is supported by the inclusion of annotations that indicate data security and privacy position on the data flow diagrams. The STATSports software developers valued these additions. The type of data and where it was in the system was more visual and the data flow diagrams more informative.

The research provides a categorised set of security and privacy controls developed from security, privacy and medical standards that can be applied to mitigate extracted threats. This provides a complete risk management process encompassing identification, assessment, and mitigation of risks to the software system. This supports the demonstration that appropriate controls have been implemented to mitigate the identified threats to the software system.

A key contribution of this research is the threat to attack type starter kit. This library was developed after the researcher conducted a workshop at the 26th EuroSPI Conference in 2019 (Treacy and Macher 2019). During the workshop the implementation

Chapter 6 Summary and Conclusion

of the framework came to a stop when it came to threat analysis. All of the participants could follow the framework to this point. They did not have the knowledge, experience or resources to continue. The participants of the workshop were based in the medical device and software development domains. There were software engineering participants however, they had little to no experience in threat analysis for security and privacy. The researcher completed a retrospective literature review and discovered there was a gap in research and resources mapping threat categories to attacks. The library was developed as a response to the lack of progress in the framework implementation at the workshop and this retrospective literature review. The library can be used as an independent resource outside the framework as it is developed on established TMs in security and privacy and mapped to established and renowned attack libraries from OWASP and CWE. There is also potential to map other well-known libraries to expand this resource. The library can be updated when changes are made to these libraries. For inexperienced software developers the library is an invaluable resource to support implementing threat analysis and build confidence and experience. The threat to attack library was essential for the STATSports software development team to fully implement the framework. The software team commented that they would have found this task much more difficult if they did not have these resources and had to find the attack types. Following the implementation of the framework the STATSports software development team stated the threat to attack library starter kit is really a necessity. They acknowledged that people could probably figure it out, but it would be a difficult task. Dr. Wuyts suggested the threat to attack type starter kit was a particular strength in this research *“especially for people new to it”*.

An additional, contribution of this research is a systematic approach for software developers to assist in demonstrating security and privacy by design and default in the software development process. The focus for software developers is completing development tasks within the sprint. Unless there is a process included in the development sprint for security and privacy, these requirements would not be completed. This research provides a framework for software developers to include security and privacy requirements into development. Many SME software development teams do not have a dedicated resource within the development team addressing security and privacy requirements. This largely means they do not have the experience, knowledge or time resources to refine a process in their development. The development team lack the understanding to know where to start and would not have the time to research and learn

how to begin or complete the process to meet security and privacy requirements. This is a key issue for development teams generally but, particularly within the context of small companies where the responsibility is in getting the product developed and the teams' priority is to meet the deliverables for a particular sprint. Therefore, without the framework the development team would not have been able to address the security and privacy requirements. The framework contribution is to enable an SME, which would not have the time to do this themselves, to simplify the process of meeting the GDPR data protection principles as part of their day-to-day work. Essentially the framework simplifies the incorporation of data security and privacy into the SME developers' day to day work.

One of the key benefits described by the STATSports development team was having all of this data protection information in relation to software development on hand, controlled and in one place. They stated that the organisation is receiving more requests from their clients to complete data security and privacy audits. The clients are auditing STATSports as a processor of personal and sensitive data to ensure there are appropriate controls in place for data protection. STATSports has noted that these data protection audits are becoming customary. The clients' motivation for the data protection audits include; use of the cloud in STATSports product; the greater legal and regulatory requirements around the world; increased cybersecurity threats; requirements from cybersecurity insurance companies and heightened awareness among their data subjects and consumers. The advantage of having the DPIA document that demonstrates the application of data protection through the software development process has benefited STATSports in meeting the data security and privacy audits. The software team can provide the information to demonstrate meeting data protection requirements from the DPIA. The team have used the data categorisation and lawful processing tables DFDs, risk assessments and controls, in addition to other parts of the framework, to provide evidence to clients for the data security and privacy audits.

6.4.3 To the Knowledge of Demonstrating Compliance to the GDPR Data Protection Principles to the SME Software Development Community

The introduction of the GDPR and its data protection requirements has changed the landscape for data privacy. Data privacy has been elevated to an equal position alongside data security. The GDPR requires that any software system or product processing personal data must demonstrate they have put appropriate controls in place to meet the

data protection principles and protect the rights of data subjects. The literature and STATSports' feedback identified challenges in understanding the security and privacy requirements and how to implement these requirements in software development. This research has mapped the GDPR data protection principles into security and privacy requirements that can be applied to the software development process. The research translated the GDPR data protection requirements for both security and privacy into properties. The preservation of these security and privacy properties demonstrates the software system has complied with the GDPR data protection principles. This includes the legal aspects of the GDPR data protection principles. This research has provided components to support developers in ensuring the legal obligations for processing personal data are addressed in software development.

Documenting the framework process provides evidence that a software development project has implemented the appropriate technical and organisational measures to ensure and demonstrate compliance with the regulations (ICO 2020). A requirement of the GDPR is a DPIA. A DPIA is an effective way to assess and demonstrate the project's compliance with the data protection principles and obligations (ICO 2020). This research has structured the documentation of the implementation of the framework to meet the DPIA GDPR requirements. This is a considerable contribution to SMEs and their developers. The literature has found that these groups struggle in distinguishing the GDPR data protection principles and implementation of a DPIA. The DPIA includes the implementation of data security and privacy risk assessment in software development. Furthermore, the GDPR regulation leads in the requirement for data protection by design and default. It is now required that privacy and security are built into the core of technical products. Documentation of the framework's components and processes that aligns with the GDPR data protection principles, supports in demonstrating compliance.

6.5 Impact on the Field

The framework provides a systematic approach which can be used by software developers to conduct a risk management process to assess security and privacy of data in flow for their IoMT product to assist in meeting the GDPR data protection requirements. It removes the need for an organisation to find and determine the appropriate standards or models and interpret their requirements in order to demonstrate compliance with the GDPR. The framework presents the requirements of the GDPR data

protection regulations on the level of software development, which developers can use to understand what needs to be done to conform to the GDPR data protection requirements. Experts during the development and review of the framework have stated the usefulness of having a standardised systematic approach to the creation of a DPIA, which can be used to demonstrate compliance to the GDPR data protection requirements. During the focus group with the STATSports software development team the participants agreed the implementation of the framework from the conception of a new software project would be extremely valuable for ensuring the application of security and privacy to address the GDPR data protection requirements in a new project. The results of implementing the framework can be used by the developers as a baseline against future software development projects. The STATSports software team noted the positive impact on future development projects having applied the framework to the Sonra cloud project.

Experts from the review and the software development team reported that the framework provided a greater understanding of the:

- GDPR data protection and legal requirements for processing personal data;
- The potential threats and corresponding attacks;
- Security and privacy controls for mitigation of threats;

This understanding is facilitated using the additional information and links in the framework, which encourages the developers to look outside the framework for additional resources and guidance. This improved understanding particularly of the GDPR and of the threats and attacks.

6.6 Research Limitations

Several limitations should be acknowledged in the work performed here. Firstly, the AR approach was used to develop and implement the framework into one software development team. Whilst the use of expert validation was conducted during the development and on the developed version of the framework it should be noted that, the implementation of the framework also took place in a single SME. It should also be noted that during the final focus group the developers communicated the steep learning curve that was required in the implementation of the framework. The learning curve is a notable challenge revealed in the literature review. This is also noted by Dr. Wuyts in her expert review. The development team and Dr. Wuyts described that the level of information in the framework is overwhelming. However, the software team did state that once they got used to the language, read the information a few times, and began to apply parts of the

Chapter 6 Summary and Conclusion

framework it started to make sense and was easier. However, it should also be noted that with AR the researcher was embedded in the organisation and was available to assist the software development team when they required clarification. The approach to the development of the framework ensures that a SME software team can adapt the framework to suit its context of use and that the framework is generally applicable. However, future use of the framework in SMEs of differing experience may facilitate a better understanding of how the maturity of the software development team impacts the use and tailoring of the framework.

The implementation of the framework was in a software project focused on the development of a cloud feature add-on to a current product. This project was chosen as it was the first time the SME had developed a product for the cloud, for their elite product. This means it was the first-time clients' elite data would be out of their environments and exposed to the IoT. This required STATSports to demonstrate to their clients that the security and privacy of the data in flow met the GDPR data protection requirements. Therefore, the development was completed on a current project that did not follow the framework. This required the team to implement the framework retrospectively on aspects of the previous product that linked to the new cloud feature. This slowed down the implementation of the framework and required the software development team to retrospectively consider security and privacy. As noted in the literature this is generally challenging and time consuming. Therefore, the period to implement the framework was extended.

The final version of the framework was reviewed by a carefully selected expert Dr. Wuyts, to focus on privacy. The intention was to have a dedicated privacy expert as the framework development was completed with security experts. In the review with Dr. Wuyts they recommended that it would be beneficial to have the framework assessed by legal experts to ensure the legal GDPR requirements were met. A limitation of the validation is that the complete framework was not reviewed by a GDPR legal expert. This limitation was minimised by the fact that the draft privacy policy provided with the framework was reviewed by the STATSports solicitors. This limitation was also minimised by the fact that STATSports achieved ISO 27001 certification and satisfied their clients' GDPR requirements. In addition, this limitation was minimised using the text from the GDPR regulation in Table 7 Lawful Processing in the development of the questions for this component. This limitation was also minimised in relation to the screening questions providing a rationale as to why a DPIA is required. The standard

ISO/IEC 29100:2011+A1:2018 Information technology - Security techniques - Privacy framework (ISO/IEC 2018b), was used to assist the developers in developing the screening questions. The Annex A Framework Principles, provide detailed guidance and questions based on GDPR data protection, to assist the developers and SMEs in creating the screening questions.

The framework security and privacy controls have been developed using the current version of standards NIST SP 800-53r5, IEC 62443-3-3, and ISO/IEC 15408-2. As the standard ISO/IEC 15408-2 is under revision, the framework's controls will need to be revised to consider any changes to or additional requirements which are introduced because of the revision of the standard. This is also a consideration for IEC 62443-3-3 as the stability date for the current publication is 2021. The publication will remain unchanged up to the stability date and at this date, will be either reconfirmed, withdrawn, replaced by a revised edition, or amended.

6.7 Research Validity

For assessing reliability and validity in qualitative research, it is essential to establish rigor in a qualitative research study in terms of its truth value (internal validity), applicability (external validity), consistency (reliability) and neutrality (objectivity) (Guba and Lincoln 2003). The measures taken to address the validity of this research have been outlined in chapter 3. This section reviews those measures under the headings: reliability, internal validity, external validity and generalisability, and construct validity.

6.7.1 Reliability

For this research project, reliability provides a measure of confidence that repeating the process would ensure consistency and replicability over methods, over time and over groups of respondents (Cohen et al. 2005; Bush 2007). This includes that reliability for the project is achieved by ensuring that statements made by participants and interpretation by the researcher are distinguishable (Flick 2008). To meet this requirement for the data collected during the expert review and focus group sessions, the transcript and validation section report was circulated to the expert and all focus group participants following the session. This distribution process was completed to allow participants to confirm the findings of the review and focus group session and correct any errors or omissions. Additionally, a questionnaire was used to collect initial feedback mapped to the research. From this questionnaire the follow-up review and focus group used scripted questions.

6.7.2 Internal Validity

As outlined in chapter 3, internal validity *relates to the validity of the study itself, including both the design and the instruments used* (Mathers et al. 1998, p.53). Essentially this means the extent of confidence that the intervention causes the outcomes in the research and cannot be explained by other factors. To address concerns over internal validity several measures were used which included:

1. Throughout the research triangulation was used. Data triangulation was used in the AR development of the framework in applying a literature review, multiple experts, and participants to determine the appropriate components and processes for the framework. Investigator triangulation was used to minimise biases coming from the researcher's supervisors, security experts, and a medical software development organisation in the development of the security and privacy controls. Theory triangulation was supported using external domain experts. Finally, method triangulation was also used with data being collected through questionnaire and interviews and between the participants of the interviews.
2. STATSports selected the software project the framework would be applied and undertook to employ no other security and risk processes during this period. This was to limit the chances of other factors influencing the result of the implementation.

6.7.3 External Validity and Generalisability

External validity relates to the extent to which the findings from a study can be generalised. The framework was developed using CAR, over multiple iterations within one company. To be confident that the framework can be used in another environment or by other developers, then it would be needed to be implemented and tested in another company. It is important to distinguish that each IoMT setting is unique, with its own set of contextual factors that may influence the success of the framework in a different environment. These contextual factors are presented by Cruzes et al. (2018). They include aspects such as the organisational culture, the level of resources available, the level of technological sophistication, and type of relationship between key stakeholders in the organisation (Davison et al. 2004; Cruzes et al. 2018). It would be also important to consider the ability of a software development team to adapt and modify the framework to fit their particular needs and challenges without the support of the researcher.

However, there were steps to support the generalisability of this research. The challenges identified in the literature were consistent with those experienced by STATSports. The framework was built on established risk assessment, medical, security and privacy standards and models. Using AAMI TIR 57 as a basis for the structure of the framework ensures that, with tailoring, the model is generally applicable. Even though the CAR project was conducted in an SME setting, the framework is based on the principles of threat modeling and aligned to the risk assessment processes of ISO 14971 and AAMI TIR 57. This means the framework has been designed to be adapted for use in a variety of development settings. Using established standard based risk assessment processes and threat models support that, with tailoring, the framework is generally applicable. In addition, components of the framework were subject to expert review by security developers, expert review by an expert who developed the LINDDUN TM for privacy, a medical app development organisation, and medical standards experts during its development. This group represent a diverse set of stakeholders drawn from varied domains. During the implementation of the framework in STATSports, an understanding of the context of the organisation and the software development project was acquired and is described to understand the limitations that this may represent in the findings.

6.7.4 Construct Validity

Construct validity is concerned with whether the data collection measures, measure what it aims to measure. To address construct validity, consideration was given to several aspects. The first considered whether the research is too narrow and neglects significant aspects of a construct. To address this construct validity concern, the development of the framework included expert participants to avoid bias. The experts considered the use of the methods applied to the framework and if these methods were applied in accordance with the meanings of the theoretical terms. The second consideration was the construct irrelevant variance, which is an important threat to validity, especially for composed response assessments with rich contextualised information. To address this concern, the questionnaires were reviewed before conducting the interviews. In addition, the comments from the expert were discussed in the focus group with the software team who implemented the framework. This contributed to a collective decision on what changes should be made to the framework.

6.8 Further Research

With the implementation and validation of the framework there are many opportunities for further research and future work to enhance and automate the framework to increase its value, composition, and usability to improve its uptake and implementation. The opportunities for further research are outlined in this section.

The framework would benefit by the addition of a formal described requirement for a compatibility assessment. A compatibility assessment is used to make sure all the purposes specified up front for collection of the data are the only processes on the data items. It also includes assessing that the data collected is only used for that specific purpose. The compatibility assessment process would run through the per-interaction process. The developers would assess if the processes developed in the system or product are compliant with the reason and consent for the collection and processing of the personal data. If the compatibility assessment reveals gaps, the project will have address these to continue being compliant.

Separate the security and privacy properties, repudiation, and non-repudiation respectively, and distinguish as distinct categories. This change will be required all the way through to the categorisation of the DFSPCs. This would further help make the distinction between security and privacy mind-sets in the framework, addressed in the expert review.

Both the software development team and the expert reviewer noted the complexity of the framework in its academic form. The future work on this aspect would be the creation of a summarised version of the current academic document to include a quick guide on how to use the framework or an implementation manual for use by developers. As suggested by Dr. Wuyts, an implementation manual or high-level overview could be developed out of the implementation of the framework within STATSports with the developers. The expert suggested to investigate with the development team what a high-level technical or 'How To' manual should contain. The development team suggested that a technical document would be very useful but also encouraged using this along with the current academic document due to the rich information in the academic document. In addition, the software team suggested the development of a set of accompanying videos in bite size for each step or process of the framework with a working example. They considered this would make the reading and implementation of the framework less academic and more appealing to developers.

Another factor, for consideration with development in small organisations are third party suppliers. As established in the literature review, SMEs depend on third party suppliers to assist in development and building their products and systems. No third-party supplier for STATSports was subject to using the framework or meeting the security and privacy requirements as this is completed by the in-house development team. However, moving forward this could be something that the organisation could require. For example, if they have third party development suppliers during a project, the third-party supplier should also use and feed into the framework. Particularly relevant in relation to the GDPR is ensuring that third party suppliers are meeting the data protection principles requirements for not only their organisation but, also for any services they provide, including development. This is important from a wider GDPR legal perspective, especially for the aspect of privacy, given the potential fines for a breach of data, a SME can apply the requirement for a third-party supplier to follow the processes of the framework. Therefore, if there is a breach the SME using a third-party supplier can show due diligence in the development process. This is of greater importance if the organisation is developing a medical device. If that software fails, it is not the third-party supplier that has to address the crises, it is the organisation that carries the responsibility. The framework contribution is to enable an SME that would not have the time to do this themselves, provide the process that the third-party supplier should follow. It simplifies the process for the SME that they can potentially de-risk their third-party suppliers.

6.9 Conclusion

With the introduction of the GDPR, consideration of security and privacy is a requirement in any software product or system processing personal data. However, because of numerous challenges, developers in SMEs struggle to implement adequate security and privacy for the data in flow in the IoMT to meet the GDPR data protection requirements. To assist the software developers in SMEs, implement compliant security and privacy of data in a systematic way, this study has developed a framework to demonstrate the measures taken to ensure security and privacy of data in flow in their IoMT products to meet GDPR data protection requirements. The framework has been confirmed by experts from the software security and privacy domains as being suited for use in SME software development environments. Several conclusions in relation to the utility of the framework have been drawn as part of this research and are discussed in this section.

Chapter 6 Summary and Conclusion

The implementation of the framework in a SME software development team has confirmed the utility of the framework for use in this focused environment. However, this implementation revealed that further support procedures are required to strengthen assistance for implementation. Both the organisations' software developers and the expert reviewer confirmed that the framework could be overwhelming for developers operating at a lower level of security and privacy maturity. This is consistent with the experience of the software team during the implementation of the framework. The software team would have been at a lower maturity level in security and privacy when beginning the implementation. However, they did state in the focus group validation, that as they progressed through the implementation of the framework and became more comfortable with the language and processes, their confidence and knowledge increased, and implementation became easier. Nevertheless, the software team suggested having interactive support through videos showing working examples with a more technical oriented document to support the heavily academic document. A 'How To' or less academically orientated document. The development of this type of document with feedback from the software team, was also endorsed by the expert reviewer.

During the framework implementation, the software architect took ownership of the processes and acted as the coordinator for the software development team. The software architect identified the software team as being ideally placed to perform this role due to their focus on system development and ability to understand the requirements of the overall system. It is the conclusion of the researcher that the successful implementation of the framework for a SME software development team, this level of leadership on the part of the software architect or a senior member of the software team is essential.

An evaluation of the framework, through validation with the privacy expert and the participating organisation, clearly indicates the value of the framework for developers inexperienced in the application of security and privacy in development. Both stated that the information provided in the framework is very useful and provides strengths in information and knowledge. The software team stated that they now have knowledge and expertise in the application of the GDPR data security and privacy requirements in development, that they did not previously have. Furthermore, they considered that the framework provided them with guidance and real direction for long term data security and privacy in future development projects because their products are based on a comparable architecture.

Chapter 6 Summary and Conclusion

Several measures have been taken to address both the reliability and validity of this research. The generalisability of the framework to other organisations may still be a concern as it has only been implemented in one SME organisation. To strengthen claims of generalisability, implementation of the framework in other software development projects of other organisations is required. However, this was deemed impractical due to resource requirements and the CAR approach of the study. To address this concern, the framework has undergone review by experts in both security and privacy development domains and has been published in international conferences and journals. Additionally, its development is based on established risk assessment standards, specifically AAMI TIR 57 and NIST SP 800-30, threat modelling methods, specifically STRIDE and LINDDUN and security and privacy standards for controls, specifically NIST SP 800-53r5, IEC 62443-3-3 and ISO/IEC 15408-2.

References

- AAMI. (2016). *Technical Information Report TIR57:2016 Principles for medical device security - Risk Management*. Arlington.
- Acar, Y., Stransky, C., Wermke, D., Weir, C., Mazurek, M.L. and Fahl, S. (2017). Developers Need Support, Too: A Survey of Security Advice for Software Developers. *Proceedings - 2017 IEEE Cybersecurity Development Conference, SecDev 2017*, 2017, pp.22–26.
- Adams, W.C. (2015). Conducting Semi-Structured. In: Newcomer, K. E., Hatry, H. P., and Wholey, J. ., eds. *Handbook of Practical Program Evaluation*. Fourth Edi. John Wiley & Sons, pp.492–505. Available from: https://www.researchgate.net/publication/301738442_Conducting_Semi-Structured_Interviews.
- Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A. (2017). 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, 2017, pp.193–199.
- Al-Karaki, J.N. and Kamal, a E. (2004). Routing Techniques in Wireless Sensor Networks: A Survey. *IEEE Wireless Communications*, 11(December), pp.6–28. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1368893.
- Alshammari, M. (2019). *A Principled Approach for Engineering Privacy by Design* [unpublished]. Worcester College: University of Oxford.
- Alsubaei, F., Abuhussein, A., Shandilya, V. and Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things*, 8, p.100123. Available from: <https://doi.org/10.1016/j.iot.2019.100123>.
- Alsubaei, F., Abdullah, A. and Shiva, S. (2018). A Framework for Ranking IoMT Solutions Based on Measuring Security and Privacy. In: *Proceedings of the Future Technologies Conference (FTC) 2018. FTC 2018. Advances in Intelligent Systems and Computing*. pp.104–121. Available from: http://dx.doi.org/10.1007/978-3-030-02686-8_67.
- Alsubaei, F., Abuhussein, A. and Shiva, S. (2017). Security and Privacy in the Internet of Medical Things : Taxonomy and Risk Assessment. In: *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. IEEE, pp.112–120.
- Al Ameen, M., Liu, J. and Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems* [online], 36(1), pp.93–101. Available from: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3279645&tool=pmcentrez&rendertype=abstract> [accessed 7 October 2014].
- Anandarajan, M. and Malik, S. (2018). Protecting the Internet of medical things: A situational crime-prevention approach. *Cogent Medicine*, 5(1), pp.1–23. Available from: <https://doi.org/10.1080/2331205X.2018.1513349>.
- Anderson, S. (2016). *The effectiveness of ISO 80001-2-2 , to adequately communicate security needs , risks and controls given a specific security implementation framework*. [unpublished]. Flinders University.
- Anderson, S. and Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?. *Computer Standards and Interfaces*, 56(October 2017), pp.134–143. Available from: <https://doi.org/10.1016/j.csi.2017.10.001>.
- Appari, A. and Johnson, M.E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise*

References

Management, 6(4), p.279.

Araxan. (2014). *State of Mobile App Security : Apps Under Attack - Special Focus on Financial, Retail/Merchannt and Healthcare/Medical Apps*.

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*. Brussels: European Commission.

Arxan. (2016). *5th Annual State of Application Security Report Perception vs. Reality*. San Francisco. Available from: https://www.arxan.com/wp-content/uploads/2016/01/State_of_Application_Security_2016_Healthcare_Report.pdf.

Asthon, K. (2009). That ' Internet of Things ' Thing. *RFID Journal*, 22(7), pp.97–114. Available from: <http://www.rfidjournal.com/article/print/4986>.

Ataei, M., Slimani, S. and Kray, C. (2020). *General Data Protection Regulations Guidelines for Developers and Designers*. Münster. Available from: https://www.uni-muenster.de/imperia/md/content/angewandteinformatik/aktivitaeten/publikationen/gdpr_report.pdf.

Avison, D., Lau, F., Myers, M. and Nielsen, P.A. (1999). Action research. *Communications of the ACM*, 42(1), pp.94–97.

Balandina, E., Balandin, S., Koucheryavy, Y. and Mouromtsev, D. (2015). IoT Use Cases in Healthcare and Tourism. *Proceedings - 17th IEEE Conference on Business Informatics, CBI 2015*, 2, pp.37–44.

Barbour, R. (2008). *Theorizing in Qualitative Data Analysis*.

Barlette, Y. and Fomin, V. V. (2008). Exploring the suitability of IS security management standards for SMEs. In: *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp.1–10.

Basir, R., Qaisar, S., Ali, M., Aldwairi, M., Ashraf, M.I., Mahmood, A. and Gidlund, M. (2019). Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors (Switzerland)*, 19(21), pp.1–38.

Baskerville, R. and Wood-Harper, A.T. (1998). Diversity in information systems action research methods. *European Journal of Information Systems*, 7(2), pp.90–107.

Baskerville, R.L. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, 2(19).

Bell, J. (2014). *Doing Your Research Project: A guide for first-time researchers*. Fifth. Maidenhead: McGraw-Hill Education (UK).

Berger, B.J., Sohr, K. and Koschke, R. (2016). Automatically extracting threats from extended data flow diagrams. In: *International Symposium on Engineering Secure Software and Systems*. pp.56–71.

Bitglass. (2021). *Healthcare Breach Report 2021 Hacking and IT Incidents on the Rise*. Available from: <https://www.bitglass.com>.

Braun, V. and Clarke, V. (2013). *Successful Qualitative Research: A Practical Guide for Beginners*. London: Sage. Available from: https://books.google.com/books?id=EV_Q06CUsXsC&pgis=1.

Brien, G.O., Edwards, S., Littlefield, K., McNab, N., Wang, S. and Zheng, K. (2018). NIST SP 1800-8 Securing Wireless Infusion Pumps In Healthcare Delivery Organizations. , 2018, p.354. Available from: <https://nccoe.nist.gov/projects/use-cases/medical-devices>.

Burgess, T.F. (2001). A general introduction to the design of questionnaires for survey research. *Guide to the Design of Questionnaires*, 30(4), pp.411–432.

Bush, T. (2007). Authenticity in research—reliability, validity and triangulation. In: Briggs, A., Coleman, M., and Morrison, M., eds. *Research methods in educational leadership and management*. 2nd ed. London: Sage Publications Ltd, pp.1–400.

References

- Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, 21(5), pp.811–831.
- Cavalcante, E., Alves, M.P., Batista, T., Delicato, F.C. and Pires, P.F. (2015). An analysis of reference architectures for the internet of things. In: *CobRA 2015 - Proceedings of the 1st International Workshop on Exploring Component-Based Techniques for Constructing Reference Architectures, Part of CompArch 2015*. pp.13–16.
- Cavoukian, A. (2010). Privacy by Design. *Identity in the Information Society*, 3(2), pp.1–12. Available from: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
- Cavoukian, A. (2009). *Privacy by Design ...take the challenge*. Information & Privacy Commissioner Ontario.
- Chanal, P.M. and Kakkasageri, M.S. (2020). Security and Privacy in IoT: A Survey. *Wireless Personal Communications*, 115(2), pp.1667–1693. Available from: <https://doi.org/10.1007/s11277-020-07649-9>.
- Chen, H., Bao, D., Goto, Y. and Cheng, J. (2015). A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045. In: Park, J. et al., eds. *Computer Science and its Applications. Lecture Notes in Electrical Engineering*. Berlin Heidelberg: Springer, pp.1359–1366.
- Cho, Y.-S., Hoel, T. and Chen, W. (2016). Mapping a Privacy Framework to a Reference Model of Learning Analytics. , 2016, pp.1–7. Available from: http://www.laceproject.eu/wp-content/uploads/2015/12/ep4la2016_paper_4.pdf.
- Cisco. (2017). *2017 Annual Cybersecurity Report* [online]. San JOse. Available from: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf [accessed 18 March 2020].
- Cisco. (2018). *2018 Annual Cybersecurity Report* [online]. San Jose. Available from: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf [accessed 18 March 2020].
- Cisco. (2019). *Defending against today's critical threats*. Available from: <https://www.cisco.com/c/dam/en/us/products/se/2019/2/Collateral/cybersecurity-series-threat.pdf>.
- Cohen, L., Manion, L. and Morrison, K. (2005). *Research Methods in Education*. Available from: <http://books.google.com/books?id=5twk1pHwyL8C&pgis=1>.
- Cole, R., Purao, S., Rossi, M. and Sein, M.K. (2005). Being Proactive: Where Action Research meets Design Research. In: *ICIS 2005 Proceedings*. pp.1–21. Available from: <http://aisel.aisnet.org/icis2005/27>.
- Common Criteria for Information Technology Security Evaluation. (2012). Part 2 : Security functional components. , 2012, pp.1–321. Available from: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA406677>.
- Coughlan, M., Cronin, P. and Ryan, F. (2007). Step'by-step guide to critiquing research. Part 1: quantitative research. *British Journal of Nursing*, 16(11), pp.658–663.
- Creswell, J.W. (2003). *Research design: qualitative, quantitative, and mixed methods approaches*. Third Edit. London: Sage.
- Cronin, P., Ryan, F. and Coughlan, M. (2008). Undertaking a literature review: a step-by-step approach. *British Journal of Nursing*, 17(1), pp.38-43.
- Cross, N. (2001). Designerly Ways of Knowing: Design Discipline Versus Design Science. *Design Issues*, 17(3), pp.49–55. Available from: <http://oro.open.ac.uk/3281/>.
- Crotty, M. (1998). *The Foundations of Social Research: Meaning and perspective in the research process*. London: Sage.

References

Cruzes, D.S., Jaatun, M.G. and Oyetyoyan, T.D. (2018). Challenges and approaches of performing canonical action research in software security. *ACM International Conference Proceeding Series*, 2018.

CWE. (2019). *2019 CWE Top 25 Most Dangerous Software Errors* [online]. Available from: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html [accessed 5 March 2020].

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R. and Schiffner, S. (2014). *Privacy and Data Protection by Design - from policy to engineering*. Available from: <http://arxiv.org/abs/1501.03726>.

Data Protection Commission Ireland. (2020). *Data Protection Impact Assessments* [online]. Website [online]. Available from: <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments> [accessed 10 January 2020].

Data Protection Commission Ireland. (2018). Draft List of types of Data Processing Operations which require a Data Protection Impact Assessment. , 2018, pp.1–6. Available from: https://www.dataprotection.ie/docimages/documents/DPIA_DPC.pdf.

Data Protection Commission Ireland. (2019a). Guide to Data Protection Impact Assessments (DPIAs). , 2019.

Data Protection Commission Ireland. (2019b). Quick Guide to the Principles of Data Protection. , 2019, pp.1–5. Available from: https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance_on_the_Principles_of_Data_Protection_Oct19.pdf.

Davison, R.M., Martinsons, M.G. and Kock, N. (2004). Principles of canonical action research. *Information Systems Journal*, 14(1), pp.65–86.

Davison, R.M., Martinsons, M.G. and Ou, C.X.J. (2012). The roles of theory in canonical action research. *MIS Quarterly: Management Information Systems*, 36(3), pp.763–786.

Dawson, C. (2009). *Introduction to research methods: A practical guide for anyone undertaking a research project*. 4th ed. Oxford: How To Books Ltd. Available from: <http://www.lavoisier.fr/livre/notice.asp?id=OLXWR6AXA63OWT%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Introduction+to+research+methods,+a+practical+guide+for+anyone+understaking+a+research+project#0%5Cnhttp://scholar.google.com/schol>.

Dempsey, K., White, G. and Ricke, D. (2014). *Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B. and Joosen, W. (2010). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 1(16), pp.3–32. Available from: <http://web.b.ebscohost.com.library.capella.edu/ehost/pdfviewer/pdfviewer?sid=e7ebe3bc-59f7-43a0-ace9-60485dc3acd3%40sessionmgr111&vid=1&hid=118>.

Denzin, N.K. (1978). *The research act: A theoretical introduction to sociological methods*. 2nd ed. New York, NY: McGraw Hill.

Department of Business Enterprise and Innovation. (2020a). *Focus on Medical Technologies*.

Department of Business Enterprise and Innovation. (2020b). *Focus on Medical Technologies August 2020*. Available from: <https://enterprise.gov.ie/en/Publications/Publication-files/Focus-on-Medical-Technologies-2020.pdf>.

Department of Enterprise Trade and Employment. (2018). *Research Priority Areas*

References

- 2018 to 2023. Dublin. Available from: <https://enterprise.gov.ie/en/Publications/Research-Priority-Areas-2018-to-2023.html>.
- Dhillon, D. (2011). Developer-Driven Threat Modeling: Lessons Learned in the Trenches. *IEEE Security and Privacy*, 2011, pp.41–47.
- Dorst, K. (2008). Design research: a revolution-waiting-to-happen. *Design Studies*, 29(1), pp.4–11.
- Duricu, A. (2019). *Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR)* [unpublished]. Luleå University of Technology.
- Dwivedi, R., Mehrotra, D. and Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research*, 12(2), pp.302–318. Available from: <https://doi.org/10.1016/j.jobcr.2021.11.010>.
- Easterbrook, S., Singer, J., Storey, M.-A. and Damian, D. (2008). Selecting Empirical Methods for Software Engineering Research Guide to Advanced Empirical Software Engineering. In: *Guide to Advanced Empirical Software Engineering*. London: Springer, pp.285–311. Available from: http://dx.doi.org/10.1007/978-1-84800-044-5_11.
- Elshekeil, S.A. and Laoyookhong, S. (2017). *GDPR Privacy by Design* [unpublished]. Stockholm. Available from: http://www.isaca.org/chapters4/Sweden/OmOss/Documents/Stipendie2017_ElShekeil-Laoyookhong.pdf.
- ENISA. (2021). Cybersecurity Challenges and Recommendations for SMEs. Challenges and Recommendations. Sarri, A., Paggio, V., and Bafoutsou, G., eds. , 2021, pp.1–61. Available from: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.
- ENISA. (2017). *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR*. Heraklion,: European Union Agency for Network and Information Security. Available from: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/>.
- Enterprise Ireland. (2021). *The Irish Advantage* [online]. Website [online]. Available from: <https://irishadvantage.com/growth-irelands-medtech-sector/> [accessed 10 December 2021].
- EU General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. , 2016, pp.1–88. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>.
- European Commission. (2014). *Green Paper on mobile Health ('mHealth')*. Brussels.
- Falah, B., Akour, M. and Oukemeni, S. (2015). An Alternative Threat Model-based Approach for Security Testing. *Journal of Secure Software Engineering (IJSSE)*, 6(3), pp.50–64. Available from: https://www.researchgate.net/profile/Mohammed_Akour/publication/281309296_An_Alternative_Threat_Model-based_Approach_for_Security_Testing/links/56982e1608aec79ee32b7771.pdf.
- Filkins, B. (2014). *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*. SANS Institute. Available from:

References

- <https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735>.
- Finnegan, A. (2014). *Security Case Development for Medical Devices* [unpublished]. Dundalk Institute of Technology.
- Finnegan, A. and McCaffery, F. (2014). A Security Argument Pattern for Medical Device Assurance Cases. In: *IEEE International Symposium on Software Reliability Engineering Workshops*. Naples: IEEE, pp.220–225. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6983842>.
- Flick, U. (2009). An introduction to qualitative research. *Sage*, 4th, p.529. Available from: <http://books.google.cz/books?id=sFv1oWX2DoEC>.
- Flick, U. (2008). *Managing quality in qualitative research*. London: Sage.
- Focardi, R. and Gorrieri, R. (2000). Classification of security properties★ (Part I: Information flow). In: *International School on Foundations of Security Analysis and Design*. Berlin Heidelberg: Springer, pp.331–396. Available from: https://link.springer.com/content/pdf/10.1007/3-540-45608-2_6.pdf.
- Fox, W.S. and Denzin, N.K. (1979). *The Research Act: A Theoretical Introduction to Sociological Methods*. London: Transaction Publishers.
- De Francesco, G.P. (2019). The General Data Protection Regulation’s Practical Impact on Software Architecture. *Computer*, 52(4), pp.32–39.
- Fremantle, P. (2017). *An Approach to Enhancing Security and Privacy of the Internet of Things with Federated Identity* [unpublished]. University of Portsmouth.
- Fusch, P., Fusch, G.E. and Ness, L.R. (2018). Denzin’s Paradigm Shift: Revisiting Triangulation in Qualitative Research. *Journal of Social Change*, 10(1), pp.19–32.
- Galletta, A. (2013). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. Vol. 18. New York: NYU Press. Available from: <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso,cpid&custid=ns000798&db=e000xww&AN=575563&site=eds-live>.
- Galvez, R. and Gurses, S. (2018). The Odyssey: Modeling Privacy Threats in a Brave New World. In: *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, (EUROS&PW) 2018*. IEEE, pp.87–94.
- Garcia-Pardo, C., Andreu, C., Fornes-Leal, A., Castello-Palacios, S., Perez-Simbor, S., Barbi, M., Valles-Lluch, A. and Cardona, N. (2018). Ultrawideband Technology for Medical In-Body Sensor Networks: An Overview of the Human Body as a Propagation Medium, Phantoms, and Approaches for Propagation Analysis. *IEEE Antennas and Propagation Magazine*, 60(3), pp.19–33.
- Gardašević, G., Katzis, K., Bajić, D. and Berbakov, L. (2020). Emerging wireless sensor networks and internet of things technologies—foundations of smart healthcare. *Sensors (Switzerland)*, 20(13), pp.1–30.
- Gatouillat, A., Badr, Y., Massot, B. and Sejdic, E. (2018). Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. *IEEE Internet of Things Journal*, 5(5), pp.3810–3822.
- Gebremichael, T., Ledwaba, L.P.I., Eldefrawy, M.H., Hancke, G.P., Pereira, N., Gidlund, M. and Akerberg, J. (2020). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access*, 8, pp.152351–152366.
- Ghazouani, M., Faris, S., Medromi, H. and Sayouti, A. (2014). Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*, 103(8), pp.36–42.
- Gray, D.E. (2014). *Doing research in the real world*. Third. Sage. Available from: <http://www.uk.sagepub.com/books/Book239646#tabview=toc>.

References

Greenhalgh, T. and Peacock, R. (2005). Effectiveness and efficiency of search methods in systematic reviews of complex evidence: Audit of primary sources. *British Medical Journal*, 331(7524), pp.1064–1065.

Guba, E.G. and Lincoln, T.S. (2003). Competing Paradigms in Qualitative Research. In: Hesse-Biber, S. N. and Leavy, P., eds. *Approaches to Qualitative Research: A Reader on Theory and Practice*. New York: Oxford University Press, pp.105–117.

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G. and Tsatsoulis, C. (2019). Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. In: *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019*. IEEE, pp.457–464.

Hernan, S., Lambert, S., Ostwald, T. and Shostack, A. (2006). Threat modeling-uncover security design flaws using the stride approach. *MSDN Magazine*, November, pp.68–75. Available from: <file://staff/Home/treacyc/Mendeley/Uncover Security Design Flaws Using The STRIDE Approach.pdf>.

Herrmann, D.S. (2002). *Using the Common Criteria for IT Security Evaluation*. Boca Raton: CRC Press. Available from: <http://books.google.com/books?id=PFi96wddAw8C>.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH. *MIS Quarterly*, 28(1), pp.75–105.

Horgan, D., Kranen, H.J. van, Morré, S.A., Van Kranen, H.J. and Morré, S.A. (2018). Optimising SME Potential in Modern Healthcare Systems: Challenges, Opportunities and Policy Recommendations. *Public Health Genomics*, 21(1–2), pp.1–17. Available from: <https://pubmed.ncbi.nlm.nih.gov/30145589/>.

Howard, M. and Lipner, S. (2006). *The Security Development Lifecycle*. Redmond: Microsoft Press.

HPRA. (2020). HPRAGuide to Placing Medical Device Standalone Software on the Market. , 2020, pp.1–18. Available from: <https://www.hpra.ie/docs/default-source/publications-forms/guidance-documents/sur-g0040-guide-to-placing-medical-device-standalone-software-on-the-market-v1.pdf?sfvrsn=9>.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G. and Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, 26(4), pp.1607–1609.

ICO. (2020). *What is a DPIA?* [online]. *Data Protection Impact Assessments (DPIAs)* [online]. Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/> [accessed 13 January 2020].

IDA. (2021). *IDA Ireland* [online]. *Website* [online]. Available from: <https://www.idaireland.com/doing-business-here/industry-sectors/medical-technology> [accessed 10 December 2021].

IEC. (2013). 64223-3-3 Industrial Communication Networks - Network and System Security – Part 3-3: System security requirements and security levels. , 2013, p.81. Available from: http://www.iec.ch/dyn/www/f?p=103:22:0:::FSP_ORG_ID:1250.

IEC. (2012). *TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices Part 2-2 : Guidance for the disclosure and communication of medical device security needs, risks and controls*. BSI Standards Publication

IEC/TR. (2016). *80001-2-8:2016 Application of risk management for IT-networks incorporating medical devices — Application guidance Part 2-8 : Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*.

IEEE Standards. (2012). IEEE802.15.6: Standard for Local and metropolitan area networks - Wireless Body Area Networks. , 2012.

References

- Iivari, J. (2007). A Paradigmatic Analysis of Information Systems As a Design Science. *Scandinavian Journal of Information Systems*, 19(2), pp.39–64.
- Iivari, J. and Venable, J. (2009). Action Research and Design Science Research. In: *17th European Conference on Information Systems*. pp.1–13.
- Illing, J. (2014). Thinking About Research: Theoretical Perspectives, Ethics and Scholarship. In: *Understanding Medical Education: Evidence, Theory and Practice: Second Edition*. 2nd ed. Wiley Blackwell, pp.331–347.
- IMDRF Software as a Medical Device (SaMD) Working Group. (2014). *IMDRF International Medical Device Regulators Forum*. Available from: <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf>.
- Information Commissioner's Office. (2018). *Guide to the General Data Protection Regulation (GDPR)*. Available from: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>.
- Irish Medtech Association. (2019). *Irish Medtech Association Statement of Strategy 2016-2020*.
- ISME. (2021). *SME Facts & FAQs - ISME* [online]. Website [online]. Available from: <https://isme.ie/advice/sme-facts-and-faqs/> [accessed 1 September 2021].
- ISO. (2012). 14971:2012 Medical devices - Application of risk management to medical devices (ISO 14971:2007, Corrected version 2007-10-01). , 2012, pp.1–82.
- ISO. (2019). 14971:2019 Medical devices — Application of risk management to medical devices. , 2019.
- ISO/IEC. (2014a). 15408-1 Information technology — Security techniques — Evaluation criteria for IT Security. , 2014.
- ISO/IEC. (2008a). 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. , 2008. Available from: http://standards.iso.org/ittf/PubliclyAvailableStandards/c046414_ISO_IEC_15408-2_2008.zip.
- ISO/IEC. (2008b). 15408-3:2008 Information technology - Security techniques - Evaluation Criteria for IT Security - Part 3: Security assurance components. , 2008.
- ISO/IEC. (2000). 2382-7:2000 Information technology - Vocabulary - Part 7: Computer Programming. , 2000.
- ISO/IEC. (2015a). *2382:2015 Information Technology - Vocabulary* [online]. *ISO Online Browsing Platform (OBP)* [online]. Available from: <https://www.iso.org/standard/63598.html> [accessed 15 September 2021].
- ISO/IEC. (2013a). 27001:2013 Information technology — Security techniques management systems — Requirements. , 2013.
- ISO/IEC. (2017a). 27001:2017 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013). , 2017.
- ISO/IEC. (2013b). 27002:2013 - Information technology — Security techniques — Code of practice for information security controls. , 2013.
- ISO/IEC. (2017b). 27002:2017 Information technology — Security techniques — Code of practice for information security controls. , 2017.
- ISO/IEC. (2018a). 27005:2018 Information technology. Security techniques. Information security risk management. , 2018, pp.1–80.
- ISO/IEC. (2015b). 27033-1 Information technology — Security techniques — Network security Part 1 : Overview and concepts. , 2015, p.62.
- ISO/IEC. (2010). 27033-3 Information technology — Security techniques —

References

Network security Part 3: Reference networking scenarios — Threats, design techniques and control issues. , 2010, p.40.

ISO/IEC. (2016a). 27033-6 Information technology — Security techniques — Network security Part 6 : Securing wireless IP network access. , 2016, p.40.

ISO/IEC. (2014b). 27034-1 Information technology — Security techniques — Application security Part 1 : Overview and concepts. , 2014.

ISO/IEC. (2015c). 27034-2- Information technology — Security techniques — Application security Part 2: Organisation normative framework. , 2015, p.62.

ISO/IEC. (2019). 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. , 2019, pp.1–76.

ISO/IEC. (2008c). 27799:2008 - Health informatics - Information security management in health using ISO/IEC 27002. , 2008, pp.1–70.

ISO/IEC. (2018b). 29100:2011+A1:2018 Information technology — Security techniques — Privacy framework. , 2018, pp.1–30.

ISO/IEC. (2017c). 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment. , 2017.

ISO/IEC. (2016b). TR 20748-1:2016 BSI Standards Publication Information technology for learning , education and training — Learning analytics interoperability Part 1 : Reference model. , 2016.

ITU-T. (2003). Recommendation X.805 Security architecture for systems providing end-to-end communications. , 2003.

ITU. (2005). *ITU Internet Reports 2005: The Internet of Things – Executive Summary*. Geneva. Available from:
http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.

Järvinen, P. (2012). *On boundaries between field experiment, action research and design research*. Available from:
https://trepo.tuni.fi/bitstream/handle/10024/66319/on_boundaries_between_2012.pdf?sequence=1&isAllowed=y.

Jasmontaitè-Zaniewicz, L., Calvi, A., Nagy, R. and Barnard-Wills, D. (2021). *The GDPR made simple(r) for SMEs*. VUBPRESS. Available from:
<https://library.oapen.org/handle/20.500.12657/46614>.

Jiang, S., Skibniewski, M.J., Yuan, Y., Sun, C. and Lu, Y. (2011). Ultra-wide band applications in industry: A critical review. *Journal of Civil Engineering and Management*, 17(3), pp.437–444.

Johnson, R.B. and Onwuegbuzie, A.J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, 33(7), pp.14–26.

Jones, S.R., Torres, V. and Arminio, J. (2014). Negotiating the complexities of qualitative research in higher education: Fundamental elements and issues. In: 2nd, ed. *Negotiating the Complexities of Qualitative Research in Higher Education: Fundamental Elements and Issues*. New York: Routledge.

Joyia, G.J., Liaqat, R.M., Farooq, A. and Rehman, S. (2017). Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain. *Journal of Communications*, 12(4), pp.240–247.

Jump, M. and Finnegan, A. (2017). Using Standards to Establish Foundational Security Requirements for Medical Devices. *Biomedical Instrumentation and Technology*, 51(s6), pp.33–38.

Katzis, K., Jones, R.W. and Despotou, G. (2016). The challenges of balancing safety and security in implantable medical devices. *Studies in Health Technology and Informatics*, 226(January), pp.25–28.

References

- Khan, J.Y. and Yuce, M.R. (2010). Wireless Body Area Network (WBAN) for Medical Applications. In: Campolo, D., ed. *New Development in Biomedical Engineering*. InTech, pp.591–623. Available from: <http://www.intechopen.com/books/new-developments-in-biomedical-engineering/wireless-body-area-network-wban-for-medical-applications>.
- Kitchenham, B.A.P.B., Turner, M., Niazi, M.K., Linkman, S., Pretorius, R. and Budgen, D. (2010). Refining the systematic literature review process—two participant-observer case studies. *Empirical Software Engineering*, 15(6), pp.618–653.
- Kitzinger, J. and Barbour, R. (1999). Introduction: The Challenge and Promise of Focus Groups. In: Barbour, R. S. and Kitzinger, J., eds. *Developing Focus Group Research*. 6 Bonhill Street, London England EC2A 4PU United Kingdom: SAGE Publications Ltd. Available from: <http://methods.sagepub.com/book/developing-focus-group-research>.
- Kompara, M. and Hölbl, M. (2018). Survey on security in intra-body area network communication. *Ad Hoc Networks*, 70, pp.23–43. Available from: <https://doi.org/10.1016/j.adhoc.2017.11.006>.
- Kontio, J., Lehtola, L. and Bragge, J. (2004). Using the focus group method in software engineering: Obtaining practitioner and user experiences. In: *Proceedings - 2004 International Symposium on Empirical Software Engineering, ISESE 2004*. IEEE Xplore, pp.271–280. Available from: https://www.researchgate.net/publication/4090791_Using_the_Focus_Group_Method_in_Software_Engineering_Obtaining_Practitioner_and_User_Experiences.
- Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D. and Douligeris, C. (2020). Security in IoMT Communications: A survey. *Sensors (Switzerland)*, 20(17), pp.1–49. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7506588/>.
- Lachaud, E. (2020). ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *European Data Protection Law Review*, 6(2), pp.194–210. Available from: <https://dx.doi.org/10.2139/ssrn.3521250>.
- Li, D. (2019). 5G and intelligence medicine - How the next generation of wireless technology will reconstruct healthcare?. *Precision Clinical Medicine*, 2(4), pp.205–208.
- Li, M. and Lou, W. (2010). Security and Privacy in Wireless Body Area Networks. *IEEE Wireless Communications*, 17(1), pp.51–58.
- Liaqat, S., Akhunzada, A., Shaikh, F.S., Giannetsos, A. and Jan, M.A. (2020). SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). *Computer Communications*, 160(February 2021), pp.697–705. Available from: <https://doi.org/10.1016/j.comcom.2020.07.006>.
- Lynn, T., Mooney, J.G., Lee, B. and Takako, P. (2020). *The Cloud-to-Thing Continuum. Opportunities and Challenges in Cloud, Fog and Edge Computing*. Lynn, T. and Mooney, J. G., eds. Cham: Palgrave Macmillan.
- Mann, S.P., Savulescu, J. and Sahakian, B.J. (2016). Facilitating the ethical use of health data for the benefit of society: Electronic health records, consent and the duty of easy rescue. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083).
- Manso, C., Rekleitis, E., Papazafeiropoulos, F. and Maritsas, V. (2015). *Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small medium enterprises*. Heraklion. Available from: [file://staff/Home/treacyc/Mendeley/Information security and privacy standards for SMEs.pdf](file://staff/Home/treacyc/Mendeley/Information%20security%20and%20privacy%20standards%20for%20SMEs.pdf).
- Marback, A., Do, H., He, K., Kondarmarri, S. and Xu, D. (2009). A threat model-

References

based approach to security testing. *Software - Practice and Experience*, 39(7), pp.701–736.

Marr, B. (2018). *Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018* [online]. *Forbes* [online]. Available from: <https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#7cbe068b4a3c> [accessed 9 September 2019].

Mathers, N., Fox, N. and Hunn, A. (1998). *Surveys and questionnaires*. Trent: NHS Executive.

Mayring, P. (2000). Qualitative content analysis. *A companion to qualitative research.*, 1(2), pp.159–176.

McCallister, E., Grance, T. and Kent, K. (2010). NIST SP 800-122 Guide to protecting the confidentiality of personally identifiable information (PII). *Recommendations of the National Institute of ...*, 2010, pp.1–59.

McClelland, R. (2010). European standards on confidentiality and privacy in healthcare. EuroSOCAP Project (2003-2006). , 2010.

McGraw, G. (2006). *Software Security Building Security In*. Reading: Addison-Wesley.

McManus, J. (2018). Security by Design: Teaching Secure Software Design and Development Techniques. *J. Comput. Sci. Coll.*, 33(3), pp.75–82. Available from: <http://dl.acm.org/citation.cfm?id=3144687.3144710>.

Medical Device Coordination Group. (2019). *Guidance on Cybersecurity in Medical Devices*. Available from: <http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm>.

Michaels, S., Akkaya, K. and Selcuk Uluagac, A. (2017). Inducing data loss in Zigbee networks via join/association handshake spoofing. In: *2016 IEEE Conference on Communications and Network Security, CNS 2016*. IEEE, pp.401–405.

Minerva, R., Biru, A. and Rotondi, D. (2015). Towards a Definition of the Internet of Things (IoT). *IEEE Internet Initiative*, 1(1), pp.1–86. Available from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fiot.ieee.org%2Fimages%2Ffiles%2Fpdf%2FIEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf&clen=3073176&chunk=true.

Mishra, L., Vikash and Varma, S. (2021). *Seamless Health Monitoring Using 5G NR for Internet of Medical Things*. Springer US. Available from: <https://doi.org/10.1007/s11277-021-08730-7>.

Morgan, D.L. (2007). Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research*, 1(1), pp.48–76.

Mouratidis, H. and Kang, M. (2013). Secure by Design. In: *International Journal of Secure Software Engineering*. pp.23–41. Available from: <http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/jsse.2011070102>.

Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D. and Jamalipour, A. (2014). Wireless Body Area Networks: A Survey. *Ieee Communications Surveys and Tutorials*, 16(3), pp.1658–1686.

Ngoc, T.. (2008). *Medical Applications of Wireless Networks*. Available from: <http://www.cse.wustl.edu/~jain/cse574-08/index.html>.

NIST. (2012). SP 800-30 Revision 1 Guide for Conducting Risk Assessments. *NIST Special Publication*, 2012, p.95. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800->

References

30r1.pdf%5Cnhttp://csrc.nist.gov/publications/PubsSPs.html%5Cnhttp://dx.doi.org/10.6028/NIST.SP.800-30r1.

NIST. (2020). Special Publication 800-53 Revision 5 Security and privacy controls for federal information systems and organizations. *Joint Task Force*, 80. Available from: <https://doi.org/10.6028/NIST.SP.800-53r5>.

Omojokun, G.A. (2015). A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges. *International Journal of Computer Applications*, 130(9), pp.47–55.

Osterman, L. (2007). *Threat Modeling, once again – Larry Osterman’s WebLog* [online]. *Microsoft/Developer* [online]. Available from: <https://blogs.msdn.microsoft.com/larryosterman/2007/08/30/threat-modeling-once-again/> [accessed 18 November 2019].

OWASP. (2020a). *M3: Insecure Communication | OWASP* [online]. *OWASP Website* [online]. Available from: <https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication> [accessed 7 September 2020].

OWASP. (2020b). *OWASP API Security - Top 10 | OWASP* [online]. *OWASP Website* [online]. Available from: <https://owasp.org/www-project-api-security/> [accessed 17 August 2020].

OWASP. (2017). *OWASP Top Ten* [online]. Available from: <https://owasp.org/www-project-top-ten/> [accessed 5 March 2020].

Padgette, J. and Padgette, J. (2017). NIST Special Publication 800-121 Revision 2. Guide to Bluetooth Security. *NIST Special Publication 800-121 Revision 2*, 2017, pp.1–67.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A. and Patsakis, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access*, 3536(c), pp.1–13.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J. and Lymberopoulos, D. (2020). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Transactions on Emerging Telecommunications Technologies*, 2020, pp.1–19.

Papert, S. and Harel, I. (1991). *Situating Constructionism*. , 1991.

Parker, L., Karliychuk, T., Gillies, D., Mintzes, B., Raven, M. and Grundy, Q. (2017). A health app developer’s guide to law and policy: A multi-sector policy analysis. *BMC Medical Informatics and Decision Making*, 17(1), pp.1–13.

Patton, M.Q. (2015). *Qualitative Research & Evaluation Methods*. 4th ed. Thousand Oaks, CA: Sage.

PCI Security Standards Council. (2018). Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures (Version 3.0). , 2018, pp.1–112. Available from: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Pfitzmann, A. and Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version 0.34 Aug. 10, 2010). *Technical University Dresden*, 2010, pp.1–98. Available from: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml%5Cnhttp://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

Piccarreta, B. and Hogan, M. (2018). *Draft NISTIR 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*. Available from: <https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200->

References

draft.pdf.

La Polla, M., Martinelli, F. and Sgandurra, D. (2013). A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 15(1), pp.446–471.

Ponemon Institute. (2018). *The State of Cybersecurity in Healthcare Organizations in 2018*.

Ponemon Institute/IBM. (2021). *IBM: Cost of a Data Breach Report*. Available from: <https://www.ibm.com/downloads/cas/RDEQK07R>.

Rabionet, S.E. (2011). How I learned to design and conduct semi-structured interviews: An ongoing and continuous journey. *Qualitative Report*, 16(2), pp.563–566.

Rapoport, R.N. (1970). Three Dilemmas in Action Research: With Special Reference to the Tavistock Experience. *Human Relations*, 23(6), pp.499–513. Available from: <https://doi.org/10.1177/001872677002300601>.

RM, S.P., Maddikunta, P.K.R., Parimala, M., Koppu, S., Gadekallu, T.R., Chowdhary, C.L. and Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications*, 160, pp.139–149.

Roe, M. (2010). *Cryptography and evidence*. Cambridge. Available from: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-780.pdf>.

Roth, V.J. (2014). The mHealth Conundrum: Smartphones & Mobile medical apps-How much FDA medical device regulation is required?. *North Carolina Journal of Law & Technology*, 15(3), pp.359–424. Available from: <http://ncjolt.org/wp-content/uploads/2014/04/Roth-Color-Final.pdf>.

Rubí, J.N.S. and Gondim, P.R.L. (2019). IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on oneM2M and openEHR. *Sensors (Switzerland)*, 19(19), pp.1–25.

Saleem, S., Ullah, S. and Kwak, K.S. (2011). A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors (Basel, Switzerland)*, 11(2), pp.1383–95. Available from: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3274043&tool=pmcentrez&rendertype=abstract>.

Saunders, M., Lewis, P. and Thornhill, A. (2009). *Research methods for business students fifth edition*. 5th ed. London: Pearson Education.

Saunders, M. and Tosey, P. (2012). The Layers of Research Design. *Academia.edu* [online], 2012/2013(Winter), pp.58–59. Available from: https://www.academia.edu/4107831/The_Layers_of_Research_Design [accessed 10 November 2015].

Schneier, B. and Shostack, A. (1999). *Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards*. Chicago, Illinois, USA. Available from: https://www.usenix.org/legacy/events/smartcard99/full_papers/schneier/schneier.pdf.

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. and Khan, R.A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Switzerland)*, 8(2).

Seidman, I. (2006). *Interviewing As Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. 3rd, ed. New York: Teachers College Press.

Sein, M.K., Henfridsson, O. and Rossi, M. (2011). Action Design Research. *MIS Quarterly*, 35(1), pp.37–56.

Seliem, M., Elgazzar, K. and Khalil, K. (2018). Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing*, 2018, pp.1–16. Available from: <https://eprint.iacr.org/2019/1471.pdf>.

References

- Senseon. (2019). *The State of Cyber Security in Canada*. Available from: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2019/08/White_paper_1.pdf <http://www.wmbeck.com/wp-content/uploads/2017/06/The-State-of-Cyber-Security-in-Canada.pdf>.
- Shelke, Y. and Sharma, A. (2018). *Internet of Medical Things*.
- Shevchenko, N., Chick, T.A., Riordan, P.O., Scanlon, T.P. and Woody, C. (2018). *Threat Modeling: a Summary of Available Methods*. Available from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf.
- Al Shorman, O., Al Shorman, B., Al-Khassaweneh, M. and Alkahtani, F. (2020). A review of internet of medical things (IoMT) - Based remote health monitoring through wearable sensors: A case study for diabetic patients. *Indonesian Journal of Electrical Engineering and Computer Science*, 20(1), pp.414–422.
- Shostack, A. (2014a). Elevation of Privilege: Drawing Developers into Threat Modeling. In: *USENIX Summit on Gaming, Games, and Gamification in Security Education*. pp.1–15.
- Shostack, A. (2014b). *Threat Modeling: Designing for Security*. John Wiley & Sons.
- Silverman, D. (1993). *Interpreting Qualitative Data*. London: Sage.
- Sion, L., Wuyts, K., Yskout, K., Van Landuyt, D. and Joosen, W. (2018). Interaction-Based Privacy Threat Elicitation. In: *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*. IEEE, pp.79–86.
- Sion, L., Yskout, K., Van Landuyt, D. and Joosen, W. (2018). Solution-aware data flow diagrams for security threat modeling. In: *Proceedings of the ACM Symposium on Applied Computing*. pp.1425–1432.
- Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010). Circuits of power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), pp.463–486.
- Solove, D.J. (2002). Conceptualizing privacy. *California Law Review*, 90(4), pp.1087–1155.
- Sommer, F., Dürrwang, J. and Kriesten, R. (2019). Survey and classification of automotive security attacks. *Information (Switzerland)*, 10(4).
- Souppaya, M. and Scarfone, K. (2012). NIST Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs). , 2012, p.17. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>.
- Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P. and Aski, V.J. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, 33(12).
- Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L. and Simperl, E. (2020). Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*, 2(4), pp.1–10.
- Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S. and Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks*, 2018. Available from: <https://www.hindawi.com/journals/scn/2018/5978636/>.
- Susman, G.I., Evered, R.D., Susman, G. and Evered, R.D. (1978). An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*, 23(4), pp.582–603.
- Swiderski, F. and Synder, W. (2004). *Threat Modeling* [online]. Available from:

References

<https://msdn.microsoft.com/en-us/library/ff648644.aspx> [accessed 11 March 2016].

Tan, L. and Wang, N. (2010). Future internet: The Internet of Things. In: *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Future*. IEEE, pp.V5-376-V5-380.

Tarikere, S., Donner, I. and Woods, D. (2021). Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. *Business Horizons*, 64(6), pp.799–807. Available from: <https://doi.org/10.1016/j.bushor.2021.07.015>.

Taylor, K., Sanghera, A., Steedman, M. and Thaxter, M. (2018). *Medtech and the Internet of Medical Things: How Connected Medical Devices are Transforming Health Care*. Available from:

<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf>.

Thomasian, N.M. and Adashi, E.Y. (2021). Cybersecurity in the Internet of Medical Things. *Health Policy and Technology*, 10(3), p.100549. Available from: <https://doi.org/10.1016/j.hlpt.2021.100549>.

Tofan, D.C. (2010). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, 3, pp.128–135.

Tondel, I.A., Jaatun, M. and Meland, P. (2008). Security Requirements for the Rest of Us: A Survey. *IEEE Software*, 25(1), pp.20–27.

Treacy, C., Loane, J. and McCaffery, F. (2020). Developer driven framework for security and privacy in the IoMT. In: *ICSOFT 2020 - Proceedings of the 15th International Conference on Software Technologies*. Springer, pp.443–451.

Treacy, C. and Macher, G. (2019). Best Practices in Design of Systems Applying Functional Safety and Cybersecurity: Cybersecurity & IoT/IoMT. In: *26th EuroSPI Conference*. Edinburgh: Springer Links. Available from: <https://2020.eurospi.net/index.php/workshop#>.

Treacy, C. and McCaffery, F. (2021). Assisting Software Developers to Meet GDPR Data Protection and Privacy Requirements for their IoMT Products. In: *2021 European Medical Device Cybersecurity Virtual Conference*. Virtual: TT Group. Available from: <http://www.emergogroup.com/services/europe/european-medical-device-classification>.

Treacy, C., Loane, J. and McCaffery, F. (2021). Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things. In: *4TH International Clinical Engineering And Health Technology Management Congress (ICEHTMC)*. Lake Buena Vista, FL,: AAMI.

UcedaVélez, T., Morana, M.M., UcedaVelez, T. and Morana, M.M. (2015). *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons.

Verizon. (2018). *2018 Data breach investigations report*. Available from: http://rp_data-breach-investigations-report-2013_en_xg.pdf.

Wagner, P., Hansch, G., Konrad, C., John, K.H., Bauer, J. and Franke, J. (2020). Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises. In: *IEEE Symposium on Emerging Technologies and Factory Automation, ETFA*. pp.1544–1551.

Wei, Y.C., Wu, W.C., Lai, G.H. and Chu, Y.C. (2020). pISRA: privacy considered information security risk assessment model. *Journal of Supercomputing*, 76(3), pp.1468–1481.

Weir, C., Rashid, A. and Noble, J. (2016). How to Improve the Security Skills of Mobile App Developers: Comparing and Contrasting Expert Views. In: *Twelfth Symposium on Usable Privacy and Security {SOUPS}*. Denver. Available from:

References

- http://eprints.lancs.ac.uk/80016/1/SOUPS2016_SIW_AppDev_CW7June16_submitted.pdf.
- Whitman, M.E. and Mattord, H.J. (2011). *Principles of Information Security Fourth Edition*. Boston: Cengage Learning.
- Whitmore, A., Agarwal, A. and Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, 17(2), pp.261–274.
- Williams, P.A. and Woodward, A.J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 8, pp.305–16. Available from: <http://www.dovepress.com/cybersecurity-vulnerabilities-in-medical-devices-a-complex-environment-peer-reviewed-article-MDER>.
- Williams, P.A.H. and McCauley, V. (2017). Always connected: The security challenges of the healthcare Internet of Things. In: *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*. IEEE, pp.30–35.
- Wolf, A., Simopoulos, D., D'Avino, L. and Schwaiger, P. (2020). The PASTA threat model implementation in the IoT development life cycle. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, P-307, pp.1195–1204.
- Wuyts, K. and Joosen, W. (2015). *LINDDUN : a privacy threat analysis framework*. Available from: <https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf>.
- Wuyts, K., Scandariato, R. and Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software*, 96, pp.122–138. Available from: <http://dx.doi.org/10.1016/j.jss.2014.05.075>.
- Wuyts, K. and Wouter, J. (2015). Tutorial privacy threat modeling: a tutorial, Technical Report (CW Reports), LINDDUN tutorial. , C(July). Available from: https://linddun.org/downloads/LINDDUN_tutorial.pdf%0Ahttps://distrinet.cs.kuleuven.be/software/linddun/downloads/LINDDUN_tutorial.pdf.
- Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, 105, pp.581–606.
- Yaghoubi, M., Ahmed, K. and Miao, Y. (2022). Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges. *Journal of Sensor and Actuator Networks*, 11(4).
- Yaqoob, T., Abbas, H. and Shafqat, N. (2020). Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices. *IEEE Journal of Biomedical and Health Informatics*, 24(6), pp.1752–1761.
- Yskout, K., Heyman, T., Scandariato, R. and Joosen, W. (2006). *A system of security patterns*. Available from: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.142.4538>.
- Yuan, S., Fernando, A. and Klonoff, D.C. (2018). Standards for Medical Device Cybersecurity in 2018. *Journal of Diabetes Science and Technology*, 12(4), pp.743–746.
- Zamani, A.T. and Ahmad, J. (2014). IEEE 802.11 Wireless LAN: Security Risks. *International Journal of Research in Information Technology*, 2(2), pp.114–122.
- Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M. and Qadir, J. (2022). Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System †. *Sensors*, 22(21), pp.1–23.

Acronyms

Acronyms

AAA	Authentication, Access Control, and Authorization
AAMI	Association for the Advancement of Medical Instrumentation®
ADR	Action Design Research
API	Application Programming Interface
AR	Action Research
ASC	Application Security Controls
ASMP	Application Security Management Process
BLE	Bluetooth/ Bluetooth Low Energy
BSN	Body sensor networks
CAPs	Composed Assurance Packages
CAR	Canonical Action Research
CAREC	Common Attack Pattern Enumeration and Classification
CGM	Continuous Glucose Monitoring
CIA	Confidentiality, Integrity and Availability
CTO	Chief Technical Officer
CWE	Common Weakness Enumeration
DFD	Data Flow Diagram
DFSPCs	Data Flow Security and Privacy Controls
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPR	Data Protection Representative
DR	Design Research
DSR	Design Science Research
EALs	evaluation assurance levels
ENISA	European Union Agency for Cybersecurity
EU	European Union
FDA	Food and Drug administration
FRs	Foundational Requirements
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HPRA	Health Products Regulatory Authority
IACS	Industrial Automation and Control Systems

Acronyms

ICO	Information Commissioners Office
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMDRF	International Medical Device Regulators Forum
IOI	Items of Interest
IoMT	Internet of Medical Things
IoT	Internet of Things
IPR	Interview Protocol Refinement
IPS	Federal Information Processing Standards
ISME	Irish Small and Medium Enterprise Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
KWS	Keyword Search
MDR	Medical Device Regulation
MMA	Mobile Medical Applications (App)
NIST SP	National Institute of Standards and Technology Special Publication
ONF	Organisation Normative Framework
OS	Operating System
OWASP	Open Web Application Security Project
PANs	Personal Area Networks
PASTA	Process for Attack Simulation and Threat Analysis
PbD	Privacy by Design
PD	Personal Data
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PIMS	Privacy Information Management System
PP	Protection Profile
RSRC	Regulated Software Research Centre
SaMD	Software as a Medical Device
SAR	SAR Security Assurance Requirement

Acronyms

SbD	Security by Design
SDLC	Software Development Lifecycle
SFRs	Security Functional Requirements
SME	Small Medium Enterprise
SOP	Standard Operating Process
SSE_CMM	Systems Security Engineering - Capability Maturity Model®
SSI	Semi-Structured Interview
ST	Security Target
TM	Threat Modeling
TOE	Target of Evaluation
TR	Technical Report
TSF	TOE Security Functionality
UWB	Ultra-Wide Band
WBANs	Wireless Body Area Network
WMTS	Wireless Medical Telemetry Service

Glossary of Terms

ATTACK

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself

CONTROL

The administrative, technical, and physical safeguards employed within a system to ensure compliance with applicable data protection requirements and manage risks

CYBERATTACK

An attack, via cyberspace, targeting an enterprise for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information or obtaining unauthorized access

DATA ACTIONS

System operations that process PII

DATA FLOW

Movement of data through the active parts of a data processing system in the course of the performance of specific work

DATA PRIVACY

Can be defined as the collection, processing and dissemination of personal data in a manner that inhibits the incidence of undesirable privacy events and their negative impacts on data subjects

DATA PROTECTION

Takes into account the state of the art, cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons

DATA PROTECTION BY DESIGN AND BY DEFAULT

Means data protection must be included into your processing activities and business practices, from the design stage right through the data lifecycle

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Is a means for building and demonstrating compliance

DATA PROTECTION REGULATION

Lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

DATA SECURITY

Means that data is stored and transferred securely

INFORMATION SECURITY

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

INTERNET OF THINGS (IoT)

Can comprise a multitude of diverse devices from consumer devices, such as phones, tablets and wearables, to industrial sensors, actuators and monitors

INTERNET OF MEDICAL THINGS (IoMT)

Is essentially an IoT-based solution that enables the development of IoT enabled healthcare systems for monitoring, diagnosis and a variety of different kinds of healthcare uses

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual

PROCESSING

Operation or set of operations performed upon PII that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of PII

RESIDUAL RISK

Risk remaining after risk control measures have been taken

RISK

A measure of the extent to which an entity or individual is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence

RISK ANALYSIS

Systematic use of available information to identify hazards and to estimate the risk

RISK ASSESSMENT

Overall Process comprising of Risk Analysis and Risk Evaluation

RISK CONTROL

Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

RISK EVALUATION

Process of comparing the estimated risk against given risk criteria to determine the acceptability of the risk

RISK MITIGATION

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A subset of Risk Response

SECURITY AND PRIVACY PRINCIPLES

Are led by regional regulatory requirements and can be embedded as a part of international certification such as ISO 27001

STANDARD

A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used to ensure that materials, products, processes and services are fit for purpose

SYSTEM

Combination of interacting elements organized to achieve one or more stated purposes

THREAT

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service

THREAT ASSESSMENT

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat

THREAT MODELING

Is a form of risk assessment that models aspects of the attack and defense sides of a particular logical entity, such as a piece of data, an application, a host, a system, or an environment

VULNERABILITY

A vulnerability within the system may lead to a breach of data and system security via an exploit by a threat source

Appendix A Framework Review Information Leaflet and Questionnaire

STUDY TITLE: Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things (IoMT)
Researcher: Ceara Treacy (ceara.treacy@dkit.ie) +353 (0)879897884 Supervisors: Prof. Fergal McCaffery (fergal.mccaffery@dkit.ie) Dr. John Loane (john.loane@dkit.ie)
Background and Instructions
<p>My name is Ceara Treacy, and I am conducting this research for my PhD Degree at Dundalk Institute of Technology, Dundalk, Ireland.</p> <p>This study is being completed to assist inexperienced SMEs and developers meet security and privacy regulatory requirements for data in flow in the IoMT. The IoMT is a fast-growing domain as healthcare moves out of structured health services into care in the community. As a result, the sensitive personal and health data associated with the IoMT can potentially flow through a diversity of apps, systems, devices and technologies, public and open networks. This exposes data in the IoMT to additional attack surfaces, which requires the hardening of the security and privacy of the data. Consequently, the data is bound by regulatory security and privacy requirements enforced by the General Data Protection Regulation (GDPR). A key GDPR requirement for any project processing personal data and data concerning health, is security and privacy by design and a data protection impact assessment. Applying regulatory compliant requirements is a struggle for developers in SMEs due to lack of knowledge, experience, understanding and specific standards and guidance. This PhD research developed a framework for developers in SMEs, to assist in meeting regulatory compliance for security and privacy of data in flow in the IoMT. The framework is founded in the data protection principles of the GDPR, security and privacy by design. The framework expands on the established threat modeling steps to apply both security and privacy properties to protect data in flow in the IoMT. To mitigate the identified security and privacy threats, the framework includes a set of categorised technical security and privacy controls developed through medical device security and privacy standards. The originality of this framework is the inclusion of security and privacy requirements in the extension of the traditional threat modeling process, the security and privacy controls embedded in the medical security standards and the documentation of this systematic process in an innovative data protection impact assessment.</p> <p>You are being invited to take part in this study as an expert reviewer.</p> <p>Before you decide whether or not you wish to take part, please clearly understand the risks and benefits of taking part in this study so that you can make a decision that is right for you. This process is known as 'Informed Consent'. You do not have to take part in this study.</p> <p>This part of the research will involve expert review of the framework as part of this study. The focus will be on a review of the structure of the framework and the composition of the steps to elicit feedback on the framework's usability and value.</p>

This Document is divided into the following sections - What is Covered	
SECTION A	Participant Consent Form – This will provide consent for use of the data from the expert review and discussions from the participant for the study.
SECTION B	Participant Profile - Details that gather your experience and knowledge in this domain
SECTION C	Review Questionnaire – Three parts Framework Value Composition, Usability

Please go through the sections and where relevant:

1. Mark your choice with an “X” in the box provided
2. Use the rating system provided in the section to indicate your preference in the box provided
3. Please note that some questions require a single response, while others may require multiple responses and request for additional opinions
4. The input you provide will be treated with strictest confidentiality and with guaranteed anonymity and only used towards the completion of the afore- mentioned qualification

SECTION A Participant Consent Form

Study title: Developer Driven Framework for Security and Privacy of Data in Flow in the Internet of Medical Things (IoMT)

I have read and understood the Background and Instructions about this research study. The information has been fully explained to me and I have been able to ask questions, all of which have been answered to my satisfaction.	Yes <input type="checkbox"/> No <input type="checkbox"/>
I understand that I don’t have to take part in this study and that I can opt out at any time. I understand that I don’t have to give a reason for opting out and I understand that opting out won’t affect my future	Yes <input type="checkbox"/> No <input type="checkbox"/>
I am aware some audiotaping will be used for data collection to assist the researcher capture all information.	Yes <input type="checkbox"/> No <input type="checkbox"/>
I have been assured that information about me will be kept private and confidential.	Yes <input type="checkbox"/> No <input type="checkbox"/>
I have been given a copy of the research Background and this completed consent form for my records.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Storage and future use of information	Yes <input type="checkbox"/> No <input type="checkbox"/>
I give my permission for information collected about me to be stored or electronically processed for the purpose of research and to be used in <u>related studies or other studies in the future</u> but only if the research is approved by a Research Ethics Committee.	

Participant Name (Block Capitals) | Participant Signature | Date

To be completed by the Researcher:

I, the undersigned, have taken the time to fully explain to the above participant the nature and purpose of this study in a way that they could understand. I have explained the risks involved as well as the possible benefits. I have invited them to ask questions on any aspect of the study that concerned them.

Name (Block Capitals) | Signature | Date

SECTION B Participant Profile			
1. Is data security important for your domain?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
2. Is data privacy important for your domain?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
3. Do you work in a safety critical domain?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
If yes, how many years?		Less than 1 year	<input type="checkbox"/>
		1-2 years	<input type="checkbox"/>
		1-3 years	<input type="checkbox"/>
		1-5 years	<input type="checkbox"/>
		5years and more	<input type="checkbox"/>
What is the domain _____			
4. Have you experience applying security in development?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
If yes, how many years?		Less than 1 year	<input type="checkbox"/>
		1-2 years	<input type="checkbox"/>
		1-3 years	<input type="checkbox"/>
		1-5 years	<input type="checkbox"/>
		5years and more	<input type="checkbox"/>
5. Have you experience with STRIDE?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
If yes how many years?		Level of Experience	
Less than 1 year	<input type="checkbox"/>	Excellent	<input type="checkbox"/>
1-2 years	<input type="checkbox"/>	Good	<input type="checkbox"/>
1-3 years	<input type="checkbox"/>	Fair	<input type="checkbox"/>
1-5 years	<input type="checkbox"/>	Poor	<input type="checkbox"/>
5years and more	<input type="checkbox"/>	Very Poor	<input type="checkbox"/>
6. Have you experience with implementation of controls for security in the software development process?		Yes	<input type="checkbox"/> No <input type="checkbox"/>
If yes how many years?		Level of Experience	
Less than 1 year	<input type="checkbox"/>	Excellent	<input type="checkbox"/>
1-2 years	<input type="checkbox"/>	Good	<input type="checkbox"/>
1-3 years	<input type="checkbox"/>	Fair	<input type="checkbox"/>
1-5 years	<input type="checkbox"/>	Poor	<input type="checkbox"/>
5years and more	<input type="checkbox"/>	Very Poor	<input type="checkbox"/>
7. Please provide further details of your experience with security in software development.			

8. Have you experience in applying privacy in development?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes, how many years?	Less than 1 year	<input type="checkbox"/>	
	1-2 years	<input type="checkbox"/>	
	1-3 years	<input type="checkbox"/>	
	1-5 years	<input type="checkbox"/>	
	5years and more	<input type="checkbox"/>	
9. Have you experience with LINDDUN?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes how many years?	Level of Experience		
Less than 1 year <input type="checkbox"/>	Excellent	<input type="checkbox"/>	
1-2 years <input type="checkbox"/>	Good	<input type="checkbox"/>	
1-3 years <input type="checkbox"/>	Fair	<input type="checkbox"/>	
1-5 years <input type="checkbox"/>	Poor	<input type="checkbox"/>	
5years and more <input type="checkbox"/>	Very Poor	<input type="checkbox"/>	
10. Have you experience with implementation of controls for privacy in the software development process?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes how many years?	Level of Experience		
Less than 1 year <input type="checkbox"/>	Excellent	<input type="checkbox"/>	
1-2 years <input type="checkbox"/>	Good	<input type="checkbox"/>	
1-3 years <input type="checkbox"/>	Fair	<input type="checkbox"/>	
1-5 years <input type="checkbox"/>	Poor	<input type="checkbox"/>	
5years and more <input type="checkbox"/>	Very Poor	<input type="checkbox"/>	
11. Please provide further details of your experience with privacy in software development.			
12. Have you been involved in the development of any processes or methodologies for security or privacy in the software development process?			

SECTION C Expert Review Questionnaire**1. Framework Value**

1.1 In your opinion there is a gap for a specific individual implementation process for both security and privacy for SMEs and inexperienced developers in this domain?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

1.2 In your opinion there is a gap in explicit guidance for inexperienced SMEs and developers in the application of both security and privacy in software development within regulatory requirements?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

1.3 Do you agree that the framework provides sufficient guidance about how to go about security and privacy risk assessment in the domain?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

1.4 Do you agree the framework would provide adequate risk assessment and meet the security and privacy requirements for a system?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

1.5 Could you provide a brief overview of the main benefits you have observed the framework could provide for inexperienced SMEs and developers?

Step 1	
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	

1.6 Could you provide a brief overview of the main obstacles or problems you have observed in the framework for inexperienced SMEs and developers to assess and deliver security and privacy?

Step 1	
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	

1.7 In your experience, would the purpose of the activities and outcomes of the framework assist inexperienced SMEs and developers with security and privacy risk assessment requirements?

Step 1	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 2	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 3	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 4	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 5	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary

Step 6	No	<input type="checkbox"/>	Please provide any further details you consider necessary
	Unknown	<input type="checkbox"/>	
	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

1.8 To the best of your knowledge does the framework fail to identify any security and privacy risk assessment necessities for inexperienced SMEs and developers?

Yes	<input type="checkbox"/>	Please provide a short rationale for your opinion
No	<input type="checkbox"/>	
Unknown	<input type="checkbox"/>	

1.9 Do you have any suggestions to improve the Framework value?

Yes	<input type="checkbox"/>	Please provide any further information you deem applicable
No	<input type="checkbox"/>	

2 Framework Composition

2.1 Is the Framework Summary and rationale easy to understand and follow?

Yes	<input type="checkbox"/>	Please provide a short rationale for your opinion
No	<input type="checkbox"/>	
Unknown	<input type="checkbox"/>	

2.2 Are the framework steps easy to understand and follow?

Step 1	Yes	<input type="checkbox"/>	Please provide any further details you consider relevant
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 2	Yes	<input type="checkbox"/>	Please provide any further details you consider relevant
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

Appendix A

Step 3	Yes	<input type="checkbox"/>	Please provide any further details you consider relevant
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 4	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 5	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 6	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

2.3 Do you agree with the order of implementation depicted in Figure 2 and in the framework steps?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree or Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

2.4 Do you agree the activities for each step are correct and in the correct order?

Step 1	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	
	Strongly Disagree	<input type="checkbox"/>	
Step 2	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	

Appendix A

	Strongly Disagree	<input type="checkbox"/>	
--	-------------------	--------------------------	--

Step 3	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	
	Strongly Disagree	<input type="checkbox"/>	

Step 4	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	
	Strongly Disagree	<input type="checkbox"/>	

Step 5	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	
	Strongly Disagree	<input type="checkbox"/>	

Step 6	Strongly Agree	<input type="checkbox"/>	Please provide any further details you consider necessary
	Agree	<input type="checkbox"/>	
	Neither Agree nor Disagree	<input type="checkbox"/>	
	Disagree	<input type="checkbox"/>	
	Strongly Disagree	<input type="checkbox"/>	

2.5 Do you believe any of the activities or processes of the steps of the framework are unnecessary?

Step 1	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 2	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 3	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 4	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 5	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 6	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

2.6 Do you think any other activities or processes should be included in the steps?

Step 1	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 2	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 3	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

Appendix A

Step 4	Yes	<input type="checkbox"/>	Please provide any further details you consider necessary
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 5	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	
Step 6	Yes	<input type="checkbox"/>	
	No	<input type="checkbox"/>	
	Unknown	<input type="checkbox"/>	

2.7 In your opinion does the threat to attack starter kit library provide guidance and assistance for identification of threats to attacks for application in the framework for inexperienced SMEs and developers?

Yes	<input type="checkbox"/>	Please provide a short rationale for your opinion
No	<input type="checkbox"/>	
Unknown	<input type="checkbox"/>	

2.8 To the best of your knowledge does the framework fail to identify any security and privacy risk assessment tasks for inexperienced SMEs and developers?

Yes	<input type="checkbox"/>	Please provide a short rationale for your opinion
No	<input type="checkbox"/>	
Unknown	<input type="checkbox"/>	

2.9 Does the framework omit any key details which should be included which would assist SMEs and developers from following this framework?

Yes	<input type="checkbox"/>	Please provide a short rationale for your opinion
No	<input type="checkbox"/>	
Unknown	<input type="checkbox"/>	

2.10 Overall, how would you characterise your understanding of the framework and its outcomes?

Excellent	<input type="checkbox"/>	Please provide a short rationale for your opinion
Good	<input type="checkbox"/>	
Fair	<input type="checkbox"/>	
Poor	<input type="checkbox"/>	
Very Poor	<input type="checkbox"/>	

2.11 Can you name and briefly describe any deficiency you have observed in the framework?

3 Framework Usability

3.1 To what extent do you agree that the framework is usable for inexperienced SMEs and developers in practice?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

3.2 To what extent do you agree that the framework is adaptable and customisable for inexperienced SMEs and developers?

Strongly Agree	<input type="checkbox"/>	Please provide a short rationale for your opinion
Agree	<input type="checkbox"/>	
Neither Agree nor Disagree	<input type="checkbox"/>	
Disagree	<input type="checkbox"/>	
Strongly Disagree	<input type="checkbox"/>	

3.3 Can you outline any deficiencies you have observed in the framework's usability?

--

3.4 Do you have any suggestions to improve the framework usability? If yes, please state them?

--

Appendix B Questionnaire Questions Matrix Mapped to RSQs.

Questionnaire Question	RSQ. 1 What challenges are faced by software developers in SMEs in meeting the GDPR data protection requirements in software development in the IoMT?	RSQ. 2 What are the methods and/or standards for security and privacy risk assessment for software development?	RSQ. 3 What components should be in a framework to assist software developers demonstrate compliance with GDPR data protection requirements in the IoMT?	RSQ. 4 To what extent can the framework address the difficulties experienced by software developers in SMEs, when implementing security and privacy for data in flow in the IoMT?
1. Value				
1.1. In your opinion is there a gap for a specific individual implementation process for both security and privacy for SMEs for inexperienced developers in this domain?	X			
1.2. In your opinion is there a gap in explicit guidance for developers of SMEs inexperienced in security and privacy in software development within regulatory requirements and the application of both?	X	X		
1.2. Do you agree that the framework provides sufficient guidance about how to go about security and privacy risk assessment in the domain?	X	X		X
1.3. Do you agree the framework would provide an adequate risk assessment and meet the security and privacy requirements for a system?		X		X

Appendix B

1.4. Could you provide a brief overview of the main benefits you have observed the framework could provide for developers of SMEs inexperienced with implementing data security and privacy during development?			X	X
1.5. In your experience, would the purpose of the activities and outcomes of the framework assist developers in SMEs inexperienced with security and privacy risk assessment meet regulatory requirements?			X	X
1.6. To the best of your knowledge does the framework fail to identify any security and privacy risk assessment necessities for inexperienced SMEs and developers?			X	X
1.7. Do you have any suggestions to improve the Framework value?				X
2. Composition				
2.1. Is the framework summary and rationale easy to understand and follow?			X	X
2.2. Are the framework steps easy to understand and follow?		X		X
2.3. Do you agree with the order of implementation depicted in Figure 2 and in the framework steps?			X	X
2.4. Do you agree the activities for each step are correct and in the correct order?			X	X

Appendix B

2.5. Do you believe any of the activities or processes of the steps of the framework are unnecessary?			X	X
2.6. Do you think any other activities or processes should be included in the steps?			X	X
2.7. In your opinion does the threat to attack starter kit library provide guidance and assistance for identification of threats to attacks for application in the framework for inexperienced SMEs and developers?	X		X	X
2.8. To the best of your knowledge does the framework fail to identify any security and privacy risk assessment tasks for inexperienced SMEs and developers?			X	X
2.9. Does the framework omit any key details which should be included which would assist SMEs and developers from following this framework?			X	X
2.10. Overall how would you characterise your understanding of the framework and its outcomes?				X
2.11. Can you name and briefly describe any deficiency you have observed in the framework?				X
3. Composition				
2.1 To what extent do you agree that the framework is usable for inexperienced SMEs and developers in practice?	X			X

Appendix B

2.2 To what extent do you agree that the framework is adaptable and customisable for inexperienced SMEs and developers?	X			X
2.3 Can you outline any deficiencies you have observed in the framework's usability?			X	X
2.4 Do you have any suggestions to improve the framework usability? If yes, please state them?			X	X

Appendix C Presentation to Experts



Appendix D

Appendix D Key Word Search and Validation of Nist SP-800-53 R5, ISO/IEC 15408-2 and IEC 62443-3

Please find a Copy of the key word search and validation on the Accompanied USB in the Folder FRAMEWORK

Appendix E Interview Protocol Matrix - Focus Group Questions

STATSports Final Focus Group Questions The questions prompted from the expert review are marked with an asterisk *	RSQ.1	RSQ.2	RSQ.3	RSQ.4	RO.1	RO.2	RO.3	RO.5	RO.6
1. Framework Value									
1.1 In your opinion is there a gap for a specific individual implementation process for both security and privacy for developers of SMEs inexperienced in this domain?	X								
Focus group open-ended questions									
(a) Did the framework provide a tailored process that covers the needs for applying security and privacy of data in the individual software development project? *					X	X			
(b) Does the framework present data security and privacy requirements on an equal basis?							X		
(c) What challenges or difficulties did the software team encounter in applying security and privacy at the same time during development using the framework?						X			
1.2 In your opinion is there a gap in explicit guidance for developers of SMEs inexperienced in security and privacy in software development within regulatory requirements and the application of both?	X	X							
Focus group open-ended questions									
(a) Does the framework provide adequate information on the regulatory requirements for data security and privacy?*						X			
(b) Does the framework provide enough information on implementing the regulatory requirements? *						X			
Step 1 relevant questions									
(a) Does step 1 provide enough guidance for the software development team in understanding the data security and privacy regulatory requirements?					X	X			
(b) Does step 1 help the development team to better understand what data is required to be kept secure and private?							X		
(c) How did the development team find completing the processes to categorise the data involved in the software development project?							X		
(d) The Screening statements, process 1.5, is a significant aspect of the framework to meet GDPR requirements. Was its importance appreciated by the software team? *					X		X		
(e) How did the development team find developing the Screening statements?					X		X		
(f) Table 7 – Lawful Processing is the most significant aspect of the framework to meet GDPR requirements. Was its importance understood by the software team? *					X		X		

Appendix E

(g) Is the draft privacy policy a valuable asset to the development team? Would you recommend keeping it in the framework?						X		X		
(h) How easy/difficult did the team find populating and using the draft privacy policy?						X		X		
General questions										
(a) Does the framework present the data security and privacy regulatory requirements in a language the development team can follow?						X		X		
(b) Is there enough information and guidance in the framework for the software team for the application of both security and privacy in software development within regulatory requirements?						X		X		
(c) Would the software team have a better understanding and knowledge to address regulatory requirements for data security and privacy in software from implementing the framework?										
1.3 Do you agree that the framework provides sufficient guidance about how to go about security and privacy risk assessment in the domain?		X		X						
Focus group open-ended questions										
(a) How does the framework security and privacy risk assessment implementation differ to the former risk assessment used by software development team?							X			
(b) Was the guidance sufficient to enable the software development team to follow the risk assessment process for both security and privacy?							X			
1.4 Do you agree the framework would provide an adequate risk assessment and meet the security and privacy requirements for a system?		X		X						
Focus group open-ended questions										
(a) Were the risk analysis tables in Step 4 easy to use? *						X	X			
(b) Does the team think the risk assessment scales were adequate for the purpose of step 4? *										X
(c) Would an illustrated example help with the risk assessment process? *									X	
(d) Did the risk analysis work as well for both security and privacy?						X				
(e) Does the team have more or less confidence in completing a security and privacy risk assessment after implementing the framework?							X			
(f) Do you think the risk assessment model was sufficient to help guide the software development team on what risks to address first?										X

Appendix E

1.5 Could you provide a brief overview of the main benefits you have observed the framework could provide for developers of SMEs inexperienced with implementing data security and privacy during development?			X	X					
Focus group open-ended questions									
(a) Does it assist the software team's knowledge and understanding of data security and privacy regulatory requirements for a development project?									X
(b) Does it assist the software team's knowledge and understanding of data security and privacy regulatory requirements for a development project?									X
(c) Does it provide confidence for the software team that the regulatory requirements for data security and privacy in the development project have been met?									X
(d) Does it assist the software team in applying data security and privacy requirements for a development project?									X
1.6 In your experience, would the purpose of the activities and outcomes of the framework assist developers in SMEs inexperienced with security and privacy risk assessment meet regulatory requirements?			X	X					
Focus group open-ended questions									
(a) Does the framework provide adequate information on the regulatory requirements for data security and privacy?*									X
(b) Does the framework provide enough information on implementing the regulatory requirements?*									X
(c) Are there individual components that are more valuable than others to inexperienced developers in your opinion?									X
(d) Are there individual components or processes that are not needed or are over complicated in the framework?									X
1.7 To the best of your knowledge does the framework fail to identify any security and privacy risk assessment necessities for inexperienced SMEs and developers?			X	X					
Focus group open-ended questions									
(a) Is the security and privacy risk assessment easy to follow?									X
(b) What is missing to assist the inexperienced developer better understand security and privacy risk assessment?									X
(c) Is there anything that would make the security and privacy risk assessment more understandable?									X
1.8 Do you have any suggestions to improve the Framework value?				X					

Appendix E

Focus group open-ended questions									
(a) Does the framework make security and privacy risk assessment achievable for developers inexperienced in this domain?									X
2 Framework Composition									
2.1 Is the Framework summary and rationale easy to understand and follow?			X	X					
Focus group open-ended questions									
(a) Does the summary provide a clear overview of the framework and the steps in the framework? *									X
(b) Does figure 1 provide a clear overview?									X
(c) Do you have any suggestions that would make the summary and rationale easier to understand/clearer?									X
2.2 Are the framework steps easy to understand and follow?		X		X					
Focus group open-ended questions									
General Questions									
(a) Is there continuity with the framework steps? Do they flow naturally? *									X
(b) Which steps create an issue for implementation? *									X
Step 1 Contextual Knowledge									
(a) Is it appropriate to include awareness measures in step 1?									X
(b) How did including awareness in this step help/hinder the implementation of the framework? *									X
(c) How did the development team find completing the processes to categorise the data involved in the software development project?							X		X
(d) The screening statements, process 1.5, is a significant aspect of the framework to meet GDPR requirements. Was its importance appreciated by the software team? *							X		X
(e) How did the development team find developing the screening statements?							X		X
(f) How did the development team find the processes to populate Table 7?							X		X
(g) Is the draft privacy policy a valuable asset to the development team? Would you recommend keeping it in the framework?							X		X
(h) How easy/difficult did the team find populating and using the draft privacy policy?							X		X
Step 2 – System Decomposition									
(a) Was the process of listing already known security and privacy decisions or constraints logical and useful process for the*							X		X
i. Software development team?							X		X
ii. Organisation of the security and privacy requirements for the framework?							X		X

Appendix E

iii. System decomposition process?								X		X
iv. Risk assessment process?								X		X
(b) Were the team able to identify assets with the guidance provided in step 2?								X		X
(c) Was the information provided to produce a DFD easy to follow?								X		X
(d) What information for DFDs was particularly useful?								X		X
(e) What information for DFDs was unclear or difficult to follow?								X		X
(f) How did the team find applying the security and privacy annotations to the DFDs?								X		X
(g) Were the annotations useful in considering and separating data security and privacy requirements?								X		X
(h) The documentation of the trust boundaries, entry and exit points are a significant aspect of the threat modeling process of the framework for the step 3 per-interaction threat elicitation process. Was this importance clear in the framework?								X		X
(i) Was the information guidance acceptable/suitable to document the trust boundaries, entry and exit points?								X		X
Step 3 – Threat Elicitation										
(a) Is the guidance in step 3 adequate for developers inexperienced in threat elicitation to implement this step? *								X		X
(b) How did the team find step 3? Was it too complicated/confusing/intricate? *								X		X
(c) Are the components and processes of step 3 arduous? *								X		X
(d) Is the information on per-interaction elicitation adequate for the team to understand and complete this process?								X		X
(e) Is there enough guidance in step 3 to help the software development team elicit threats?								X		X
(f) Would step 3 be possible without the threat to attack starter kit?								X		X
(g) Was the threat to attack starter kit easy to use? *								X		X
Step 4 – Analysis and Prioritisation of the Threats										
(a) Was the guidance “understanding the risk assessment model” clear and easy to follow?								X		X
(b) Was the risk assessment model easy to follow?								X		X
(c) Did the tables help prioritise the threats to address first?								X		X
Steps 2-4 general questions – risk assessment threat modeling										
(a) Is it plain that steps 2-4 are the risk assessment (threat modeling) process of the framework?								X		X
(b) Is the threat modeling process clear and concise?								X		X

Appendix E

(c) Did the software team find the risk assessment model in the framework easy to follow?								X		X
(d) Was the process to track the risk assessment process for both data security and privacy practicable for the software team? Was it confusing?								X		X
(e) Would a full illustrated example help with the risk assessment process? *									X	
Step 5 Map Threats back to Framework Properties – potential answers for question 2.5 below										
(a) Is this step necessary? *								X		
(b) In your opinion should this step be combined with step 6? *										X
Step 6 Selection of Data Flow Security and Privacy Controls (DFSPCs)										
(a) Was it clear how to implement this step? *								X		X
(b) Were the controls easy to match to the threats mapping via the framework properties? *								X		X
(c) Was the process to find the controls easy?								X		X
(d) Is it clear how to select the most appropriate controls? *								X		X
(e) Did the controls support data security and privacy for the project?								X		X
2.3 Do you agree with the order of implementation depicted in Figure 2 and in the framework steps?			X	X						
Focus group open-ended questions										
(a) Does fig. 2 depict the steps of the framework clearly? *								X		
(b) Does fig. 2 need reworked or improved? *										X
2.4 Do you agree the activities for each step are correct and in the correct order?			X	X						
Focus group open-ended questions										
(a) Which activities create an issue for implementation?								X		
(b) Which activities do you feel are not necessary or could be shortened/reduced?										X
(c) In step 3 is the security and privacy knowledge offered in a systematic way? *										
2.5 Do you believe any of the activities or processes of the framework are unnecessary?										
Focus group open-ended questions										
Step 5 see answer to question 2.2 above								X		
Step 5 Map Threats back to Framework Properties – potentially answered in question 2.2 above										X
Step 6 Select controls to mitigate threats										
(a) Does step 6 need more information/guidance on how to apply and select suitable controls? *								X		X

Appendix E

2.6 Do you think any other activities or processes should be included in the steps?			X	X					
Focus group open-ended questions									
(a) Does step 1 require more clarification around the GDPR requirement for documenting the personal data involved in the project and how this data will be processed? *								X	
2.7 In your opinion does the threat to attack starter kit library provide guidance and assistance for identification of threats to attacks for application in the framework for SMEs and developers inexperienced in this domain?	X		X	X					
Focus group open-ended questions									
(a) Did the library help with awareness of potential threats?								X	
(b) Would this step have been possible without the library as guidance?								X	
(c) Would the team see the threat to attack starter kit library as background information or as a necessity for developers inexperienced in this domain to complete step 3? *									X
2.8 To the best of your knowledge does the framework fail to identify any security and privacy risk assessment tasks for SMEs and developers inexperienced in risk assessment?			X	X					
Focus group open-ended questions									
(a) Is there any further information or processes needed to help the developers to identify security and privacy risks?								X	X
2.9 Does the framework omit any key details which should be included which would assist SMEs and developers from following this framework?			X	X					
Focus group open-ended questions									
(a) Would a how to use guide be useful for the framework? *								X	
(b) What suggestions would you provide in constructing a how to use guide from a software development viewpoint after implementing the framework?								X	
2.10 Overall how would you characterise your understanding of the framework and its outcomes?				X					
Focus group open-ended questions									
(a) Is the complexity of the framework a barrier or deterrent for it's implementation?									X
(b) Did the team expect a quick fix for privacy and security by design? *								X	
(c) Does the software team think there is an easier way to include privacy and security by design into the development process?									X

Appendix E

2.11 Can you name and briefly describe any deficiency you have observed in the framework?				X					
Focus group open-ended questions									
(a) What information was difficult to process and apply? *									X
(b) Is there too little focus on the legal requirements? *							X		X
3 Framework Usability									
3.1 To what extent do you agree that the framework is usable for SME developers inexperienced in data security and privacy in daily practice?		X		X					
Focus group open-ended questions									
(a) What in the steps was easy to apply?									X
(b) What in the steps was difficult to apply?									X
(c) Can you identify any examples of missing guidance/information that in your opinion made the steps difficult to implement?							X		X
(d) Can you identify a part of particularly good guidance that helped with the steps implementation?									X
3.2 To what extent do you agree that the framework is adaptable and customisable for SMEs developers inexperienced in data security and privacy along with regulatory requirements?		X		X					
Focus group open-ended questions									
(a) Does the framework provide adequate information on the regulatory requirements for data security and privacy? *							X		X
(b) Does the framework provide enough information on implementing the regulatory requirements? *							X		X
(c) Does the framework need to identify which steps can/should be personalized? *									X
(d) Are there any specific challenges or obstacles in implementation?									X
3.3 Can you outline any deficiencies you have observed in the framework's usability?			X	X					
Focus group open-ended questions									
(a) Is the body of knowledge in the framework steps too complex for inexperienced developers in data security and privacy and risk assessment to use? *									X
(b) Is the body of information in the framework disorganised? *									X
(c) Do the framework steps contain too much information? *									X
(d) Was the information difficult to understand? *									X

Appendix E

3.4 Do you have any suggestions to improve the framework usability. If yes, please state them?			X	X					
Focus group open-ended questions									
(a) Does the current format of the framework work? *									X
If no, why?									X
If yes, why?									X
(b) Would the framework be better written as a technical document with an accompanying academic guide? *								X	
(c) Would the framework benefit from an accompanying tutorial? *								X	
(d) What format would you suggest for an accompanying tutorial, (written/recorded example) from a development team that have implemented the framework?								X	
(e) Would the framework benefit from an accompanying tutorial? *								X	
(f) What format would you suggest for an accompanying tutorial, (written/recorded example) from a development team that have implemented the framework?								X	

Appendix F Expert Review SSI Transcript – Dr. Kim Wuyts

Transcript of interview held over Teams on 27th April 2021.

Persons Present:

CEARA TREACY

DR. WUYTS

Dr. KIM WUYTS: Do you see anything? It says, 'Recording Pending', hmm.
CEARA TREACY: Yeah, yeah, this meeting is being recorded by joining you and giving consent for this meeting to be recorded. That's great. Yeah, no, I think what happens is, it pops up on the chat.

Dr. KIM WUYTS: Okay.
CEARA TREACY: So then, we both have access to it then.
Dr. KIM WUYTS: Good.
CEARA TREACY: You know, and then you can download it. Hopefully now, I don't want anything, I have no backup. Do you know they always say, 'Backup, backup, backup' So, I'm assuming Teams will just, to work this for me? So, what I will do, will, well, do you want to go through the actually, what your comments are first on the framework and that might-
Dr. KIM WUYTS: Yeah, that's fine.
CEARA TREACY: -help with the discussions.
Dr. KIM WUYTS: It's just very limited stuff but, I mean, some, some minor stuff.
CEARA TREACY: And I'll just take notes at the end of this document as well. I'll send you all of this whenever it's done, you know, what my-
Dr. KIM WUYTS: Where has it gone? Yeah, some of the things already come, come back but, let me see if I can share my window but I have so many depths open that it might be a bit problematic. It will not work because my, apparently, my settings are not, I will probably have to restart Teams. So...

CEARA TREACY: Oh that's, do you want to-
Dr. KIM WUYTS: I was not; I was not-
CEARA TREACY: -email it through to me and I can share my screen?
Dr. KIM WUYTS: Oh yes, or, yeah, I will, I will email it to you and then maybe we can just go through it anyway. It's just really minor stuff. I think it's this one. Hmm, is it showing it?
CEARA TREACY: Yeah, got it here.
Dr. KIM WUYTS: Do you see my comments?
CEARA TREACY: I'm just going to download it and then I'll share my screen here and we can...my, I don't know whether there's something in the operating system or whether my mouse is running out of battery, do you know, sometimes when you type-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -it doesn't hit everything, and I know that Microsoft are, yeah, did a big update on Windows 10 and I think that wrecked a whole pile of things, I don't know. Right, okay, share screen.

Dr. KIM WUYTS: Yeah, if that doesn't work, we can just go through them. Can you see my comments somewhere? Yeah, I think if you go to somewhere, you can, get them at the left, but I-
CEARA TREACY: Okay. Can you see my screen?
Dr. KIM WUYTS: Yes, I can, yeah, okay.
CEARA TREACY: 'Shouldn't the processing actions and purposes be specified first?'
Dr. KIM WUYTS: Yeah, I think I came back to, to that in the question there as well. I was just thinking, like, well, yeah, basically, what it says there, when, when you are already drafting a privacy policy in one of the first steps, it

Appendix F

- seems like you're doing it too soon because you're still, well, at least from, from the way I see it, you're still in the design phase and you're still trying to specify what you're doing and, and how you will be doing it. [0.05.05.8] So, if you already draft a policy now, you will probably have to revise it later on.
- CEARA TREACY: Okay. So, it should be, 'This is the start of the drafting, start of the, start drafting'.
- Dr. KIM WUYTS: Yeah, well, it's definitely useful because by thinking about it, you are thinking about the general privacy strategy and you will implement it within the design probably but, like, it felt to me like this was like the policy you would give out to the user which maybe not the thing you were saying here but this was how it came to mind for me.
- CEARA TREACY: No, you're correct. So, this would be, the privacy policy that the user would receive but the idea with this would be to draft the privacy policy so as, yeah, with the idea that you're thinking of privacy already.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, you're already thinking about where you're going to get the consent, how you're going to get the consent and the development. So, even before you start to look at your architecture, you're thinking, 'Okay, I need to get consent for this. How are we going to get consent? What are we looking for consent for?' So, that's not quite clear, is it?
- Dr. KIM WUYTS: Yeah, yeah, I was, well, it's only just a sentence, of course. So, this was based on the table.
- CEARA TREACY: Okay. It was not clear that this is only the beginning.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: And will need to be updated until the product goes live.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: All right.
- Dr. KIM WUYTS: And probably even later on but yeah. That continuous cycle can be something to, to include.
- CEARA TREACY: And continued cycle, yeah, cycle through the produce lifecycle or data lifecycle, product, and data lifecycle, okay. Just excuse all the red, I'll correct later.
- Dr. KIM WUYTS: It's fine, it's your notes. So...
- CEARA TREACY: I'm sure I'll be able to, I hope, gosh-
- Dr. KIM WUYTS: And we have the recording, hopefully, as well, so...
- CEARA TREACY: -yes, yeah, yeah, yes. So, I'll go over and, right, so, okay, right, yeah, that's okay, next.
- Dr. KIM WUYTS: Yeah, it's just a typo. Yeah.
- CEARA TREACY: It's actually, you know, and I hate to be such a squealer, but I saw a thesis that was done specifically on LINDDUN and he had spelt it incorrectly the whole way through.
- Dr. KIM WUYTS: Yeah, well, we didn't really think it through when we, when we created this, we were like, yeah, two, 'Ns', two, 'Ds', that's fine but it's really confusing but, yeah. We're here now, and we're not going to change the acronym. So-
- CEARA TREACY: Absolutely not, and it worked very nicely for what I wanted to do to put it in with STRIDE. So-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -you know, that was good.
- Dr. KIM WUYTS: Yeah, so, so, I was wondering here, because it's about regulatory stuff, I, I don't have a lot of the GDPR kind of requirements specified in your document. So, I was thinking, like, does this relate to the data register and the processing activities that you need to document anyways for DPIA, and if so, shouldn't you make that data register more explicit

Appendix F

- maybe in your description, or is this the same, and I did not understand it correctly because, well, I'm not a GDPR expert but we have collaborated with, with legal, with the legal department. So, I know bits and pieces but if I remember correctly, you need this, like, yeah, data register where you have an overview of what data are being used in the system and, and what processing activities and purpose belongs to that, and those were things that I don't really got from your document that, that's, might be something require from a regulatory aspect.
- CEARA TREACY:
Dr. KIM WUYTS: Right.
Not necessarily that much impact from a threat modeling perspective but they can be useful input because if you have that data, if you have those processing activities, those might help you also create the DFD or, or part of the DFD. [0.10.01.7]
- CEARA TREACY:
Dr. KIM WUYTS: Right, okay.
Although the perspective is different because we have another research project where we actually focus on the legal part and less on the technical part but I'm not sure if you came across it. I will send you that link as well.
- CEARA TREACY:
Dr. KIM WUYTS: Okay, that's great. Well, now, this was my thinking on it, and I'm very happy to get, you know, whether this is the right thinking, I was, because of the way that the framework was working and then I had pulled in that you do data flow diagrams because that's part of the threat modeling process but also then, its per-interaction. So, for each per-interaction, you'll have a list of what the processes are in that per-interaction.
- Dr. KIM WUYTS:
CEARA TREACY: Hm-mmm.
And therefore, you'll know what kind of data is being used because you're going to threat assess. So, maybe I just need to make that clearer. Would that clear that up, do you think, Kim, or is that-
- Dr. KIM WUYTS:
CEARA TREACY: Yes, if that would make the lawyers happy, because maybe that's something you need to check with the data protection lawyer if, if that is sufficient or maybe your scope is different because LINDDUN does not really focus on the legal part but, because you say data protection impact assessment, that triggered bells for me, like, this is also the legal stuff.
- CEARA TREACY:
Dr. KIM WUYTS: Yes.
So, in any case, you would, well, I read this a week ago, so, maybe I already forgot but I don't think there's a lot about purpose specification and compatibility checks and those kind of things which is definitely not a threat modeling thing or not a typical threat modeling thing but something from a legal perspective you need to do and is equally important, I would say, that you make sure that you have all the purposes specified upfront for collection and that you only use, process those data items for that specific purpose and that you can, can prove that you did that compatibility assessment.
- CEARA TREACY:
Dr. KIM WUYTS: Right, okay.
But I, that's a different research project that we have been focusing on. So, it's not something that, well, you can probably make some shortcuts or, or refer to it, or say that you focus here primarily on the technical part, which is something we, we tend to do for LINDDUN because people say, 'Okay, we do privacy threat assessment'. So, compliance check which is not the case because you have all those legal organisational stuffs that you also need to think about.
- CEARA TREACY:
Dr. KIM WUYTS: Yeah, okay. That, no, no, you're right because then can I legally say, 'It's a DPIA', because of that?

Appendix F

- Dr. KIM WUYTS: Well, I don't know. So, I don't know if you have any access to, to legal experts within your organisation or, or for them to, to give their view, their perspective on this. I, I would say this is just part of it because you will still need that legal angle and those compatibility assessments and those, yeah, the legal stuff.
- CEARA TREACY: Hmm, when I started this, you see, I was working with the, the legal firm with the company, so that supports that I have put this in and they had very little understanding, you know. So, I don't know whether that's now just growing into a better understanding and there's more knowledge about what's required in a DPIA because there were no even templates on what a DPIA should contain.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, I just went to the regulation and saw what the GDPR said what a DPIA should contain.
- Dr. KIM WUYTS: Yeah, yeah, yeah, sure.
- CEARA TREACY: So, that's, you know, that's not in this. This is, that's in the thesis itself, you know. So, I'm basing it around that but if there's legal standing, I suppose, is what I'd call it, is not complete.
- Dr. KIM WUYTS: Yeah, by talking about data protection impact assessment, for me, that triggered, like, this will be a legal thing as well.
- CEARA TREACY: [0.15.01.1] Yeah, yeah, yeah. That was the whole idea, is that we can just, you can present this as your legal DPIA to say, 'Okay, these are the processes. This is the information, and this is how we completed the risk assessment against those'.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So then, compatibility assessments are going to be needed for that.
- Dr. KIM WUYTS: Yeah, and purpose specification and those kinds of things, yeah.
- CEARA TREACY: Yeah. So, I did see that actually in the questionnaire that, so, so, we're coming up to Table 7, 'not complete, purpose', let me just, sorry.
- Dr. KIM WUYTS: Yeah, sure, go ahead.
- CEARA TREACY: 'Purpose specification and compatibility'. I'm never going to make that out. I don't know what is wrong with this. No, this does not seem to be working at all. I'm going to have to just type really slowly.
- Dr. KIM WUYTS: Okay, yeah, sure.
- CEARA TREACY: Okay, so, this table here, 'Lawful processing', would this not cover some of that?
- Dr. KIM WUYTS: Yeah, probably it does, but it seemed like, let me go through-
- CEARA TREACY: It's not enough?
- Dr. KIM WUYTS: -which, page 12.
- CEARA TREACY: So, it's Table 7, 'Lawful processing'. So, it's, the requirements-
- Dr. KIM WUYTS: Yeah, yeah, you're right. I, kind of, missed that purpose part there, yeah, yeah, yeah. I saw, 'Lawful', and I saw, 'Consent', and I thought, 'Okay, this is focusing on the technical part and the consent stuff', but I missed the specific part, yeah, yeah.
- CEARA TREACY: So, maybe I need to clarify that's not the right-
- Dr. KIM WUYTS: Yeah, maybe I should read more carefully probably, yeah. I have the tendency to when I see tables, to kind of, go over them quickly. So-
- CEARA TREACY: Yeah, whereas this is actually quite an important part.
- Dr. KIM WUYTS: -yeah.
- CEARA TREACY: Yeah. So, maybe the table is the wrong way to do it.
- Dr. KIM WUYTS: It's just a personal thing. So, I've missed a lot of content in books and stuff by just quickly going over tables. I should have known better by now, but-
- CEARA TREACY: No, it's very hard to break habits. I know this.
- Dr. KIM WUYTS: Yeah, okay, that's a relief that I'm not the only one, okay, good.

Appendix F

- CEARA TREACY: So, maybe just clarify that this is related to purpose.
Dr. KIM WUYTS: Yeah, it's related to a lot of things, but it's definitely related to purpose and, and that legal stuff I talked about before.
- CEARA TREACY: And assessment, okay. That's probably a sentence saying, you know, about those requirements in the GDPR and this is what this part is covering, yeah, okay.
- Dr. KIM WUYTS: Yeah, it's, so, I'm, kind of, nit-picking, but, yeah, to me, it felt like this is an overview of GDPR articles and some additional information, and I think it's the middle column that you want people to actually do, and think about?
- CEARA TREACY: Yes.
Dr. KIM WUYTS: So, maybe you can highlight it more or, or put that to the left and say, 'By the way, this comes from GDPR', or I'm just thinking out loud but now that, like, 'This is the stuff you need to do', did not really come to me, at least not visually.
- CEARA TREACY: Right.
Dr. KIM WUYTS: So, I decided to skip but...
CEARA TREACY: So, it's really, I need to rework this as it is a really important part.
Dr. KIM WUYTS: Well, yeah, at least your one reviewer, kind of, missed it but maybe that's just me.
- CEARA TREACY: No, well, the, well, you're the only, there's only a couple of reviewers that are, because it's been based as action research, it's based within the company. [0.20.03.6] So, I'm just getting external validators because I don't want to make it any bigger. It's already ginormous.
- Dr. KIM WUYTS: Yeah.
CEARA TREACY: So, like, this is all valuable, you know, where, and this is your domain, and you're doing research in this area now. So, like, the fact that you were confused about it, obviously, it needs complete clarification that this is an important part and needs-
- Dr. KIM WUYTS: I think that's a great approach to ask people from the field to give feedback. That's something we, at least, me and my close colleagues don't do often and that's a shame because I, well, I think you get some, some inputs that you would not think of yourself, and you might not get from a review from a conference because you need to be lucky for that conference to have somebody who's really familiar with the field.
- CEARA TREACY: Yes, yeah.
Dr. KIM WUYTS: Not over exaggerating my input, but I'm thinking of getting the same for our research that would be great. I will definitely give you as an example in our next group meeting that this is something we should look into.
- CEARA TREACY: To do, well, that's something that Professor McCaffery has just really pushed and I, even though this is action research and I'm so embedded in the company, he was very insistent that we look outside to make sure-
- Dr. KIM WUYTS: Yeah.
CEARA TREACY: -because we're all too close to what we're doing, and you know, and then, it was just purely, you know, he said, 'Well, who ideally would you like to get?' and I was, like, 'Well, it would be wonderful to get Kim Wuyts? You know, she developed the whole LINDDUN thing. So, she would have a complete understanding of this, and she's been involved in STRIDE', and then Danny Dillon was one of the other external validators but he hasn't been, he's been really busy. So, and it's, like, that's the thing, like, it's really difficult, I really appreciate that you-
- Dr. KIM WUYTS: Yeah.

Appendix F

- CEARA TREACY: -have taken the time because I understand it's hectic.
Dr. KIM WUYTS: Yeah, yeah, but the way around, if we would hand out such questionnaire to other people, we also want them to take the time. So, I think it, kind of, goes both ways but I think you made some advertisements for me because this morning I got another mail from a colleague of you asking the same thing. So-
- CEARA TREACY: Oh, really?
Dr. KIM WUYTS: -yeah.
CEARA TREACY: Pangkaj
Dr. KIM WUYTS: Yeah.
CEARA TREACY: Oh, my goodness, that's funny because Pangkaj started in the company after me.
- Dr. KIM WUYTS: But, yeah, I also, well, it sounds interesting, but it will depend on when, when he needs his feedback to see if I can squeeze it in.
- CEARA TREACY: Yeah, yeah. No, his is, now, much more technical because he is a developer. So, he's taken it from the perspective from one product and, yeah, so, it might be interesting in that sense because he's taken, not from where I've looked for controls from the standards so as you can say that you've complied with the standards. He's looked from a developer's perspective in the sense of, you know, what OWASP would say you would do and stuff like that, yeah.
- Dr. KIM WUYTS: Yeah.
CEARA TREACY: So, it's very different. Yeah, so, it's important that these questions are filled out really.
- Dr. KIM WUYTS: Yeah.
CEARA TREACY: And that it's thought about because this will affect the full development and privacy and the privacy policy. Yeah, so, maybe that's the way I take it from, okay. Next is?
- Dr. KIM WUYTS: Yeah, so, this is biased by my research background, I think. I can send you over the paper after this, but basically we created, with we, I mainly mean my colleagues, I was, was not that closely involved there but something similar like a DFD but actually the entire way around where you also specify data controller, data subject, processor, purposes, where you can have that compatibility check and the idea there is that you can have that model and link it with a threat model and then you can have, like, the joint legal and technical thing combined. [0.25.04.3] So, based on that, I would say that a DFD will not contain sufficient information to have that legal part but that's what is in your step one. So, I don't think that's an issue. I, kind of, missed that it was in step one. So...
- CEARA TREACY: Ahh, yeah, but I think that what you're saying is valid because step one will give an overview of what it is, the purposes for gathering the information and everything but through the per-interaction processes, what I think it is, is that the privacy and GDPR requirements will have to be considered in each of those processes to make sure that you're complying with what you said you're going to do and that you're not, so, that possibly is a gap. Hmm, right.
- Dr. KIM WUYTS: I will send you the paper and I think my colleague, Laurence, also gave a talk that was recorded about that whole thing. So, have a look and see if, if, if you find any gaps in what you have done but, well, now that you explained the step one, this is less relevant, I think, but I was still reading it here and thinking, 'Okay, but you want to do that full legal stuff and you only look at the DFD, so, you will probably know all the information you need to do that properly'.
- CEARA TREACY: And, yeah, okay, so, and Table 7 and potential to tie all in together,

Appendix F

- continually maybe referencing back to Table 7. I'm just thinking out now. So, if you're going through your, your, like, one per-interaction and you're looking at that process, you could continually refer back to this is the part, this is in reference to part-
- Dr. KIM WUYTS: With this, with this purpose and this data.
- CEARA TREACY: -yeah, yeah. So, that could be, yeah, okay. Okay, so, it's 18.41. I'm just putting down the times in the recording so as I can-
- Dr. KIM WUYTS: Okay, yeah.
- CEARA TREACY: -reference back to it because, do you know, sometimes, you get lost. All right, already known decisions or constraints.
- Dr. KIM WUYTS: Yeah, well, again, I did not put enough effort probably into this, but this was a bit of a confusing table. So, this was more like a note for me to ask you for more information on how to see this than...
- CEARA TREACY: Okay, because it's an SME, they're probably already tied in, from the literature, what I've found is that generally, organisations are tied into different platforms and different, you know, development and programming languages and stuff simply because that's the, the talent they have in their development team. So, that directly influences how you're going to do your development for your product. So, for example, stat supports were already tied into Azure. So, there's lots of security aspects to Azure that you can already include into where they've said they've acquired, you know, this is for privacy, and this is for security. So, and then, already libraries, so, there'll be definite libraries that the organisation tend towards because they will have other products that will have used those libraries. So, rather than reinventing the wheel, I thought, you know, a lot of SMEs will already have known decisions or constraints around their development project. So, if they had those already put into document, and they then could reference back to what they'd done previously, then they would, it would just make it a less of, you know, because personally, what I find is developers tend to do an awful lot of running around trying to find things they've done previously, and they've done before.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, like, I'd be in a meeting, and I said, 'Well, where is that?' and they're like, 'Oh, well, it's, eh, eh', and it'd take, you know, five or 10 minutes to actually find where it is. So, I just thought we're trying to get everything for the one project into one place and this would be a good place to put that. [0.30.00.1]
- Dr. KIM WUYTS: Yeah, okay, yeah. It's a bit related to what we call assumptions, I think, then, yeah.
- CEARA TREACY: Right.
- Dr. KIM WUYTS: Yeah, and well, it's already maybe sometimes also solutions that are already in place and that can influence the outcome, okay. Yeah, that makes sense.
- CEARA TREACY: Obviously it doesn't make sense because you didn't get it.
- Dr. KIM WUYTS: Yeah, yeah, yeah, but I, I, I was thinking, like, how does this all tie them back together? What will you do with it? Will it, will it really also be, well, it will be input but will it be additional, will it have additional support because, for instance, I saw that Azure mention, and I was thinking, so, are you now saying, like, 'We know this stuff about Azure, about security guarantees but also about security and privacy issues.' So, now, automatically, all this ties, well, falls into your threat model. That's also something very interesting but probably out of scope here.
- CEARA TREACY: Yes, yeah, it is, that's, like, eventually where I would be going because then, you know, the whole idea with all of the standards are, you build

Appendix F

- up this knowledge.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: But a lot of organisations don't know how to do that because, firstly, they don't know about the standards and what they suggest and secondly, it's like going, 'Well, how the heck do you do that?' So, you know, from this is the thinking that, well, for the organisation, what I have done is they now have a list of all the libraries that they've used. Like, I've organised their development team in that sense where, you know, they've listed what security they've done in different things, you know, what privacy they've, how they approached it and, you know, authentication in this product. So, it's easier for them to go back and look. So, but it is out of scope. There are loads of things I'd love to do but, you know, the scope of the-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -PhD is just already-
- Dr. KIM WUYTS: No, it's true.
- CEARA TREACY: -it's too big, you know.
- Dr. KIM WUYTS: We have this big list of all the, that would be great topics within our group and then, yeah. Some will get picked and the others are like, hopefully some day in the future.
- CEARA TREACY: Yeah, yeah. So, this is one of those things. It was more from an organisational perspective for the organisation because I know a lot of them, and I know because it's, the company I worked in, that they have done this before. It's just they don't remember or it's not there.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: And it just, rather than having all of that run around, run around, you just keep it in one spot.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: That makes so much sense. We have that discussion with some people from industry too that they say, 'Well, documenting this would be such an overhead', and then, but 'But you can reuse it', 'Yeah, but no, we don't need to, we know it, it's in our head, that's enough', and yeah.
- CEARA TREACY: And you're like, my analogy is, 'So, what happens when you get hit by a bus?'
- Dr. KIM WUYTS: Yeah, yeah, people move all the time and then the experts leave, and you're left with nothing and, yeah.
- CEARA TREACY: Yeah, so, that was part of it because that's exactly where I was coming from. You have an SME where, you know, they get the experience, they get the knowledge under the belt, and then they move onto a job that can pay more with a bigger company. They mightn't necessarily be happier but, you know, and then they take all of their expertise with them whereas if this was all here before they left, then that's, and it's, it's great as well for new developers who are coming into the organisation.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, they can look at how, you can just hand them the DPIA for the, the previous product and say, 'Have a look at this. This is, you know, a good idea and background on how we develop all of our products', you know, because what I've done is tried to tie this into the SOP for software development within the organisation as well for their ISO 27001 Certification. So, it's all trying to, it's trying to do too much maybe. That's maybe it, I don't know.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: It's, yeah, so, yeah, keep all the information together, and, yeah, and

Appendix F

- you're right anyway, Kim, because if the developers don't understand the purpose of it, then they won't do it.
- Dr. KIM WUYTS: No.
- CEARA TREACY: So, if they see this and they were like, 'Oh my God, she's just dragging us through this again', whereas if it's not fully clear, 'So, this is why you would do this', then they're not going to bother, are they really?
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Yeah. Right, okay. [0.35.00.7] Security vs privacy-
- Dr. KIM WUYTS: Yeah, so, so, when I talk about security and privacy, I always say, like, it's, you can do threat modeling for both and it's very much the same, but it requires a different mind-set. So, for security, you need the valuable assets for the organisation and for privacy, you need to think of the perspective of the individual, the data subject and it's just one sentence but it's, kind of, like, something I keep focusing on in a lot of things, in talks and so on. So, it just came to mind, and I decided to write it down anyway.
- CEARA TREACY: Yeah, no, it's very valid, think about the data subject, and do you think it is like trying to get the developers to think of the data subject as a valuable asset to the organisation as well?
- Dr. KIM WUYTS: Well, I'm, I'm, I don't know if the data subject is the asset, but you need to think of it from the perspective of the data subject while for security you think about assets from the company side. You are trying to protect, like, all data is valuable because, well, we need it for the company but from, for privacy, it might be different data that is really valuable to the data subject, not that valuable to the company but requires a lot of privacy attention because it's so valuable to the data subject.
- CEARA TREACY: Right, okay, yeah, so, what I would've done is, they would have a security champion and one of the developers would take on the role as a security champion. Maybe you're thinking of, like, a privacy champion as well in the development team so they're always looking at it from a privacy perspective.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: Hmm, it's just changing your, your head basically, like, 'Now, I'm thinking from the company perspective', and 'Now, I'm thinking more like if I was a data subject, would I be okay with all these things happening?'
- CEARA TREACY: Yeah, okay, very good, yeah, that's good. Additionally, because assets generally interact with other assets, they can act as an entry point for an attacker. Assets don't act, that's true. It's the-
- Dr. KIM WUYTS: Yeah, so, I think you were saying something related, but this just didn't feel right.
- CEARA TREACY: Yeah, yeah, no, it's, yeah.
- Dr. KIM WUYTS: So, yeah, I mentioned before sometimes the comments are really minor and nit-picky but...
- CEARA TREACY: Oh no, but, like, they're valid, you know, assets don't act. It's the attacker on the asset, that's what it is. Okay, next.
- Dr. KIM WUYTS: Yeah, I think it should be, 'Data from an external entity cannot move directly to another external entity, and you need a process in between'.
- CEARA TREACY: Oh right. Right.
- Dr. KIM WUYTS: But again, I heard other people say, like, 'For DFD, we will not impose any semantic rules. We just let them write it because maybe you get additional information if you have those communications outside of the, the scope like from external entity to other external entity. If it

Appendix F

- helps you think of stuff about assumptions, then it's all fine'. So, again, it depends on how you want to do that but...
- CEARA TREACY: Yeah, it depends, yeah, on how, yeah, yeah, the semantic rules, yeah. 'Per-interaction approach is less time consuming and exhaustive as it involves less components', oh, okay.
- Dr. KIM WUYTS: Yeah, so-
- CEARA TREACY: That's controversial because there's three people that say otherwise.
- Dr. KIM WUYTS: Sorry?
- CEARA TREACY: The three guys, these are the guys that do this.
- Dr. KIM WUYTS: But Laurens Sion is my, is my colleague, right. So-
- CEARA TREACY: Oh right.
- Dr. KIM WUYTS: -I was like, 'Did you really write this?' and he said, 'Why?' and definitely, I wrote it down more than once because, well, I was triggered by the last part of this, it doesn't involve less components. You still look at the same stuff. [0.40.03.6]
- CEARA TREACY: Right, right.
- Dr. KIM WUYTS: So, so, **it might be more intuitive** or, I don't know, yeah, I didn't check Adam's quote there but so, yeah, I know Laurens is always writing down super nuance stuff and I was thinking, like, he never, I don't think he wrote that stuff but, so, just giving it as a, as a, well, I will probably be the only one who is triggered by this but-
- CEARA TREACY: No, probably not. So, yeah, so, this is not correct.
- Dr. KIM WUYTS: Well, **there are advantages definitely of per-interaction because it's, it's more intuitive, definitely, but I'm not sure whether it will be less time consuming and exhaustive.** I should have looked this up earlier but-
- CEARA TREACY: No, no, no, no, because look, that might be the way that I determined it was because it fitted my, my wanting, you know.
- Dr. KIM WUYTS: Yeah, I, yeah.
- CEARA TREACY: Yeah. So, no, I'll look at this again and, yeah, that's fine.
- Dr. KIM WUYTS: Yeah. I always have Adam's book nearby because I often, I often look at it but I don't know it by heart yet.
- CEARA TREACY: Yeah, no, I have it here too actually, yeah, yeah. I met him at the OWASP 2017 and if only I knew that I was going in this direction, I would've, like, just stayed what I would like it to have said.
- Dr. KIM WUYTS: Yeah, yeah, yeah.
- CEARA TREACY: You know, it's just, oh well, what can you do? 'While the framework recommends that threat elicitation per', oh yeah, you're right, ah, nobody picked that up. That's dreadful.
- Dr. KIM WUYTS: Yeah, so, I, well, **I see why you would combine it because it's the same thing but on the other hand, it's like the complete opposite. So, I was just wondering, like, why did you combine them and not have non-repudiation as a, as a different item?**
- CEARA TREACY: Well, because I was trying to make it more compact and simple but since then, I've had a paper rejected which one of the commenters said exactly the same thing.
- Dr. KIM WUYTS: Yeah, because **from a security perspective, you need it. From a privacy perspective, you don't want it or might not want it.**
- CEARA TREACY: Yeah, so, yeah, no, I think they're going to have to be separated out and changed in, in the whole framework now because having looked at it, I'm trying to think on how, it's like putting on that security head and then translating, and then putting on your privacy. So, it's the idea that you look at it from the two perspectives.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: But I don't think that'll work because people will just take it from one or the other because the way, I joined them together is because you need

Appendix F

- to consider both because security and privacy aren't individual.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: And particularly in this one type of threat, you know, like you said, you know, for security, you want it but for privacy, you don't really want it. So, it's, you need to consider at that point which is the most important thing and what are you trying to do-
- Dr. KIM WUYTS: Yeah, but I actually never came across a situation so far that there is actually a conflict because even in online voting when you want possible deniability about who you voted for.
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: That is completely fine with having non-repudiation about the fact that you voted. So, it's actually in the same that you have both, but they don't conflict because they are at different, what is it, different data items, different types of information or flows or, or properties. [0.45.01.0]
- CEARA TREACY: Yeah, yeah.
- Dr. KIM WUYTS: It might be the case that they conflict but then, yeah.
- CEARA TREACY: Yeah. So, that's probably a lot more to do with my inexperience in implementing both, that I thought it would be easier or that they would conflict more-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -but they don't.
- Dr. KIM WUYTS: I don't think so, and if they do, then probably, you need to revise the entire focus of the project because I think if you need both, something with strong repudiation and strong non-repudiation features for the same property, then, well, yeah, that's not really going to happen probably, but then again, I, always interested to see if, if there are situations where it is a problem and how that would be fixed. So, if you would come across one, definitely, let me know.
- CEARA TREACY: I'll definitely, yeah, pass it onto you. No, but that's okay because funny, I did have a paper just on that and one of the comments, or commentators were like, you know, 'These are two different things, you know. They don't generally conflict. Why would you have them at consideration at the same time?' So, that's a fair point.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Okay, insecure communication.
- Dr. KIM WUYTS: Yeah, I have the same comment down with the text as well. I'm not sure why you need it as a different thing. Isn't it part of information disclosure because if you look at per-interaction, you have sender, receiver and the flow? So, isn't it about the flow of that interaction that is as information disclosure if that's or...?
- CEARA TREACY: Yeah, hmm.
- Dr. KIM WUYTS: Or is it such an important thing in this scenario that you really want to highlight it?
- CEARA TREACY: I think it's, yeah, because, what I'm thinking of is that, from the whole perspective of, you know, all, I know we're talking about per-interaction and process and threat modeling and that but when you're looking at the whole framework in the sense that insecure communication is such a big part of your flow of your data that I don't think that information disclosure, disclosure of information just fully covers all of, you know, the insecure communications in that.
- Dr. KIM WUYTS: Yeah, just was my, my hunch, why, you probably can, can, it's, to me it's all in information disclosure but if, if you find missing stuff or if you want to highlight it maybe...
- CEARA TREACY: Okay.

Appendix F

Dr. KIM WUYTS: I'm all good.
CEARA TREACY: And what makes it different.
Dr. KIM WUYTS: I'm sure also if, if you want to discuss that more in detail, Adam Shostack would be interested to give you feedback there as well.
CEARA TREACY: Oh right, okay. Yeah, I didn't send this to Adam. I thought he'd be too busy to even look at it, but I might just drop him a line.
Dr. KIM WUYTS: Yeah, I don't know. I guess he's quite busy but-
CEARA TREACY: He's always very interested in stuff going on in this domain anyway, isn't he?
Dr. KIM WUYTS: Yeah. So, if you have specific questions, I'm sure he's happy to answer those if it's about reviewing this stuff, I don't know.
CEARA TREACY: Yeah, well, that's probably a good one to, this specific one, and whether he deems that it's necessary to separate them out or, you know, whether-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -hmm, and property, yeah, okay. Right, that's the same thing.
Dr. KIM WUYTS: Yeah, that's the same thing.
CEARA TREACY: Okay, oh yeah, the threat to attack type starter kit library. This came about because I was running a workshop in a EuroSPI Conference and we got to this point in the framework and nobody had a clue where, what all of the different attacks-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -and everything were. So, it took forever and I, you know, I was sickened that I did it but, you know, I think it's useful for the framework. It's not, like, that's a whole PhD in itself, that whole piece of work but I just thought it was useful to put it in there as background for SME who have never-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -nobody has any idea. [0.50.08.3]
Dr. KIM WUYTS: Yeah, I think the strength in this kind of approach, especially for people new to it, is all that background information because, well, you can say now, 'Think about it systematically if you don't know what to think about', and you're lost.
CEARA TREACY: Yeah so, that's why it was put in there. To me, it's really untidy and, because I didn't spend an awful, like, I spent an awful lot of time in the literature review and getting all the different types of attacks and, you know, and getting the links into the CWE and OWASP as well but, to me, it's really untidy in the sense that it could be much smoother to run around, if you know what I mean, because, but it is what it is and it's not the main focus of the research. I just thought it'd be nice. In fact, the paper that got rejected was on this particular thing because I haven't had this part validated and I thought I'll write a paper and that'll be validation for it, but they refused it and one of the points was what we discussed earlier was about the non-repudiation, repudiation-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -cause and deniability, and they were, like, 'you've got to separate those out. They're not the same thing at all'. So, maybe I'll just now, with that, I'll just submit it again, but I don't think it's going to be a big, it's not like a massive, it is a big part of work, big money work but it's not a massive part of the framework. It's just useful.
Dr. KIM WUYTS: Yeah, well, and part of the programme committee of IWPE and the deadline is mid-May. So, if you're still looking for a workshop paper submission, then we would be happy to have.
CEARA TREACY: Okay. So, the conference is the...?
Dr. KIM WUYTS: Well, it's a workshop. It's part of EuroSPI and it's IWPE, the

Appendix F

- International Workshop on Privacy Engineering, and I think this actually really fits within the scope and we're always looking for, for, like, this useful stuff to be, to be applied
- CEARA TREACY: And when is the closing date again?
- Dr. KIM WUYTS: Sorry?
- CEARA TREACY: When is the closing date?
- Dr. KIM WUYTS: It should be end of this month, but it will be, I think, it's already extended, I think it will be May, let me see, is it already there, May 15.
- CEARA TREACY: Okay, okay, if I get time, I'll throw a proposal in, yeah, no, that'd be great to work, to do a workshop around that, yeah. Great, 'should this be used as input for the analysis (i.e., iterate) or is this only background information?' Yeah, it...
- Dr. KIM WUYTS: So, you know, I was thinking, like, will it be like the STRIDE and the LINDDUN trees or is it just like you read this and then you are, you have more expertise, and you can then manage it yourself? I wasn't sure based on, on...
- CEARA TREACY: Well, because, you know, that huge set of standards, God, I can't think of the name. It's for app development and it says, it very, just throws it out there saying, 'You should have a threat library and a tech library', but it doesn't tell you anything on how to do that at all but my idea behind this was the, that the company would then be able as they, like you said, become more experienced, they will have this library of-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -threats. So, they can start with what I've put there but as threats are introduced in, and they get to know about different threats and they're in that domain, they can add it to the library under whatever threat heading that they want to put it in. It wasn't anything more than that. I don't know whether it is. Okay, so, that's that.
- Dr. KIM WUYTS: Yeah, yeah.
- CEARA TREACY: Right, great. Let me just-
- Dr. KIM WUYTS: Yeah, I didn't go really thoroughly through the appendices. So, I only briefly skimmed through them. So, there are no comments there.
- CEARA TREACY: Okay. No, there's one of the appendices already has been changed because I just put the, the properties, threats and a description of the threats whereas then people wanted a description of the properties as well. So, I put them down the centre. So, I put properties and threats and then a description of both and examples on either side. So, they've already been changed a little bit. That's great. Thanks. We've 20 minutes left now. [0.55.00.5] So, I've just added some questions that, from your answers here. So, we can run through these quickly and anymore that I don't get asked within, before 10.30, would you mind if I just sent them to you-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -like, just, and then you can just maybe provide some, so, that's just, yeah, okay. So, I'll just share my screen again.
- Dr. KIM WUYTS: Oh yeah, that's easier, yeah.
- CEARA TREACY: Yeah, and there we go. Is that okay?
- Dr. KIM WUYTS: Yes.
- CEARA TREACY: Okay, so, the top bit is just getting your expertise down. So, it's Review Questionnaire, 'Please provide a short rationale, typically there is either focus on security or privacy', and, so, in your opinion, what is preventing the combined approach? Like, similar to, because there's nobody, the reason I've done this is because I haven't found anybody doing it.
- Dr. KIM WUYTS: Yeah. No, well, so, I, I think currently privacy is more being done in

companies because they have to from a legal perspective. So, it's more managed by the legal people and then somehow push those requirements to the developers and so, for security, it's, it's coming from development more. And then again, that mindset. So, you want all that data from a company perspective, and, and I have the feeling that a lot of companies are not ready to, to say, like, 'Well, maybe we don't need that data unnecessarily and it's okay'. They're still doing compliance and not doing privacy because, well, they want to do the bare minimum to not get fined and not do privacy because that's something they should be doing.

CEARA TREACY: Yeah.

Dr. KIM WUYTS: Yeah.

CEARA TREACY: No, I completely agree with that actually, but it's taken a long time for security, and it still is, you know, when I went into the company I'm in and I, and this is quite typical of most SMEs, they had never considered security at all, and it was just because of the fines coming from the GDPR if they had a breach that they, that panicked them. So, like, my belief that it is being driven by regulatory requirements. However, if you talk to Adam or, you know, I'm sure the other guys are, like, going, 'No, no, security should be there and it's been, you know, pushed, they push it out'.

Dr. KIM WUYTS: Yeah, but if I talk to security people, then they, kind of, say the same thing I'm saying about privacy. They say, like, 'Well, management is not really that interested in security. It's because they don't want to get fined', and, but really, like, having a thorough security programme in place, that's, for some companies, still something that is far from, from what's going to happen, yeah.

CEARA TREACY: And it is an additional, an additional expense, you know, like. I've seen, for, you know, stat supports, the additional expense even just to have your product pen tested at the end.

Dr. KIM WUYTS: Yeah.

CEARA TREACY: You know; a lot of companies don't do that. So, they take the massive risk, you know, and pen testing as well still looks specifically at security. So, I've always had to request that they look at the privacy aspect of it too to make sure that, you know, and to be honest, there's very little knowledge within the pen testing community and the companies as well on what they should be pen testing for in privacy.

Dr. KIM WUYTS: Yeah.

CEARA TREACY: So, that's a whole other area that needs to be looked at.

Dr. KIM WUYTS: Is there, because I've never looked into that but is there some research or are there any sources there?

CEARA TREACY: I haven't looked into it either. I'm just, like, thinking-

Dr. KIM WUYTS: Yeah.

CEARA TREACY: -you know, just, this is my experience from talking to the pen testing companies. So, to me, I think that's a whole area that is totally untapped. So, if you want to start a company on pen testing for privacy, I think you're in a pretty good position, you know. So, and then, this, this adds to the second one, 'Is it changing and do regulations play a role in this?' Yeah, so, I think we both agree that it is the idea that you're going to be fined that has brought it to the forefront, yeah.

Dr. KIM WUYTS: Yeah, that and, I think, reputation damage as well, like. If you see that, that shift from what's up to signal because they, they announce some changes in their, in their data policy stuff.

CEARA TREACY: Yeah.

Dr. KIM WUYTS: Yeah, I think that the public opinion and possible reputation damage is

Appendix F

- also something that is being a driver sometimes. [1.00.05.1] It's still not the right motivation but it's already better than just, 'Let's do the bare minimum and get it done', yeah.
- CEARA TREACY: Yeah, and I suppose, like, until the big companies, like, Facebook, -
- Dr. KIM WUYTS: Yeah ever.
- CEARA TREACY: -I just, I haven't closed my account yet. I have to have full disclosure, but I never post anything, and I removed my pictures although it's late.
- Dr. KIM WUYTS: I have an account and I; I do not often post things but it's like the platform to communicate with other Mums and with school and so, yeah.
- CEARA TREACY: Yeah, it's very difficult, isn't it, not to be a part of it?
- Dr. KIM WUYTS: It's, kind of, my newsfeed for the local stuff going on here. So, yeah.
- CEARA TREACY: Yeah, so, it is all about function but I suppose that's because we know and that's our choice, but it is, like you say, it's all about, you know, the public are only starting to really understand and that whole Cambridge analytical thing really blew the lid off it, you know, and US elections. So, that was all very interesting. 'Is there a need for a distinct approach in the guidance and standards?' So-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -I'm just thinking because I'm in the regulation domain. So, do you think that if there was a standard that looked at the approach and the impact to both security and privacy, would that help?
- Dr. KIM WUYTS: Hmm.
- CEARA TREACY: No?
- Dr. KIM WUYTS: Probably, but I'm not that familiar with standards and applying them. So, I'm probably not the right person to ask-
- CEARA TREACY: Okay.
- Dr. KIM WUYTS: -because I'm sure you have more experience with those things. I only briefly glanced at some of the standards but, yeah, I think companies use the standard as, kind of, a compliance thing as well, like. 'See, we have, we follow these standards, so, we're fine'. So, if, if standards combine, then I guess, companies will have to follow or will be more likely to follow because, well, it's in the standards, so it must be true.
- CEARA TREACY: Right, yeah. So, it's that correlation between the standards and the regulations that's there. Yeah, because, like, if you're developing medical device software, you have to follow 62304 process, software process lifecycle because it's part of the, you know, to show that you're complying with the regulations, yeah, okay.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, specifically for developers, now, what I put in here is, like, is it worth just looking specifically at developers rather than at an organisational level because I know that a lot of people say that this, this is, you know, comes from the top down and, like, a lot of security personnel as well would say, or security developers are saying that, you know, unless they get the company behind them, you know, security isn't part of the development process or it doesn't get the budget or whatever, you know, whereas I'm thinking, you know, if we looked to moving the standards towards developers, would that take it more into their hands rather than the organisation's? I'm just thinking, you know.
- Dr. KIM WUYTS: Yeah, I've heard from people saying, 'Well, management says we need to do this', or developers saying, 'We want to do this but we need to convince management'. So, it goes both ways. I think you need to find motivated people and, like you say, the privacy and the security champions but, yes, I, well, if you can make it more practical for developers to, first of all, understand because I think it's also an

Appendix F

- awareness problem and then-
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: -give practical advice on how to do that. That would make, well, if you're a developer and you need to do ISO-whatever, then, but if you understand why and you get some practical advice, I think that would be-
- CEARA TREACY: Better.
- Dr. KIM WUYTS: -better, yeah.
- CEARA TREACY: Hmm, yeah, and that, I asked that question because I know we're stuck for time, okay. Can we discuss how the current doc is too complex and then could be less complex from your reading? Now-
- Dr. KIM WUYTS: Yeah, so-
- CEARA TREACY: -this is I speak in a, you know, I write like I speak, and I speak too technical sometimes in the sense from regulatory requirements
- Dr. KIM WUYTS: I think it's a typical academic issue. I mean, we have been struggling with that comment for 10 years for LINDDUN because when we first created it, it was an academic work and now people want to use it and there's, kind of, a difference. So, I think the quick fix would be to have more, how is it called, like a one or two-page-summary for, like, general public. Like, you have the quick guide on, 'This is the framework, these are the six steps', and from a high-level perspective, 'this is what they are, and this is why you should do that'.
- CEARA TREACY: Okay.
- Dr. KIM WUYTS: And then you link to the more extensive things because you say it's for, for small companies and for people getting into it. If you drop them a document of 130 pages, they would be lost completely. So, I think you would, like, gradually need to get them into, into, like, 'These are the main steps', and then, 'Here is more information', and then you have your appendices for more information on those. I'm guessing that having that one abstraction there will already help to soften the blow, 'Like, okay, this is something we can do', and then we go into the details.
- CEARA TREACY: Okay, so, maybe even break the document down into different steps. So, you would have the overview document and then just like a chapter of the book maybe?
- Dr. KIM WUYTS: Yeah, maybe, and well, I, it was somewhere in my comments, I think as well, when I read through it, sometimes it felt like this is an instruction to do, and then you have a lot of information like, 'This is why I think you should do it', and references to academic work, and I think from an academic perspective that's useful. From a practical perspective, that's mostly just a footnote or I'm not that interested. So, maybe you can, like, distil a manual really from it without having all that overhead of, 'And this is why, and I'm sure because those five people also say it', and, but that's, that's, I mean that's detail. The content is there. I think it's, like, making it more polished as an instruction or as a manual, and whether that's that one or two-page-summary or whether that's really a manual on how to do that.
- CEARA TREACY: Right, okay, yeah. So, it's just too mixed up. Yeah.
- Dr. KIM WUYTS: But, I mean, it's a challenge because this is your PhD. So, it should be in there but for people to use it in a company, then they might need different focus or different, or only a subset.
- CEARA TREACY: Yeah, I suppose, what you could do is just put all of the information on why you should do it into maybe an appendix for that section?
- Dr. KIM WUYTS: Yeah, yeah.
- CEARA TREACY: Yeah, maybe.

Appendix F

- Dr. KIM WUYTS: Yeah, I don't know how, your PhD text or something should look like but for me, this reads like a paper or a PhD text. So, you could also do it a way around and have, like, a technical report which is the manual for -
- CEARA TREACY: Manual for the developers?
- Dr. KIM WUYTS: -easier to use, yeah.
- CEARA TREACY: Okay.
- Dr. KIM WUYTS: But yeah. That's a bit biased because that's, kind of, what I did for LINDDUN. I'm not saying that that's the way to go but I see people, well, I wrote my PhD five years ago and I basically introduced version two of LINDDUN based on empirical studies and, yeah, it was academic and then I had this manual for how to use LINDDUN version two, and I see people referring to it. It's really not a great manual. So, there's a lot of things to learn from how I did it but that's something that people more refer to than the actual PhD because they, they are more comfortable with that stuff.
- CEARA TREACY: Yeah, yeah, yeah, and it's easier, plus maybe that's because it's like the target audience as well. You're looking at people who want to move into actually implementing privacy into. So, it's easier to use the manual then, yeah, yeah.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Yeah, well, I went back and read the whole PhD.
- Dr. KIM WUYTS: Yay, somebody read it.
- CEARA TREACY: Your PhD didn't sit on a shelf unread, yeah, because I found it very interesting how you went back and the Pfisman, all of their privacy because I was going to Canada and I'm dreadful with names, I can't remember names, and the woman in Canada who was developing the whole privacy-
- Dr. KIM WUYTS: Ann Cavoukian [1.10.16.1]
- CEARA TREACY: Pardon?
- Dr. KIM WUYTS: Ann Cavoukian
- CEARA TREACY: Yes. So, yeah, so, it was, it was great to go back to where you picked up or developed or gathered all of the language around privacy terminology and stuff even. It just made so much sense, you know.
- Dr. KIM WUYTS: So awesome to hear.
- CEARA TREACY: Yeah, but, you know, like, I had to go back, and I had to read what you'd done in order to understand where-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -it was coming from, you know. So, it was great. Too complex and less complex, that's done. Okay, the controls could be less overwhelming. Now-
- Dr. KIM WUYTS: It's the Excel sheet, right?
- CEARA TREACY: -yes. So, I put them in the Excel sheet and what I did was then categorised them. So, I actually, when I first did this way back before the most recent version of NIST SP 800-53 revision five came out, I spent hours and bloody hours with a security developer and my colleagues in the RSRC trying to distinguish what were organisational and what were technical controls, and we had done that but then revision five came out and they had decided to do that. So, it, sort of, confirmed to me that there was a need to start separating what were organisational controls and what were actual technical controls but then that meant that all of the controls that I had developed were obsolete because they were just an opinion from me and not of the wider NIST community-
- Dr. KIM WUYTS: Yeah.

Appendix F

- CEARA TREACY: -that developed 800-53, R5, but what it did do was made it much easier for me to actually then extract the controls because all I did was use the security and privacy property definitions and I literally put that into the standards and then extracted the controls that were related, and they were just technical controls. They weren't organisational. So, it made that part easier.
- Dr. KIM WUYTS: Okay, yeah, I, again, only looked at it briefly but it's on my to-do list to dig into it more thoroughly because, well, we really want to update our mitigation solution and so on as well. So, this might be a great inspiration for us to do so. Yeah, no, so, I'm, I don't think you necessarily need to do a lot of things about that categorisation and, and, as such because it's a great overview but maybe that's also going back to the manual. I have to go back, its step six, no, yes.
- CEARA TREACY: Yes.
- Dr. KIM WUYTS: Yeah, so, you just say, like, 'Well, we looked at these standards and we have extracted all this stuff', and the process is one or two sentences, maybe you can just give some more information there, like, an example or, like, 'If I have this, then where should I go? How should I tackle this giant beast of a document to look for those things that are useful for me?'
- CEARA TREACY: Okay, yeah, no, that's, yeah, yeah, that would make it much easier, just one simple example, like, 'This is a threat, this is the attack, this is the security property it violates'.
- Dr. KIM WUYTS: Yeah, yeah, and how to-
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: -yeah, and probably you can have a lot of future work on how to make the, the table more useful and add more [inaudible] information and, I don't know. You can have a lot of stuff you can do probably but, but I think just showing, like, 'This is how you use it', because now it's just a big list, kind of, a block of information and how should you approach this.
- CEARA TREACY: Yeah. Well, if it put it into a framework, I could take those, or if I put it into a workshop, I could take those examples. So, the workshop would probably work for me in that sense, if I could give people a scenario and then they had to work through it through the framework and then-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -find the controls.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Then I could use what they find and put it into the, my thesis, yeah, okay.
- Dr. KIM WUYTS: Yeah. The content is all there but, but, yeah, making it more user friendly or, yeah. Soften the blow of, like, 'This is a big framework because, well, you need it basically but, but now, here is how to, to get familiar with it and, and this is in general what you will do', and then you can go into more detail. [1.15.00.2]
- CEARA TREACY: Okay, yeah. So, yeah, no, I like your idea of having a technical document and then just a manual because, for a thesis, I was trying to combine both and it's obviously not working.
- Dr. KIM WUYTS: Yeah, yeah, yeah, that makes perfect sense for a thesis perspective, but I was thinking, like, well, with, if SMEs have to go through this, they might get a bit lost but it's really easy as a, as a reviewer to say because, well, it's a mistake I make all the time myself. So...
- CEARA TREACY: Okay, could you provide me with the main benefits, so, I'm happy. I'll just keep those there. I don't need. So, obstacles, so, awareness as an

Appendix F

initial activity (policy/consent) while the processing operations and purposes are not clear, the assessment might change the system. Well, we've talked about that already. I'll just say, 'See comments on DPIA'. Could a complete risk assessment capture all of the information required? Can a DFD capture? We've talked about that already.

Dr. KIM WUYTS: Yeah.
CEARA TREACY: Is there anything you think the framework does not capture that would need included?
Dr. KIM WUYTS: Well, that's related to the comments I had before, I think.
CEARA TREACY: Yeah.
Dr. KIM WUYTS: So, again, I'm also not a risk management expert. I will, well, I will mail you, well, you came across it. Laurens is, kind of, our, our expert in a lot of things, but he also just, half a year ago, finished his PhD on risk assessment and automation. So, that might be a useful background.
CEARA TREACY: Oh, that would be very useful, yeah.
Dr. KIM WUYTS: Yeah.
CEARA TREACY: Okay, yeah. So, step five, why is this required? Isn't this a sub-step of six and it seems to be so basic to have a whole step assigned for it? Yes, you're right, but I felt it was a necessary step just because to stop the confusion.
Dr. KIM WUYTS: Okay.
CEARA TREACY: Because from
Dr. KIM WUYTS: Yeah.
CEARA TREACY: So, you're going from your attack to your threat back to your security properties, and your privacy properties. So, it was just, it is a very basic step, I know that.
Dr. KIM WUYTS: Yeah, it was just such a small portion of the document that I was thinking, like, does it make sense, but, no, it's okay. yeah.
CEARA TREACY: Like, now, if you feel that it would be okay to put into step six because step six is pretty small as well. I can break it down to five steps. I was just thinking, you know, with everything that's going on, if it gets simpler towards the end, people will be like, going, 'Great, this is getting easier', you know.
Dr. KIM WUYTS: Well, maybe you can position it as you just mentioned, like, this is step five, and now, we're moving from the problem space into the solution space. So, we're thinking about requirements and solutions and...
CEARA TREACY: Very good, that's a great line, thank you, Kim.
Dr. KIM WUYTS: I'm, kind of, just giving you stuff that we include. So, yeah, make sure it doesn't look too much like, like LINDDUN. Well, it is LINDDUN, so...
CEARA TREACY: Yeah, into the resolution stage, yeah. I think it's just, it'll be, actually, quite good once it's done, and I have written papers on it just for everybody to see how it actually worked combining them both into a development team to see-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -you know, if it worked because I've just basically sucked in all of the information out there on this and put it into a framework to try to have a company-
Dr. KIM WUYTS: Yeah.
CEARA TREACY: -able to fulfil it, yeah. So, we're at 10.32 now. We said half 10. Do you need to go?
Dr. KIM WUYTS: I have, like, 10 minutes if that's sufficient.
CEARA TREACY: Yeah, well, we'll just run through this and then, might be too complex to understand and choose from, we've done that. Basic things like documentation of processing, yeah, we've talked about that. We might

Appendix F

- have talked about a lot already in these, great body of knowledge, might be over, yeah. So, that's about breaking it down, yeah, might be a bit over, hmm, basic building blocks seem to be in place, deem applicable, it will now mainly be about improving the usability. So, that's future work, I think, maybe Kim. [1.20.01.5]
- Dr. KIM WUYTS: Yeah, well, but that's also about that manual, and so, so, like, making it more practical, maybe, yeah.
- CEARA TREACY: Yeah, because, you know, I think it's easier for me because I'm actually in the organisation and the developers just listen and go on but whereas if it's just handed to a developer, it would be-
- Dr. KIM WUYTS: Yeah, I think they would be lost. So, you would need, like, a workshop or tutorial and, yeah. Well, in the current stage, but if you have manuals and, and those kinds of things, maybe they already can get started with that, but in the current stage, I think you would need to have, to provide them, like, some getting started, introduction anyway.
- CEARA TREACY: Right, okay, and that's the same for this question here, we've already discussed, currently feels there's a mix of several things, how to find the overall structure of the sub-steps. Okay, so, that again is just the...
- Dr. KIM WUYTS: Yeah, I think it's just cosmetics.
- CEARA TREACY: Okay, it's just, it's not structured very well.
- Dr. KIM WUYTS: Or it might be a visual thing, I don't know, it's, yeah. I, well, let me go back but I, remember I was a bit lost at the first table in step one. It first read like this is the entire thing to do but it's just the sub-steps in step one because there is not that, that, that overview of, this is the thing in general from a high level, from a high-level perspective. So, I was reading with the expectation I would get this high-level overview and then I dive into the details but it was already the details and that confused me a bit but...
- CEARA TREACY: Right, okay. So, maybe diagrams rather than a table or put, leave the table and put a diagram just to show-
- Dr. KIM WUYTS: Yeah, no, it's okay but have, at least, like the step one to six but it is in there, now, I remember, it is in there.
- CEARA TREACY: It's at the beginning, yeah.
- Dr. KIM WUYTS: There's a picture in there, yeah, yeah, yeah, no, yeah, hmm.
- CEARA TREACY: It's just not easy to work.
- Dr. KIM WUYTS: Well, if I'm nit-picking anyways, like, figure one, that's a really overwhelming picture.
- CEARA TREACY: Okay.
- Dr. KIM WUYTS: I'm so, it depends again on who you're planning to impress if, this is great for academia, I think.
- CEARA TREACY: Hmm.
- Dr. KIM WUYTS: But for the developer, it's like, 'Wow, this is complex', well, again, I'm not a developer. So, I don't know whether that's a correct statement.
- CEARA TREACY: Yes, hmm. So, it's caught between-
- Dr. KIM WUYTS: Again, this is just, like, have you extract the useful content, the instructions from your manuscript and put it into something more practical, a manual, an overview, a quick guide, getting started and, I don't know what, but, and that's also something more, more easy to share with the community. Like, this is, 'Look at this, this is something you can use and if you want to know more information, here's my PhD'.
- CEARA TREACY: Right, very good, okay, yeah. Right, okay, step two, creating a DFD should be feasible with this info, body of knowledge, overwhelming, subject assessment of likelihood and impact should be feasible, straightforward, great body of information, might be overwhelming.

Appendix F

- Dr. KIM WUYTS: So, it's just, there's an awful lot of information, I know that.
Yeah, well, there's a lot of information but how should I process it, how should I apply it, that, that, yeah.
- CEARA TREACY: Yeah, and so, yeah, it's really all just about the application. It's just, yeah. So, just rework it into a more usable document for developers, right.
- Dr. KIM WUYTS: Yeah, I think the content is there. You said you had a couple of things you would shuffle and then just extract it into the developer document and, yeah. [1.25.01.8]
- CEARA TREACY: Yeah, well, that's very interesting because what I'll do is I have a meeting with my supervisors on Thursday and I'll obviously discuss this, you know, interview and then say to them, 'How can I present this in my PhD as a, you know, do I present just a framework and then', what I'm thinking now because I have a chapter in the thesis on the framework. So, what I might do is put in the technical document as it is and then in the appendix, just the manual for actual developers and just pull all of that information-
- Dr. KIM WUYTS: Hmm.
- CEARA TREACY: -out and just then I could test that through a few companies and see if people find it a more usable structure, yeah.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Yeah.
- Dr. KIM WUYTS: Yeah, that was going to be my question, will you apply it in practice as well or...?
- CEARA TREACY: Yes, I'm applying it at the minute under the current, but that's with me embedded in the organisation because-
- Dr. KIM WUYTS: Okay.
- CEARA TREACY: -it's action research. So, everything they do is through me. So, not everybody's going to have a me in the organisation.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, yeah, I think it's going to be very useful. What I will do with the company is when we're done as a final interview or workshop, we will actually just extract all of the stuff they don't think they need it in, and maybe-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -build the manual out of that.
- Dr. KIM WUYTS: Okay.
- CEARA TREACY: Yeah? And that would then-
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: -have the input of the developers who have my knowledge and have the knowledge of actually implementing the framework and then, say, if I gave this to you as a developer, what's, what's the basics, do you need to know all of this stuff behind it.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: Or what's the basic you need.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, that might be where I go from now.
- Dr. KIM WUYTS: Yeah.
- CEARA TREACY: So, that might be useful.
- Dr. KIM WUYTS: Good.
- CEARA TREACY: Yeah, yeah, but that's great. Listen, thanks so much. I, in knowledge that we're 10 minutes over, I really appreciate your time, thank you very much. That's great.
- Dr. KIM WUYTS: You are welcome. I'm not sure when you're planning to, to have your PhD defence and whether it will be a public presentation but if so, then

Appendix F

- let me know, and if I have time, I'm happy to, well, I would be interested to see what the end result would be, and...
- CEARA TREACY: Well, absolutely, no, I'd be happy to share the end result with you and everything but, as well, if, you know, if you think there's any opportunity for collaboration in, you know, anything that you guys are doing, I'd love to be involved with that. I know that this is an area that the RSRC, the regulated software research centre in Dundalk is looking to get into more. Like, they're, you know, we're working now with IBM as well on machine learning as well. That's the new project I'm involved in but what, I'm from the perspective of, you know, making sure their privacy and security is in line with the regulatory requirements. So, that'll be very interesting because I've never done machine learning, and I don't know what's out there in relation to privacy and machine learning as well. So, like, that might be a whole field that's untapped. People like to call it, 'AI', but it's not AI, it's like, machine learning.
- Dr. KIM WUYTS: Yeah, yeah, yeah, it's different. Well, I definitely will let my colleagues know if there are upcoming research projects or, like, bigger European projects, well, my geography is not that great. Is Ireland part of...?
- CEARA TREACY: Yes, yes, yes.
- Dr. KIM WUYTS: Yeah? Okay.
- CEARA TREACY: No, no, no, we've a part of Ireland that's stuck in the UK.
- Dr. KIM WUYTS: Okay.
- CEARA TREACY: They've left, but we're still here.
- Dr. KIM WUYTS: Okay, good. So, well, I will inform my colleagues who are more into the project funding stuff and those kinds of things that you are on the radar for future projects but...
- CEARA TREACY: Yeah, absolutely, no, and I'll be happy to share the research with you when it's done and even like when I get it tied down, I'll let, like, send you on the framework and see, you know, what you think of it and if it's workable or any input at all, you know, and maybe for you to work out of it as well, whether it's going to be a doable, you know, can there even be a product built around it, you know, or, you know, do you, to me, I think pen testing is, with privacy, is a massive gap.
- Dr. KIM WUYTS: Hm-mmm.
- CEARA TREACY: So-
- Dr. KIM WUYTS: Yeah, but what are matrix for privacy, what are, yeah... [0.30.00.5]
- CEARA TREACY: Yeah, that's it, yeah. I suppose, you just keep hacking at it to see if you can get any information and then they might just call that security rather than privacy. You know, so, yeah, it's like, how much information can you get, what is the information, is it worthwhile, because I know definitely in the health domain now, there's, like, health data is worth a lot more than any other kind of data. So, it's a big, big part of, you know, the regulations here and stuff now, and looking to make it good, yeah. Right, Kim, thank you so much.
- Dr. KIM WUYTS: Okay.
- CEARA TREACY: I really appreciate it. Thanks so much.
- Dr. KIM WUYTS: You are welcome. I hope it was a bit useful to you.
- CEARA TREACY: Absolutely, but it's good that you don't see that it's, there's a major gap or that I've made a massive mistake or anything in any of it. So-
- Dr. KIM WUYTS: No, not so far-
- CEARA TREACY: -that's great.
- Dr. KIM WUYTS: -not so far, no, not from what I've seen, no, it looks, it looks really interesting and I'm looking forward to seeing how, well, I think it's there, but it needs some polishing here and there. So, I'm looking

Appendix F

forward to seeing the end result and...

CEARA TREACY: Well, the deadline has been slipping, slipping, slipping. It's really hard when you work.

Dr. KIM WUYTS: Yeah.

CEARA TREACY: So, it'll be a busy-

Dr. KIM WUYTS: I know, I know, it's, even without work, it's, I think, quite normal that the deadline keeps slipping and, yeah.

CEARA TREACY: Yeah, yeah. So, but look, it'll get there. I'm determined to get it finished. So, I really appreciate your time. Thanks, Kim, and I'll be in touch.

Dr. KIM WUYTS: Okay, great. Good luck, bye.

CEARA TREACY: Okay, thanks, bye-bye.

Appendix G STATSports Final Focus Group Transcript

Transcript of focus group held over Teams on 7th September 2021.

Persons Present:

Ceara Treacy – Researcher
CSA – STATSports Chief Software Architect
SD1 – STATSports Software Developer One
SD2 - STATSports Software Developer Two

Ceara Treacy And I'll start record in Teams and it will do the transcript as well.

CSA Yeah, sounds good.

Ceara Treacy Thank you very much for coming along and taking part in this focus group to review the framework that you guys implemented, and the developer driven framework for security and privacy and add in flow in the Internet of medical things. So, what I've done is thanks for your replies to the questionnaire that I sent and what I have here are some follow up questions based on areas that I would like to focus on that relate to the research questions and objectives and the answers that you gave and also on an international expert review.

I'm just grateful that you guys have come in as developers because it is targeted to developers and you giving your feedback on the framework will be an excellent aspect to the research. So, if you want to just introduce yourselves quickly and say, what you do in the organization and what you did in development if the product.

CSA Yeah, yeah, so OK. CSA at STATSports and I put the design together for the whole cloud architecture. That's essentially my role in the product project.

Ceara Treacy Thanks CSA.

SD1 Yeah, I'm SD1 and software developer and I helped to build and one of the developers that implemented the cloud into the Sonra product.

SD2 Yeah, and SD2 and the other software developer a STATSports.

I helped implement the solution for the cloud, both local and remote.

Ceara Treacy Great.

So, we're just going to go through the questionnaire that I sent and there are three section and it's the first section is number one. We're looking at the framework value and so the question was, in your opinion, is there a gap for specific individual implementation process for both security and privacy for developers inexperienced in this domain.

So, thanks for your answer. Your answer was that you agree and that there is a gap and guidance in. There is no one destination for developers to identify a framework that can be used.

Appendix G

So, follow on question is did the framework provide a tailored process that covers the needs for applying security and privacy and data in your individual software development program in your opinion.

CSA Yeah so.

I think yeah, like and this point will probably come up as like feedback, probably on the number of points, but I think it did and what I think. One of the things that I found, and the guys found as well as that the framework gave everything that was needed and it was very easy to pull up like all the specific threats that could happen within a particular let's say process or boundary.

Gu

Th

But those threats included everything and it would have been like network related hardware related and software related.

Gu

And so I think yes, the tailored process was there though, narrowing down that approach would be better.

HT/Im

Th

You know that end kind of decision point where you are kind of saying OK, what threats you know fit to this particular process? Applying the number of filters on that I think would definitely help

U-Ob

Th

Ceara Treacy Right, OK? And would you have like off the top of your head filters? That would be specific. Do you think of?

CSA So, I think yeah, if it was broken down into maybe like network related threats and if there was anything that was specifically hardware related threats and then software related threats.

Th

HT/Im

And developing software then you could nearly filter that again. Maybe if you're doing a web app there's specific types of threats that would be applicable there versus like a mobile app. And so, you could apply like different layers of filtering, and the thing would just be much easier, like when you when you get to that destination will pick and the threats to kind of pluck them out.

HT/Im

Ceara Treacy Right and SD1 and SD2? Would you say the same thing?

U-Ob

Th

SD2 Absolutely yeah, because I think whenever we, whenever you open it up first there was there was a lot of information around threats and it was like the CSA said, if the threats were more specific but you could choose any number.

Ceara Treacy OK, and so this is like rolls into question B. Does the framework in your opinion, present data security and privacy requirements on an equal basis? Did you get this impression from the framework?

HT/Im

CSA Yeah, I think so yeah. You know, like. Let's say data security during transmission and like any of the process boundaries there's transmission of data there. Oh, you know there was everything was covered off in terms of security and then the privacy of the data in terms of let's say storing in the database. Everything was covered off in terms of like a percent, viable data and how? How that should be dealt with.

Se/P

Se/P

Appendix G

Ceara Treacy You found that process was equal. It didn't give security more preference over privacy or vice versa.

Se/P

CSA Oh no, no, no, it didn't really feel like yeah, didn't really feel like one was favoured over the other.

Ceara Treacy And previously, would you have considered privacy as much or did the framework really enforce that?

Se/P

CSA I think, yeah, the framework really enforced privacy and I think. You know, I'm probably what you'll see in a lot of the responses where you were asking for, like a kind of like a time range of when you've really kind of part of their data security and data privacy. It's only really in the last one to three years when all this stuff as you know, started to get more important in GDPR and stuff came in, and so that's really when we started to think about it more. But yeah, the framework kind of forces you know you're looking at these two specific things, security, and privacy, at each of your processes and your process boundaries.

Re

Be

Se/P

Ceara Treacy Right and question C is then what challenges or difficulties did the software team encounter and implementing security and privacy at the same time during the development and using the framework. Was there any particular point where you thought or like there's nothing to do with privacy here? There's nothing to do with security, or how do we apply both? Or, you know, is there any conflict?

Se/P

Use

CSA And I think for us there was there was no real conflict between security and privacy, or that we couldn't apply something. And I think that the way the architecture of the system is a lot of a lot of our processes and services are developed the same way under the same patterns. So there was a lot of like reputation for us. You know, we really only had to kind of like.

Be

Dig deep into one of the one of the services and then that was able to be applied across the board.

Ceara Treacy OK, right and so then in question 1.2 A. in your opinion, is there a gap in explicit guidance for developers so around the regulatory requirements and the application opposed security and privacy regulatory requirements.

So, you strongly agreed with this in your response. So, the follow up question in the Focus group is does the framework provide, in your opinion, adequate information on the regulatory requirements for both security and privacy?

CSA 08:27.240 Yeah, I think so. Yeah, I think you know everyone's aware of let's say GDPR for privacy and but actually having framework where you go through and lays it out. Feel it definitely helps a lot.

Se/P

Gu

Gu

Ceara Treacy And was that useful in? The way the framework added the security and privacy properties that then linked to the threat categories that then linked to the individual threats? Was that a good enough way to link it, because the properties are to aligned to meet the data protection principles of the GDPR, which there are seven, but it was how do you translate those into development terms? So do you think that worked in the framework?

Appendix G

CSA yeah I think so. Like you know it kind of puts the GDPR into like the mindset of thinking about it the whole way through, you know, because you have to link it back to the GDPR through the properties and then link it to the threat. So yeah, I do think it did alright.

Re

Ceara Treacy Right, and were there any of the properties that didn't make sense at all in the framework? You know them like you obviously have confidentiality, integrity, and availability. That's the CIA that everybody knows about security, but there's quite a substantial number of other properties that the framework where they explained enough. And did you understand how to apply all of the framework properties?

C-Ob

CSA Yeah, I think so, there probably was a wee bit of Googling on the side to, you know, kind of get fully up to speed with the some let's say more obscure properties to do with privacy. But I think generally it kind of gave a good outline of them all.

Ceara Treacy And do you think that the regulatory requirements, does the framework provide enough information on how to implement them and that how important it is?

CSA I think it's and I think I touched on this in the feedback as well as that.

U-Ob

You know what we were not sure of you kind of go through with us.

Use

So, we had said we have a number of services that very much followed the same architecture. So, once you kind of go through and get used to the framework then I think it's much easier and I think we probably all of us probably just struggled a wee bit just at the start. And you know, just kind of figuring everything out. But I think once we went through it and once or twice then it you know it became very easy. It took a couple of reads and working through it to get the hang of it.

U-Ob

Ceara Treacy And it was very clear on what data is required to be kept secure and private.

Re g

CSA Oh yeah, yeah

Ceara Treacy And how did you find categorizing the information according to the GDPR - you had personal data and then special categories. Was that clear?

CSA Yeah, for sure.

Re g

Ceara Treacy No problem good and the screening statements in process 1.5. That's a significant aspect of the framework to meet GDPR requirements, and in your opinion was the importance of that screening are in this process. 1.5 appreciated by the software team. Like did you understand how important the process was? Was it clear enough in the framework?

CSA Yeah, I think so. Like you know I think you know we definitely have an awareness of, a big awareness of the GDPR requirements you know from, from working with you and this framework. So yeah, I think you know it was spelled out pretty clear to us.

Re σ

Appendix G

Ceara Treacy And how did the team manage Table 7, the lawful processing?

Again, one of the most significant aspects of the framework in in looking at being compliant with the GDPR requirements.

Do you have you any feedback on how that could be improved or how to make it easier? Or was it difficult? Anything at all.

Gu

CSA yeah, to be honest I don't think so because it again it's something that you know we are familiar with. It wasn't totally new to us and so yeah, I yeah, I don't really have any kind of specific feedback that we misunderstood it was pretty clear to us.

Re
σ

Ceara Treacy Yes. OK, and it was clear from your reading the framework that that was a really important part of the framework.

CSA Yeah, for sure and then also we, done this and with you.

Gu
C-Ob

Ceara Treacy OK, good. So, a quick question on the draft policy. Do you think that's a valuable asset for the development team?

CSA Yeah, for sure yes 100%.

Gu
Us

Ceara Treacy 100%. You'd recommend keeping it in the framework?

CSA Yeah, yeah, I think so. And I think I even mentioned in the in the questionnaire there just, having an interactive draft policy potentially might be very beneficial to people. You know, just taking them through the whole the process. How it relates to the software or product they are building

HT/I

And you know, using that draft? I guess as the basis.

Ceara Treacy So having an interactive example for the privacy policy too. To outline each part of it and what will change for each project?

Gu
C-Ob

CSA Yeah, for sure like we done this with you and that really helped us understand it and complete it.


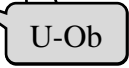
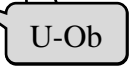
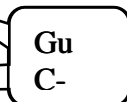
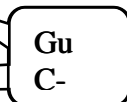
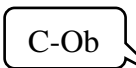
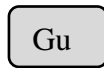
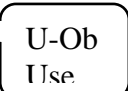
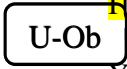
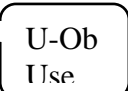
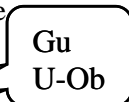
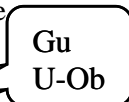
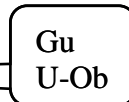
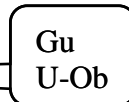

Gu
Us

Ceara Treacy OK and so is the language in the framework understandable for developers? Some of the feedback has been divided on this. So, I'd appreciate what you would say, what you think of it.

C-Ob

CSA Yeah, so yeah I think and this is probably where some more Googling came but, you know, it's the first time seeing a framework like this so it's I guess typical of the language I would expect and I don't really have any kind of feedback on how to water it down, let's say for the likes of us, you know, I think there is terminology in there that you probably have to use, and what it is I guess it's just about making sure that the definitions are there so that people can easily kind of understand it.


Appendix G

- Ceara Treacy Right, and what did SD2 and SD1 think? Because you wouldn't have been as familiar with the language as the CSA. 
- SD2 That for me anyway was a big step up like but after a few meetings going through with the CSA and you like everything started to click. Like as soon as you got further in, and we got into the processes and going through each one like. The language started to make sense and you knew how to work your way around and understand the whole framework a lot better by the end of it. 
- Ceara Treacy And was it overwhelming SD1? 
- SD1 Initially I thought it was a wee bit overwhelming. 
- SD2 Yeah. 
- Ceara Treacy OK, and what made it easier then? 
- SD1 I just I think that the time spent going through on each of the meetings as SD2 touched on there, going through it. The CSA was a big help to us explaining it as well. 
- Ceara Treacy And if you didn't have somebody there who didn't have the CSA's knowledge and experience, do you think it would have been more of a struggle?
- SD1 Well, I think we would have got there eventually. But yeah, just this. 
- SD2 It would have been initially in getting started it would have been difficult 
- SD1 Yeah, just the getting started would have been a struggle. 
- Ceara Treacy Do you think there's enough information and guidance in this? The framework for software team to apply both security and privacy? 
- SD1 Yeah, well there is plenty of information. Yeah, it's just I guess we were kind of doing it in dribs and drabs, and probably not, do you know not taking it all in initially where we kind of doing parts and then stop thinking about it until we came to a new development and then doing another wee bit, you know that sort of way. 
- Ceara Treacy Great ok thanks for that. So, it would feel like you have to jump back in and refresher or something? 
- SD1 Yeah. 
- Ceara Treacy OK and so at the end of it all, would you say you have a better knowledge and understanding to address the regulatory requirements by implementing/through implementing the framework?
- SD1 Yeah, definitely. 

Appendix G

SD2 Absolutely yeah.

Ceara Treacy Would you say that your confidence in regulatory requirements and how to apply them will be better or higher?

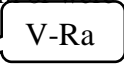
SD1 Yeah. 

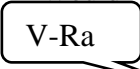
SD2 Yeah.

Ceara Treacy So question 1.3 is again a lot of this already probably been answered because do you agree the framework provides sufficient guidance about how security and privacy risk assessment in the domain.

So that would be step four really off the framework where you're looking at the risk assessment where we would have done a likelihood against impact and those tables that come from NIST SP 800-30.


How does the framework risk assessment differed differ to former risk assessments used by the software development team or were there so former risk assessments done?

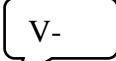
CSA Yeah, so **we wouldn't have really done former risk assessments like this**, and I think you know **we would have taken security into consideration in development, and you know, obviously.** 

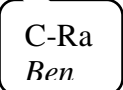
Ceara Treacy Would it have been documented or anything to keep track of the decisions? 

CSA And **not from the initial**. So when, **let's say when we started developing Sonra, there was worked on around that you know with yourself documenting the privacy and security requirements from the GDPR and that very much followed through because of a lot of the services are the same that very much followed through for the other services as well. And so yeah, we like since then we wouldn't have gone through like a formal kind of framework like this and documenting things out.**

Ceara Treacy So, on that note, do you think the steps in the process and the risk assessment part of the framework were sufficient to have to get you through it?

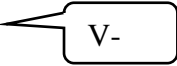
CSA Oh yeah, yeah, definitely yeah, yeah. 

Ceara Treacy Were the processes easy to follow? 

CSA Yeah. Exactly, yeah, yeah. And like we **in some aspects we were doing it retrospectively. You know on stuff we'd already done, but I think obviously the main benefit comes if you're starting a project from scratch that you know we include this in the requirements phase that you actually go through and do your DPIA on what your actual design is.** 

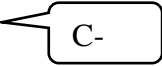
Ceara Treacy So, for the new part to the system, developing into the cloud. It was very beneficial to start this from the beginning?


Appendix G

CSA Yeah, exactly. 

Ceara Treacy Great thanks for those answers. So question 1.4 and to follow up to that question. Do you agree the framework will provide an adequate risk assessment to meet the security and privacy requirements?


And then we've answered some of these already really where the risk analysis tables and Step 4 easy to use?

CSA Yeah, definitely. 

Ceara Treacy Does the team think the risk assessment skills were adequate for the purposes? So, as you know and the scales provided for rating the risk in the framework, they were adequate? 


CSA Yeah. Yeah, I think so yeah, yeah.

Ceara Treacy And would an illustrated example help with the risk assessment process?

CSA And kind of like I said in the above where I was kind of saying like an interactive one, even you know. I think like the more kind of visual stuff definitely helps. 

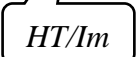
Ceara Treacy And that would be from the very beginning of the framework having like a type of tutorial or interactive tutorial?

CSA Right

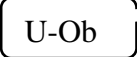
Ceara Treacy What kind of a tutorial or an interactive tutorial? 

CSA Yeah. Something along those lines are right. There is one example system, and you would show this through each step of the framework.

Ceara Treacy Alright, so like you said in your questionnaire answer, for each step you could have like a video going for process one. This is what you would do?

CSA Exactly. 

Ceara Treacy OK and follow it through each step of the framework.

CSA Exactly, yeah, you know because. I think that shows you know, for people coming to a framework like this for the first time you know it can be very kind of. You know when you open up the framework and there's a lot of information there and different sheets and Excel that can be. Maybe we've been overwhelming, so having a break down of each step in a visual, you know, a separate for each separate part, will just ease that a wee bit. 

Appendix G

HT/I

Ceara Treacy: Alright, so did you think that the risk analysis worked well for both security and privacy? Or was did it work better for one over the other?

Se/P C-RAs

CSA: Yeah no, I think yeah like before, I didn't feel like one weighted above another there, you know I think everything was really on par.

Ceara Treacy: Great, does the team have more or less confidence in completing their risk assessment after implementing the framework.

SD2: Ah more.

SD1: Yeah, absolutely yeah.

C-RAs

Ceara Treacy: More confidence then.

C-RAs

SD2: Absolutely.

Ceara Treacy: So, you'd be happy if somebody said oh can you do a risk assessment of this? You'd be yeah, no problem. I can figure that out?

C-RAs

SD1: Yeah.

SD2: Yes.

Ceara Treacy: Great, question 1.5 brief overview of the main benefits you have observed for developers.

So, I'm just going to go down to the additional follow on question.

And again, lots of this has already been said above.

Does it assist if you think of anything while I'm reading them out? Absolutely just answer it.

SD2: Yep.

Ceara Treacy: Does the framework assist the software teams' knowledge and understanding of data security and regularly for requirements in developing a software project?

SD1: Yeah.

Ben

SD2: Yes.

CSA: Yeah, yeah for sure

Re
g

Ceara Treacy: Yeah, does it provide confidence for the team that you are actually meeting the regulatory requirements when you're implementing it?

Appendix G

SD2 Yeah. I feel that following it will keep you online with these

CSA Yeah, yeah for sure.

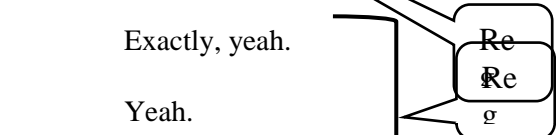
SD1 Yeah.

Ceara Treacy So implementing the framework you feel like you're actually fulfilling the requirements of the GDPR?

SD2 Yeah.

CSA Exactly, yeah.

SD1 Yeah.




Ceara Treacy Oh, good feedback thank you all for your input.


We move on to question 1.6 in your experience with the purpose and activities and outcomes of the framework assist developers in SMEs, inexperienced and security and privacy risk assessment, meet regulatory requirements and you said yes to all steps.

So, there's a couple of questions that came in the follow up here, I just want to run through with you Do you think that the framework provided adequate information on the regular requirements for data and security and privacy?

CSA Yeah.



Ceara Treacy Does the framework provide enough information on implementing the regulatory requirements?



CSA Yeah, I think so. Yeah, and I think it even that there's a lot of links in there to bring you to even additional information, and so I think that was very helpful that you have put those in the framework. You know you have the direct point of where to go. If you need more information.

SD2 Yeah. I feel that

SD1 Yeah.

Ceara Treacy So, the fact that you didn't have to look for the additional information that you didn't have to Google it essentially link was there. So, would you trust those links that that's the proper correct information from the right source?

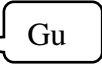







CSA Well, if I'm trusting the framework, I'll trust the links.

Ceara Treacy OK great and so I'm just going to run through this then.

Are there individual components that are more valuable than others for inexperienced developers in your opinion, in any of the steps?

So, in step one. Is there anything in individual component that's more valuable?

Appendix G

- CSA I'm gonna say no. 
- SD2 Yeah. I agree with that
- SD1 Yeah.
- Ceara Treacy OK, and what about Step 2? 
- CSA Yeah again, yeah no, I think. Going to say that for all of them. There was nothing really. I don't think that any of the processes is more valuable than one of the others.
- Ceara Treacy It was all valuable information. Is there anything that is not needed or overcomplicated in any of the steps?
- CSA I don't think so, no, I think. You know I don't really have anything to compare it to either, you know, and so I think you know we were taking this that it's OK, we'll learn in the framework and we're taking that for granted. But yeah, I don't think there was. And there was nothing that wasn't really valuable. 
- Ceara Treacy Right 
- CSA Yeah, and there wasn't really one thing more valuable, or you know.
- Ceara Treacy OK so, to the best of your knowledge, then the framework doesn't fail to identify any security and privacy risk assessment.
- CSA No no. 
- Ceara Treacy Is there anything that would make the risk assessment more understandable, or was it clear?
- CSA Yeah, I think it was. I think it was clear. 
- Ceara Treacy Right, OK? And then question 1.8. You give an extensive answer to this about, I believe adding multiple layers of filtering will help improve the framework value. Currently all possible threats are included, but these can cover a wide array of domains. Having the ability to allow developers filters threats to be more specific to their domain will help greatly in the overall ease of use of the framework and help with framework adoption. 
- So I think we've pretty much covered that.
- It's like, you recommended dividing it into different areas of development.
- CSA Exactly, yeah. 

Appendix G

Ceara Treacy And just final one. Do you think that the framework makes security and privacy risk assessment achievable for developers inexperienced? So this would probably be more for you SD1 and SD2. You weren't experienced in it before you implemented the framework. So do you think the framework makes it achievable?

SD1 Yeah. Yeah, absolutely.

C-Ras
Gm

SD2 Absolutely yeah. You know I like that there is a set structure in place to go through and actually put your products against before you even start them, with developing them like before you begin, and I wouldn't even have a clue where to start with this without the framework.

Ceara Treacy Right, OK,

SD1 Yeah, exactly.

C-
RAs

Ceara Treacy So, 2 framework compositions

Question 2.1 Is the framework summary rationale easy to understand and follow?

So, you know and the summary and the diagram of the steps at the beginning does it provide a clear overview of the framework and the steps in the framework.

SD1 Yes, it is easy to understand once you get used to it or and go through it once or twice.

CSA Yeah, yeah, I think so.

Use
GUI

Ceara Treacy It does because there was some feedback that it was a little unclear that they're they weren't sure how many steps were in the framework, but you were fine with it all. It was clear enough for you guys.

CSA Yeah, I think so.

Use
GUI

Ceara Treacy And figure one, that provides a clear overview along with the summary.

CSA Yeah.

Ceara Treacy And is there anything that you think would make the summary and rationale easier to understand for new users, or is it just what it is?

Us
e

CSA Yeah, for me I think, it is just what it is, I think. Like a point I made before you know potentially that interactive demo, which I know we touched on before well that, just so it's a complete run through.

But other than that, yeah, I think once you kind of get your head around that then it's OK.

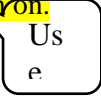
Appendix G

Ceara Treacy Would you say that there is continuity with the framework steps? Do the steps flow naturally or do they hesitant or stammers in them?

CSA No, I think **I think it flows naturally enough, yeah?**

Ceara Treacy Are there any of the steps that create an issue for implementation where you had to do extra, say Googling, or look for feedback from me.

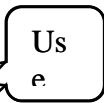
CSA I think there was one point I do remember we did get clarity from you in a particular area. I think there was there was one point. I do remember that we did get clarity from you just on a I can't remember exactly what. What it was, but I do remember in one of our catch-up calls, we did bring it up and but no I think in terms of the Googling stuff I don't think so. I think **you provided like a lot of links there to more information, so they were kind of sufficient enough for us for anything that we feel we needed more information on.**

Ceara Treacy OK and in step 1 it is named contextual knowledge. 

Is this the right title for that step or would you suggest anything else?


CSA No seems OK to me.


Ceara Treacy Included in step 1 is awareness and did having the awareness in step 1 help or hinder the implementation for the team?

CSA And well, Yep, **they certainly didn't hinder it anyway** 


Ceara Treacy Did they help it either?


CSA I mean **it helped with the overview of the thing. So yeah, I'd say that would have helped.**

Ceara Treacy Step 1 the screening statements in the framework, it's processed 1.5. This is one of the major aspects of the framework. Was that importance appreciated by the development team? 

CSA **Yeah, I think so, yeah.** 

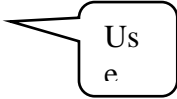
Ceara Treacy So, this part is highlighted sufficiently on how important that part is. Is there a need to increase its profile?

CSA I don't think so, no. 

Ceara Treacy And just jumping out from ~~that~~, do you think that the framework should highlight the parts that are particularly important to meet GDPR requirements. 

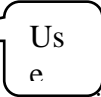
CSA Yeah, I guess **would be no harm in pointing it out, but I mean, to me it's all kind of part of the one process you know. So, we were kind of treating them all of equal importance.**

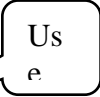
Appendix G

Ceara Treacy: Right, OK? 

And also in Step 2 follow on question - the process of listing already known security and privacy decisions or constraints.

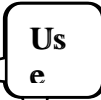
Was that logical and useful for the software team?

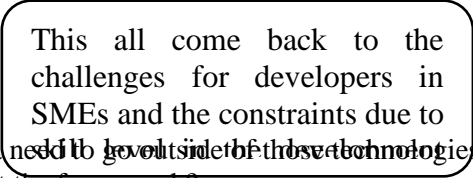
CSA: **I think yeah.** 

Ceara Treacy: And do you think that was particularly useful because you were a SME? Or is it because that you were bound to different technologies anyway? 

CSA: **It was probably more due to the technology let's say, more so than an SME**

Ceara Treacy: Would that be because of the level of experience in the software development team?

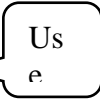
CSA: Probably yeah. 

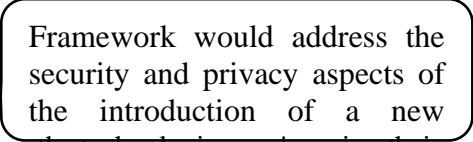
Ceara Treacy: Do you think that if there was a need to go outside of those technologies that would take longer to implement the framework? 

CSA: **Potentially yes because it be outside the skill set of the of the team.**

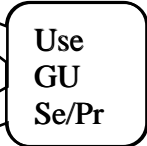
Ceara Treacy: Do you think that then the step process were listing the already know security and privacy decisions or constraints?

If you had a new technology to use within a project, that this process would help in establishing bringing the technologies security and privacy into the project?

CSA: **Yeah, I think so.** 

Ceara Treacy: So, were you able to tap into say the technologies you're using their security and suggestions because you had listed this already? The previous are the known. 

CSA: Yeah, yeah. **We use basically the best practices provided by those technologies.**

Ceara Treacy: And you tied this into the development cycle. 

CSA: **Exactly for the implementation of it.**

Ceara Treacy: Oh fantastic.

So, with the system decomposition process did they already know constraints and decisions help with this process or did the team see these individual things anyway?

Appendix G

CSA This the boundaries and processes, isn't it?

Ceara Treacy Yes, this is where you're developing the data flow diagrams and so the decomposition process having listed the previous or known security and privacy constraints or decisions? Did that help in the data flow diagram?

CSA Yeah, yeah absolutely.

Us
e

Ceara Treacy Were the team able to identify the assets with the guidance provided?

CSA Yeah.

Ceara Treacy Was the data flow diagram guidance easy to follow or was there anything that caused any difficulties?

CSA No, it was easy to follow.

Us
e

Ceara Treacy Was it useful?

CSA Yes, because of the particular format. I think was that particular style of DFDs, it was useful to have the complete table of explanations there. All of the examples were clear, and yeah having it all there to use made it easier and keep it the same the whole way through, yeah, the same all the way through. Also, everyone worked off you know same template so you know all of DFDs would have the same format.

Us
e

Ceara Treacy Right, OK? And then when you added in, the privacy annotations and the security annotations, was that an easy or was that a challenging process?

Us
e

CSA I'd say probably in it like it wasn't, it wasn't that challenging. You know it's more just putting a lot of thought into it and going through each one. And because a lot of our boundaries and processes would be the same or very similar, it was just about continuing that on from when we did the initial one and check to see if anything was to be added or had changed.

Ceara Treacy So, would you say the more you used it and the more you understood it, it got easier?

CSA Exactly, yeah.

Us
e

Ceara Treacy OK, so do you think the annotations were useful when you got to the part where risk assessment and threat analysis?

Us
e

CSA Yeah, for sure. well, it was just explicit of you know where we had to do the risk analysis and concentrate on threats. We had already established where the data was, or yeah the type of data is was and so yeah it was just highlighting it in the DFDs and you know, like making you think of where all of the data is and yeah the type of data. It was much more visual you know

Appendix G

you could look at the DFD and see where you know had to look at privacy and security.

Ceara Treacy Oh, it did OK? Because you had knew that there was like a security annotation or privacy annotation at that part.

CSA Exactly, yeah.

Ceara Treacy So that would be a big part of it for the team.

CSA Yeah

Ceara Treacy Did you think that the information and the colours of the trust boundaries helped you with developing the DFDs?

Or is it just another a hindrance to developing DFDs?

Use

CSA Different colours and stuff for me no because I like visual stuff so.

Ceara Treacy Right, OK, so you think the visual stuff is very good because there's difference in?

Use

CSA Exactly. It just makes it clearer when you're looking at it, you know and it makes it easier when you are putting the DFDs together you have to think about what type of boundary it is. This will make a difference to the security, privacy level or how you think about them.

Ceara Treacy would say that for the annotations as well, in fact that they were different colours that are helpful.

CSA Yeah.

Th

Ceara Treacy Step 3, threat elicitation. Do you think the step provided enough information for developers inexperienced in this aspect to implement this step?

CSA Might be one for the guys there was I think was fine, yeah.

C-Oh

SD1 Yeah, I think so, again, it was probably a wee bit of a learning curve to sort of understand what exactly was needed. But, once you get your head around it, it was pretty straight forward.

Ceara Treacy And how would you have deemed it? Complicated/Confusing/too intricate? Or what is initially was just too much information.

SD1 And yeah, I kind of felt a little bit overwhelmed at times with it. I just thought it was kind of bombarded with information.

Ceara Treacy And what do you think would help you with that?

C-Ob

Use

Appendix G

SD1 Well, me personally I like things broken down and the layman terms really kinda breaking it into chunks nearly to make it just really. Understandable and clear.

C-Ob

Ceara Treacy Was it just this step 3 that was too? And what would you say? Was it just too? How would you describe it

SD1 I wouldn't say difficult, probably just, oh what is the word I'm the word I'm trying to look for.

U-Ob

SD2 It's that it was a bit tedious at times because of the like the jumping back and forth to try and find out which risk you were dealing with. Like whenever we did the first one it took a bit of time to get my head around how the way it worked. But after we done one the rest of them were pretty much the same idea and it was understandable to do after that.

It's probably just more the formatting of how it was done, which took the most time to get use to

Ceara Treacy OK., so, there was a lot of jumping around the place back and forth through the different spreadsheets.

SD2 Yeah, there was a lot of jumping around the place

Th

Ceara Treacy Right, OK? And do you think SD2 that the threat to attack starter kit made it easier for you to find out threats?

SD2 Yeah, absolutely yeah.

Ben

U-Ob

U-Ob

SD1 Yeah, without a doubt.

SD2 But I think if you if you a way of being able to link between, say, your interaction and the threats that you do have in your interaction and between that starter Kit it would be make things a lot easier.

Ceara Treacy So you're talking about links right through the Excel sheet? So having a link between the threats and the starter kit to the security controls? Or is it to the DFDs?

SD2 To the security controls right through to say the threat through the properties, maybe.

Ceara Treacy Right, OK. So this would move us on to step 4 so this step involves once you had your threats you complete the analysis and prioritization of the threats? Was the guidance enough to help you complete that?

SD2 Oh yeah, absolutely yeah.

Gu

U-Ob

SD1 Yeah.

Th

Ceara Treacy And you see the ones you had to apply controls for, you could you prioritise the threats you had to apply controls for, which ones were more important?

SD2 Yep.

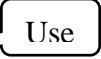
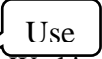

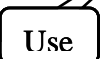

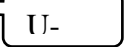
Use

Use

Appendix G

- SD1 **Yeah, yeah.**
- Ceara Treacy Just some more general questions on steps 2-4 in this section.
- Was the process to track risk assessment for security and privacy practical for the software team or was it confusing? You get confused between which ones you should prioritize first whether it was privacy or security or was it clear cut do you think?
- Were the processes in steps 2-4 practical for the software team for both privacy and security?
- SD1 **No, it was fairly clear, I don't really remember having a priority of one over the other or actually thinking that one was easier or more difficult than the other. Having a priority over one or the other whenever we're implementing it.**
- Ceara Treacy OK so you didn't see that one more as prioritized over the other?
- CSA **No, I think it was pretty. There wasn't an emphasis on one over the other. I don't think either.**
- SD1 **Yeah.**
- Ceara Treacy OK moving on to Step 5. In your opinion is Step 5 and necessary step?
- So, this is Step 5 where you've established your threats and then you have to link that threat back to a framework property. This is where SD1 and SD2 you were coming in to say the link back from threat to property to controls was repetitive or tedious. Link into the controls was clunky. Is that what you're saying, SD2?
- SD2 **Yeah.**
- SD1 **Yeah, I would say that too.**
- Ceara Treacy So, given that is Step 5 necessary? Completing Step 5 going from threats to security and privacy properties to controls?
- SD2 It was step five. I think there was another step in there as well. So I'm trying to find it.
- Ceara Treacy So, step 5 is a small back mapping step that rolls into step 6 where then you select the security and privacy controls.
- So, lets put it like this, in your opinion, should Step 5 and step 6 be together, or should Step 5 stay separate?
- SD2 Uh. OK
- Ceara Treacy So step 5 is where you get all of your prioritised threats listed and you map them back into the different security and privacy categories whether it be confidentiality, availability, integrity or linkability and you put the threats not their category to look for the controls

Appendix G

- SD2 **Yep. I think whenever we done it, we did it like the whole process at a time rather than breaking it up as like step 5 or six we, we did them combined.** 
- Ceara Treacy Right, so you don't see Step 5 as a necessary step. You think you could just roll that into steps 6 and make it just a five-step process.
- SD1 Yeah.
- SD2 Possibly, yeah.
- SD1 **It's kind of personal opinion. We kinda did do it in that it was rolled into one, but for me personally, I kind of like it separated out because you've got that wee better extra granularity, it breaks it down that wee bit more.** 
- Ceara Treacy Right, OK, that was the whole point in putting as an extra step was to make it less complicated. But if it's going to be just rolled into one step anyway, do you think that it's still necessary to leave it as an individual step?
- SD1 **I would be of the opinion that yes, it is still necessary to have it as a separate step,** but the guys might disagree with me on that. 
- Ceara Treacy OK.
- CSA Eh no. **I'd agree, I think. I think yeah, this the smaller the steps the better. It's better to have more small steps than. Do a large steps in my opinion as well.**
- Ceara Treacy Right, OK yeah, yeah. So, you don't lose your way?
- CSA Exactly, yeah. 
- SD1 Yeah. Yeah, yeah.
- Ceara Treacy OK, so step 6. I know we've touched on this already a little bit where you're selecting the controls from the spreadsheet.
- Did step 6 explain clearly enough how to do this step?
- CSA yeah, I think so. 
- SD1 Yeah.
- Ceara Treacy I know that you said there was a difficulty with the formatting going back and forward, but were the controls easy to match to the threats?
- CSA **Yeah, I think it just was like took a wee bit of work. You know because all the threats and attacks were listed, but when you kind of click in for more info on the attacks. They may not have been directly linked or correlated to whatever your threat was and you had to look through all of the attacks in the threat category they were listed in.** 
- Ceara Treacy OK The particular attack and threat that came from the threat, when looking at the control categories the control didn't really apply to mitigating that specific attack.

Appendix G

And is there anything you think that could be done to help that?

Or is it just a little more working with the controls to become familiar which ones in the categories would work for particular threats?

U-Ob
HT/Im

CSA Yeah, or even you know, adding a kind of filter and stuff in that we kind of talked about where you could filter them down based on a particular/kind of domain that you are working in.

Ceara Treacy OK, right. So, you think this would make it easier to select the most appropriate controls, having a filter in?

CSA Yeah

U-Ob
HT/Im

Ceara Treacy OK good. So, question 2.3. Do you agree with the ordering implementation in figure two of the framework steps? Does it depict the steps clearly? And do you agree with them? Is their rework needed or is it just fine the way it is?

CSA Yeah, I'd say it's fine the way it is because I yeah, I didn't really think the way it was laid out there was any major issue with it, like I have nothing really to compare it to so it was fine for me.

Use

Ceara Treacy Right, OK, and do you think that there's anything needed more at the beginning of each step to go back to that Figure 2 depiction, or just it's fine with the one at the beginning?

CSA Think it's probably fine at the beginning, yeah?

Use

Ceara Treacy OK. Do you think that the privacy and security knowledge is offered in a systematic way throughout the framework?

Or is there one step that's lacking in a systematic manner, more than the others?

CSA I don't think so, no.

Use

Ceara Treacy And are there any activities or processes that are unnecessary in the steps?

CSA Nothing comes to mind

Ceara Treacy That's it for the follow up on question 2.6 I believe. I'll run through the last few questions here for this question but, I think we have we've answered many of these questions already.

There are 6 steps would it be better to incorporate step 5 into 6?

Does section 6 need more information or guidance on how to select suitable controls?

We've talked about that.

Appendix G

Does step 1 require more clarification around the GDPR requirements for documenting personal data involved in the project? We discussed this too in step one.

Ceara Treacy So, question 2.7. In your opinion, does the threat to attack starter Kit provide guidance in the systems being developed for identification of threats to attack for application in the framework?

Is this particularly significant from an SME and developer inexperienced in this domain?

So would you see the threat to an attack library starter kit as background information or as a necessity for developers and SME to get a kick start on this process?

Quite a lot in that question

Use
Th
Re

CSA I think the threat to a attack library starter kit is really a necessity to get the kick start.

Ceara Treacy Right, so you don't think that there was enough experience in the team to find those, or it would be just a difficult task?

CSA Yeah, I mean to be honest, people could probably figure it out alright, but it would be a difficult task to. You know, particularly with when you don't have experience with any similar type frameworks or nothing in threats and actually finding or thinking about the threats for a specific part.

Ceara Treacy Yeah.

Use
Th
Be

SD2 Even if you didn't have the threat to an attack library, you might miss a few as well, so having it there makes you see all the possibilities rather than you could be single minded and only pick out a few. Rather, this puts it all in front of you and all of the potentials.

Ceara Treacy And did the library encourage you to go and find out other potential areas or to look at, say, the OWASP top 10 or the other CWE and threats that are out there at the minute.

CSA Yeah, we view them quite a number of times, alright?

Use
Th
Re

Ceara Treacy You did? OK! So it did its job of, you know, making you look outside of the library table in the framework.

CSA Yeah.

Use
Th
Re

SD2 Yes

SD1 Umhuh, yes

Use
Th
Re

Ceara Treacy Alright, that's good to know. Do you think the linking into the resources for the library made further investigation easier for the team?

CSA Yeah for sure.

Ben

Appendix G

- SD2 **It is good to have these resources**
- Ceara Treacy And to the best of your knowledge, does the framework fail to identify any security and privacy risks? Do you think there's anything further needed to help the team to identify security and privacy threats? **C-Ra**
- CSA **I don't think so now we kind of go to those external sources as well, but I believe they were linked in some respects throughout the framework as well And so no from me.**
- Ceara Treacy OK, and if you had a how to use guide. What way would it be, in your opinion, having used the framework, how would it be best to do it?
- CSA **HOW TO USE I think an interactive demo. You know, some kind of going through each step and explaining each step of the way what they're doing, and you know, even given an example system and doing up the DFDs for that, or at least one 1 DFD and then taking that the whole way through the framework and each step.** **HT/Im**
- Ceara Treacy And the user would just like click a link and have that up on the web somewhere that people can go. And as just watch that one step.
- CSA **Yeah, I think so.**
- Ceara Treacy OK, so break it down into each step and have a demonstration for each step.
- CSA Yeah, you could do it for. Yeah, **you could do it for each step if you wanted to do it like that like a series of bite size videos. And or I think just one overall video might actually that might be quite long and maybe people might click off it. So maybe the smaller videos on each step is better.** **HT/Im**
- Ceara Treacy OK, and do you think it would benefit as well from a technical document rather than just the huge academic document it is currently?
- Or so the technical document will be paired down, but it would reference sections in the academic document. Or do you think it's like just leave it the way it is with a demonstration? **HT/Im**
- CSA **I don't know if this is the right answer to say both because I think it's good to have it all there. Let's say the first one or two times you kind of go through this, but then as you kind of get more familiar with it, then maybe haven't just the technical stuff. You know it's just a cleaner approach.**
- SD1 Sorry, my Internet has dropped.
- SD2 Hey, you know I haven't.
- SD1 So, I've kind of missed the last couple of minutes.
- Ceara Treacy All right, no, that's OK, and so we're just talking about, you know, if there was a how to use guide for the for-software development team from your perspective, what it would be. The CSA suggested a step-by-step video for each step, and then we talked about, the framework in its current form. Is the

Appendix G

current version of the framework too heavily academic? Would it be better with a technical document to accompany the heavy academic document as well?

So just to get some feedback from your use of it how you feel would be best suited. You know, given that you guys had very little experience in threat modeling, extracting security and privacy threats and risk assessments, and how would you think another team from a different IT company would use the framework documented in its current state.

SD1 Yeah, like SD2 said.

SD2 Thank heaven.

SD1 Go ahead, I could cut the cross here.

HT/Im

SD2 I think a technical document would be a lot easier to get into since we like I wouldn't feel as overwhelmed from compared to the academic document and then combine that with a series of small videos based in each step. And I don't think it would that be all I'd need really.

SD1 Yeah, yeah I totally agree.

SD2 And to be able to do this confidently.

Ceara Treacy All right, so you think that just a technical document with the videos would be good and there's no need for the academic document as well? Or would you like to have that in the background information available if you wanted further information?

SD2 Yeah no, I think keep the academic document, but if you had your videos that you say if you're doing this first time your videos guide you through the whole way and then you always have your technical document which you could reference with the videos. It's from the videos and then use that going forward as you go to and then you'd also have your academic information if you need more information or links on any particular subject that's there as well. Because I think this, for doing this sort of thing, the more information you have around the better it is.

Ceara Treacy Right? Well, the goal of the framework is to inform you of everything that's required without you having to go looking for it on your own and not find the correct or appropriate information. So you think that the academic document provides that?

SD2 Yep.

Ben

SD1 Yeah.

Ceara Treacy Great, so at the end of it, overall, how would you characterise your understanding of the framework and the outcome?

SD1 Say that again, sorry, I only caught bits that are getting dropped.

Appendix G

Ceara Treacy I am sorry it might be my Internet. Having done it. How would you characterize now your understanding of the framework and its outcomes and what it wanted to achieve?

SD1 Yeah, for me it's a whole lot clearer like whenever I first kind of started like a mess, mess around it kind of felt overwhelmed. I thought there's a lot of stuff in here. But yeah, now once you sort of get a step-by-step picture and how things are meant to work. Yeah, it's it does your understanding and confidence as well increases. Use

Ceara Treacy Right and would you be confident to put somebody else through the framework?

SD1 Yeah, but I would like to do a bit more studying on it to refresh my mind but yeah.

Ceara Treacy OK, good thank you SD1 SD2 do you have any feedback? Use

SD2 Ah I agree. Whenever we started to like the 1st and so like the first process, we did like identifying different boundaries and that sort of thing, and whenever we start doing that, everything started making sense. And even from that now I'm sort of looking at different things. It's implanted it's almost in the back of my head, seeing the different potential threats and I was like, oh that's a search party and this is the possible outcomes with that before I even need to do a process like this again. It's just. It's always got me thinking about it now. Ben

Ceara Treacy Well, that's great. That's a brilliant outcome. So, it's just implanted the idea, security and privacy in your head and developing.

SD2 Pretty much.

Ceara Treacy Ah, good. I'd say that's a bonus. So quick question. Then, did the team expect to have a quick fix for privacy and security by design?

CSA I wouldn't say like quick fix, but maybe like a framework that you know would be, you know more closely included in the development process.

Ceara Treacy Right? Use Ben

CSA And you know, I, I think you know as a kind of said that a lot of our stuff follows the same architectural pattern. So a lot of these principles and so would apply across the board, and but I think is like SD2 said, you know everyone is more aware that you know if we introduce a new process or new boundary that, you know we go back and go through this and OK, yes it may be something that's very similar to one we've already mapped out. But there also could be a couple other things that we need to include in it.

Ceara Treacy Right, OK good so would the team say that introducing security and privacy would be a bit of a drawn-out process?

Appendix G

CSA Yeah, I don't know if it's a drawn-out process. I think obviously extra work in the development effort like but yeah, I don't think it's a drawn-out process.

Ceara Treacy And do you think the frameworks fits well within the development lifecycle or could there be a little more work done around that?

CSA Yeah, I mean to me it was fine. Obviously, we were doing this on a project that you know is out there and we're currently working on like. But I could also see it being, you know very beneficial to actually completing this before we start on any additional kind of new projects.

Ceara Treacy OK, so you would encourage using the framework at the beginning of a development project?

CSA Exactly, yeah.

Ceara Treacy And then I suppose if there were any developers brought into the project then they would be introduced to the idea from the introduction as well.

CSA Yeah, but it also helps it to get the boundary or not the boundary but the basis of you know a privacy and security framework in place. You know to start developing an rather than it being an afterthought.

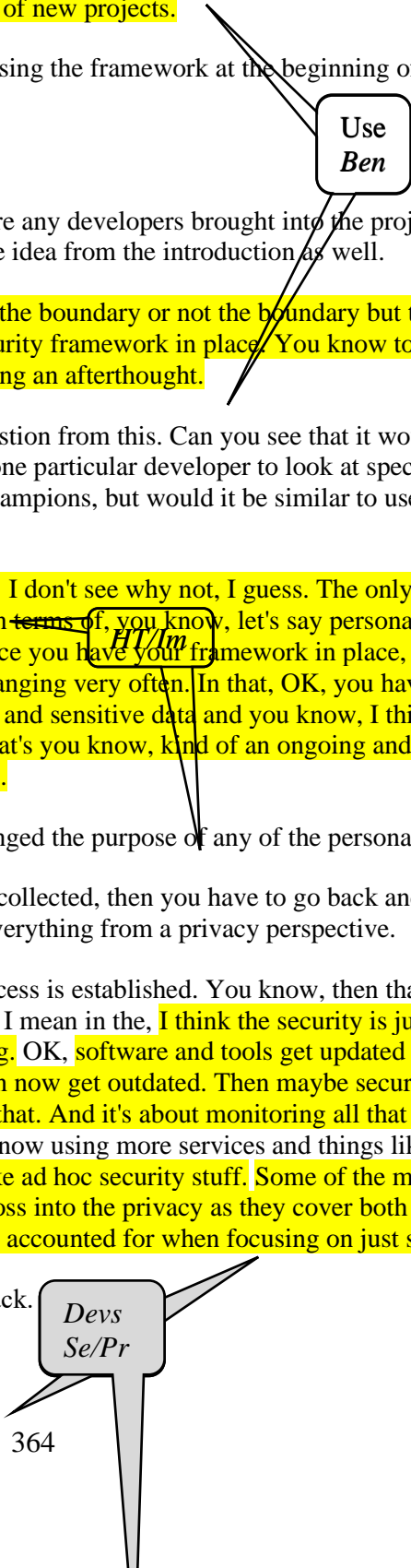
Ceara Treacy Excellent, great. One more question from this. Can you see that it would be beneficial possibly to appoint one particular developer to look at specifically like I know you use security champions, but would it be similar to use like a privacy champion?

CSA Yeah, yeah, I mean, I don't see. I don't see why not, I guess. The only thing is if we're talking about privacy in terms of, you know, let's say personal identifiable data you know. Once you have your framework in place, it's not something that you know is changing very often. In that, OK, you have your process for protecting Personal and sensitive data and you know, I think. Where security is something that's you know, kind of an ongoing and ongoing kind of chore, let's say.

Ceara Treacy Right? The fact that if you changed the purpose of any of the personal identifiable data that you have collected, then you have to go back and get consent again and re address everything from a privacy perspective.

CSA Exactly, yeah, so once that process is established. You know, then that's it is kind of covered off nearly. But I mean in the, I think the security is just a bit more, you know a moving thing. OK, software and tools get updated and you know the ones who might be on now get outdated. Then maybe security holes in it and patches and stuff like that. And it's about monitoring all that kind of stuff. And even with the cloud now using more services and things like that and there's, a lot more kinda like ad hoc security stuff. Some of the main properties of the framework cross into the privacy as they cover both security and privacy. So these would be accounted for when focusing on just security.

Ceara Treacy Yeah. That's interesting feedback.



Appendix G

- CSA Kind of like. Let's say ad hoc security stuff where you know they have the security champion, I think is you know more beneficial than a privacy champion, so to speak.
- Ceara Treacy So, you would see security as an ongoing concern, but once you have your system established and up and running, and has decided on the use of the personal data. Then it doesn't really change. But privacy does change with an added feature or change for use of the personal data.
- CSA Exactly, yeah, because we'll like we'll classify data and if anything gets added to that, it falls into the classification. And if it's classified as personal, identifiable data, it's going to be number one. It is going to be encrypted using field level encryption. And on the when it's stored in the database and all data will be transmitted over SSL over network board. That person identified data will also remain at field level encryption over the network as well, so there's always that extra layer but that process in place and anywhere that data goes. It follows that process. And whereas yet the security stuff is just a wee bit more hands on.
- Ceara Treacy OK, and then you've answered question 2.11 with previous feedback too.
- Th
HT/Im Provide the ability to filter the framework on a number of levels to allow or enable different classifications of threats specific to the type of product being developed.
- So would you suppose there was too little focus on the legal requirements in the framework?
- CSA Are you saying in the legal requirements in respect to GDPR?
- Ceara Treacy Yes.
- CSA Ah I don't think so, no. I guess and maybe that's the point, is that if we you know maybe the framework includes somewhere there and kind of regulations or whatever that you may be bound by in in other countries outside Europe.
- Gb
- Ceara Treacy Oh yeah, the framework just specifically looked at EU regulation. And but, yes, you're right. There is other regulation for example HIPAA and some other laws outside EU that I'm sure the framework could be adapted to.
- CSA Yeah, yeah. I think so because if we moved to the states working with personal data and medical data.
- Ceara Treacy The framework provides a lot of aspects that could actually be used for HIPAA. GDPR is more stringent for privacy, but HIPAA has different requirements. It's just distinguishing what those requirements are and applying them to this framework.
- CSA Yeah.

Appendix G

Ceara Treacy So we're done on the framework usability and then there's just like many of these questions have already been answered, so I'm not going over them again.

Is there is a particular step that you found easier to apply in the whole framework?

CSA I don't think so, no.

Use

Ceara Treacy Was there a particular step that was difficult?

U-

SD1 Probably working out which threats, there actually was.

CSA I mean, there's probably maybe just a wee bit more time consuming than difficult.

SD1 Yeah, well, probably.

Ceara Treacy Was there any particular part of the framework that you would single out as really great guidance and you felt made you very confident in doing it?

CSA Yeah. May contradict what SD1 said there, but the picking out the threats like you know, I thought it was just maybe more time consuming, but having the library helped.

Gu Ben

Yeah, yeah for sure. I think like because it would have been even more time consuming. I think if it wasn't there because you'd have to go look it up yourself. And then it would be where do you start with that.

Ceara Treacy And is there any step that you would really needs to have a considerable modification?

CSA Nothing comes to mind.

Ceara Treacy So, question 3.2 and again, we've gone over much of these through the feedback already given. All of these provide adequate information and regulatory requirements and provide enough information on implementing regular requirements and does framework need to identify which material? So yeah, we've answered all of those as well, and there are 3.3 is can you outline any deficiencies you've observed in the frameworks? Usability, and we've discussed that already about filtering and choosing the appropriate security and privacy controls. So are you in agreement with this?



CSA Yep.

U-Ob

Ceara Treacy A recap again, do you think there is in the body of knowledge in the framework that is too complex for inexperienced developers in data security and privacy risk assessment? Or it just takes awhile?

CSA Thing just well, yeah, I think it just takes awhile and maybe just a bit of help in googling to understand some of the language. Yeah, but apart from that it is all pretty much there

Appendix G

- Ceara Treacy OK, and is the framework organized or disorganized from your experience?
- CSA Yeah, it didn't really come across disorganized. Think everything was laid out pretty well.
- Ceara Treacy Great and there wasn't anything too difficult to understand at all. 
- CSA No.
- Ceara Treacy So, we've covered 3.4 as well. 
- We've talked about, technical document and videos. Would it be written as a technical document?
- We've discussed already and what the framework benefit from an accompanying tutorial. Yeah, we discussed that.
- So, is there anything else now that you would like to offer an opinion on about the framework before we bring the interview to a stop?
- CSA No, all go for me.
- SD1 Yeah no, I'm happy enough.
- SD2 No, I'm good with everything.
- Ceara Treacy Well, thank you very much guys for taking part in this focus group and for your commitment to implementing the framework.

Appendix H

Appendix H Framework

Please find a Copy of the Framework on the Accompanied USB in the Folder
FRAMEWORK

Appendix I

Appendix I Implemented Framework – STATSports

Please find a Copy of the Framework on the Accompanied USB in the Folder
IMPLEMENTED FRAMEWORK - STATSPORTS