Editorial Manager(tm) for Software Quality Journal
Manuscript Draft

Manuscript Number:

Title: Risk Management Capability Model (RMCM) for the Development of Medical Device Software

Article Type: Manuscript

Keywords: Software Risk Management; Software Quality; Software Engineering; Software Process Improvement; Software Reliability; Software Design; Computing Methodologies; Medical devices; United States Food and Drug Administration.

Corresponding Author: Dr Fergal Mc Caffery, DPhil, BSc, PGCUT

Corresponding Author's Institution: Lero - the Irish Software Research Centre

First Author: Fergal Mc Caffery, BSc, DPhil, PGCUT

Order of Authors: Fergal Mc Caffery, BSc, DPhil, PGCUT; John Burton, BSc; Ita Richardson, BSc, MSc, PhD, CPIM, CDipAF, MBCS, CEng

Risk Management Capability Model (RMCM) for the Development of Medical Device Software

Fergal Mc Caffery, John Burton & Ita Richardson
Lero – the Irish Software Engineering Research Centre
University of Limerick
Limerick, Ireland.
Email: fergal.mccaffery@lero.ie, john.burton@ul.ie, ita.richardson@ul.ie

Abstract.

Failure of medical device (MD) software can have potentially catastrophic effects, leading to injury of patients or even death. Therefore regulators penalise MD manufacturers who do not demonstrate that sufficient attention is devoted to the areas of hazard analysis and risk management (RM) throughout the software lifecycle.

This paper has two main objectives. The first objective is to compare how thorough current MD regulations are with relation to the Capability Maturity Model Integration (CMMI®) in specifying what RM practices MD companies should adopt when developing software. The second objective is to present a Risk Management Capability Model (RMCM) for the MD software industry, that is geared towards improving software quality, safety and reliability.

Our analysis indicates that 41 RM sub-practices would have to be performed in order to satisfy MD regulations and that only an additional 8 sub-practices would be required in order to satisfy all the CMMI® level 1 requirements. Additionally, MD companies satisfying the CMMI® goals of the RM process area by performing the CMMI® RM practices will not meet the requirements of the MD software RM regulations as an additional 20 MD specific sub-practices had to be added to meet the objectives of RMCM.

- **Keywords:** Software Risk Management, Software Quality, Software Engineering, Software Process Improvement, Software Reliability, Software Design, Computing Methodologies, Medical devices, United States Food and Drug Administration.

1.

1. Introduction

Software is becoming an increasingly important aspect of medical devices and MD regulation. Software enables highly complex systems to be built. However, complexity is the enemy of safety (McDermid 1993), therefore strict adherence to well documented processes is important within the domain of MD software. Medical devices can only be marketed if compliance and approval from the appropriate regulatory bodies of the Food and Drug Administration (FDA) (FDA/CDRH 2005, FDA Regulations 2006, FDA/CDRH 1999) (US requirement), and the European Commission under its Medical Device Directives (MDD) (European Council 1993) (CE marking requirement) is achieved. MD companies must produce a design history file detailing the software components and processes undertaken in the development of their products. Due to the safety-critical nature of MD software it is important that a highly efficient RM process is in place within MD companies. The risk of patient injury from software defects is a concern due to the manufacture and deployment of increasing numbers of software-embedded devices (Bassen et. al. 1985, Crumpler & Rudolph 1997, Munsey 1995, US General Accounting Office 1997). There have been a number of major MD product recalls over this past 25 years that were the result of software defects (Bovee et. al. 2001). For example, four people died and two were left permanently disfigured from massive radiation overdoses due to software defects in the Therac-25 line of medical linear accelerators (Leveson & Turner 2001). A major contributor to such defects is the presence of software quality assurance issues (Bassen et. al. 1985). The CDRH reviewed MD recalls due to software failures from 1983 to 1991 and estimated that 90% were due to inadequate design and 19% were caused by inadequate change control (US Department of Health and Human Services 1992). Therefore, to reduce the risk of failure it is important that the software design process includes efficient RM practices.

Software quality may be defined and measured in many ways. For MD companies, one way to define and measure software quality is in terms of the risk of software-containing devices in exposing patients, operators, bystanders, service personnel or the environment to hazards. Although such devices are developed to increase the well-being of patients, on occasion they fail to operate properly, or are misused in ways that are associated with injuries and death (Rados 2003). According to the Institute of Medicine report ‘To Err is Human’ (Kohn et. al. 2000), between 44000 to 98000 people die throughout the world in hospital from preventative medical errors. The

report also says that more people die every year as a result of medical errors than from motor vehicle accidents, breast cancer or AIDS.

MD companies are responsible for ensuring that they take adequate precautions to produce safe and effective software that does not pose a severe hazard should a software-related failure occur. Therefore, MD companies who market within the USA must ensure that they comply with the regulations for medical devices outlined by the FDA. They must also be able to produce sufficient evidence to support this compliance. The FDA "is responsible for protecting the public health by assuring the safety, efficiency, and security of…medical devices…" (FDA's Mission Statement 2007). To this end, the Center for Devices and Radiological Health (CDRH) has published guidance papers for industry and MD staff which include risk-based activities to be performed during software validation (FDA/CDRH 1999), pre-market submission (FDA/CDRH 2005) and when using off-the-shelf (OTS) software in a MD (FDA Regulations 2006). Although the CDRH guidance documents provide information on which software activities should be performed, including risk based activities, they do not enforce any specific method for performing these activities.

Within the MD industry, several predominant standards have emerged for performing risk-based activities including: ANSI/AAMI/ISO:14971 (ISO:14971), (ANSI/AAMI/ISO:14971 2007) and ANSI/AAMI:SW68 (SW68) (ANSI/AAMI 2001) and more recently ANSI/AAMI/IEC:62304 (IEC:62304) (ANSI/AAMI/IEC 2006) which is based on SW68 and aims to both improve upon and replace SW68. Previous research has asserted that both ISO:14971 and SW68 require that RM activities include software, without providing any detail on how it should be done (AAMI 2005, AAMI 2004). In 2005, the Association for the Advancement of Medical Instrumentation (AAMI) produced a Technical Information Report (TIR32) (AAMI 2004) on performing risk based activities in accordance with ISO:14971 to help rectify this situation. The report focuses on "software system safety design issues" and provides insight into the key concepts behind performing various risk-based activities. It also highlights many of the pitfalls associated with RM activities. However, TIR32 does all this without committing to specific methods or documentation requirements when performing the various activities. It clearly states that it "does not define any specific documentation requirements". Likewise, the International Society for Pharmaceutical Engineering (ISPE), published a guide, GAMP 4 (ISPE 2001), which included guidance

1.

for performing validation of software systems and risk-based activities. The guide provides many of the RM high-level concepts with some detail and practical examples. It falls short in that it does not cover all the requirements necessary to achieve full compliance in the area of RM.

None of the standards or guides produced provide a one-stop-shop for MD software risk based activities making it harder for MD companies to quickly measure their capability with respect to software RM. Although IEC:62304 acknowledges that risk is very well addressed in ISO:14971, it points out that there is a need for additional RM requirements to address software specific requirements. IEC:62304 addresses these additional requirements but does so in the context of ISO:14971. It is only through a combining the various standards that one may gain a complete picture of what is required for software RM.

This paper outlines a proposed RMCM for use by MD companies to assist them in producing safe and effective software. It seeks to extract, interpret and combine the disparate knowledge within the MD industry and associated standards. It does so in the context of the following regulations: ISO:14971, IEC:62304, TIR32, BS/EN:60601-1-4 (BS/EN 2000) and GAMP 4, in addition to the CDRH (FDA specific) guidance documents.

Section 2 examines the need for the RMCM and how similar software process improvement (SPI) based models have been used within other safety-critical software industries. Section 3 presents an overview of the RMCM. Section 4 describes the development of the RMCM. Section 5 details the mappings that were performed between the MD regulations and the CMMI® (SEI 2006) for RM. This section describes the content of the RMCM including the capability level structure. It details what additional practices had to be added to the CMMI® RM process area in order to satisfy MD regulations, as well as what CMMI® practices are not required in order to satisfy basic MD regulatory requirements. Commentary is supplied indicating how the RM process adopted by MD companies could benefit by incorporating CMMI® practices that are not deemed necessary by MD regulations. Section 6 details a summary of the results from the research. Finally, section 7 contains our conclusions.

2. Background and the contribution of this research

MD companies have to adhere to MD regulations in relation to RM. The main area of concern for MD companies in relation to RM is to ensure that the RM elements

required by the FDA are in place rather than trying to improve their overall RM practices. The majority of the literature available on MD RM discusses RM from a high level perspective where some of the key concepts of RM are discussed (Wood 1999, Schmuland 2005, Elahi 1993) and the FDA's role in the regulation of MD software is examined (Rados 2003, Rudolph 2003, Kim 1993, Theisen & Neill 2004, Ciarkowski 2000, Munzer 1988). The literature's focus is on what is and what can be done by the FDA to prevent MD manufacturers from releasing un-safe medical devices.

Much has been done in the area of user-centred design (Johnson et. al. 2005) and how poor user interface design can render software applications unusable or lead to incorrect diagnosis of patients due to missing or incorrect information that is important to the diagnosis of the patient (Bates et. al. 1999, Tang & Patel 1994, Tierney et. al. 1987). In fact, the FDA views this as a critical issue (Sawyer et. al. 1996) and has produced a guide specifically aimed at addressing human interface concerns through the design process (FDA/CDRH 2000). Through such guidance it is hoped that the design of software will be driven by safety conscious decisions and consideration for potential human misinterpretation of results and misuse or abuse of the system, thus leading to safer software. The consideration of how software may potentially be used or misused is one of several important practices required for any software RM model.

Other literature has focussed on the progression of the FDA in the regulation of MD software (Kim 1993, Eagles & Murray 2001). This literature is interesting in that it presents the progression of key standards aimed at the MD sector from the perspective of the FDA. It provides a good insight into the evolution of standards and establishes a number of core standards within MD RM.

Wallace and Kuhn have conducted research into the reasons why MD software fails or has been recalled by the FDA (Wallace & Kuhn 2001). The research analyses over 15 years of recall data and discusses how the majority of MD errors are preventative by providing examples of prevention and detection techniques. The research does not directly discuss hazard analysis and RM but is useful in that it does discuss many of the techniques which are associated with risk mitigation such as inspections and reviews, traceability, code reviews, use of simulations, unit testing and interface testing. Through the examination of re-call data, the researchers provided some lessons into why MD software fails and how these failures can be prevented.

1.

Other research has been conducted into formal techniques for quantifying reliability of MD software and analysing risks associated with the devices (Voas et. al. 1993, Sayre et. al. 2001). Again, this research is seen as complimentary to analysing MD software and producing safer software but is not, and does not claim to be, a complete replacement for existing RM practices.

The MD industry itself has identified the requirement for a guide and for practical examples for performing relevant MD software practices including RM. GAMP 4 details RM practices that MD companies may adopt in order to comply with MD regulations. However, no standards exist within the MD domain in relation to how such practices could be improved by incorporating practices from formal software engineering SPI models for RM. Previous research has investigated the suitability of using existing software quality assurance standards in order to achieve FDA compliance related to the areas of process management, requirements specification, design control and change control (Bovee et. al. 2001). However, the area of RM was not investigated and no specific SPI model has been developed for the industry.

If we investigate other regulated industries such as the automotive and space industries we realise that these domains are not content with satisfying regulatory standards. Instead, they have proactively developed SPI models specifically for their domain so that they may continuously improve the development of their information systems to achieve higher levels of safety, greater efficiency, and a faster time to market, whilst seamlessly satisfying regulatory quality requirements. The major SPI models that currently exist, namely ISO/IEC:15504 (ISO/IEC 2003) and CMMI®, do not address the regulatory requirements of either the MD, automotive or space industries. Therefore, a new SPI model was developed specifically for the automotive industry. This model was based upon ISO/IEC:15504 and is referred to as Automotive Spice (Automotive SIG 2005). Likewise, a new ISO/IEC:15504 based SPI model was developed specifically for the space industry - this model is known as SPiCE for SPACE (Cass & Volcker 2000). Both of these models contain reference and assessment information in relation to how companies may improve their RM practices within their domain.

This paper will not address the issue of developing an entire SPI model for the MD industry (a high-level structure for such a model is discussed in (Mc Caffery et. al. 2005, Mc Caffery & Coleman 2007)), but shall instead focus upon the individual

process area of RM (this research extends the research presented in (Mc Caffery et. al. 2005, Burton et. al. 2006)). This work develops a SPI model for RM within the MD industry, providing an opportunity to integrate the regulatory issues and SPI mechanisms to achieve improvements that are critical to the RM of software for medical devices.

3. Overview of the RMCM

The RMCM outlined in this paper was developed following an extensive literature review and input from a MD company. The primary focus of the research area as a whole is to investigate if the MD regulations for RM may be improved through adopting disciplined software engineering practices. This paper describes an integral part of this research by detailing the development of a RMCM that is based upon a formal SPI model. Upon development, the RMCM will be an extension of the RM process area within the CMMI®. This is specifically tailored to fulfil the RM regulations of the MD software industry. The RMCM may then be adopted by MD companies to improve their software development practices by providing them with a SPI model. This SPI model will also ensure that their hazard analysis and risk control procedures satisfy the current MD regulations and guidelines.

4. The Development of the RMCM

The RMCM was developed with assistance from a MD company who is bound legally by the regulatory bodies of the British Standards Institution (BSI) and the FDA (FDA/CDRH 2002). The regulatory bodies regularly review this organisation's process and procedures, through audits, to ensure the organisation is compliant with the regulations set out by the bodies. Therefore, the organisation possessed a solid base of documented process and audit feedback.

The organisation requested that a model should be created with a comprehensive and reusable software hazard analysis and RM procedure. It was a requirement that the procedures should fully comply with the RM requirements set forth by both the FDA and BSI. It was envisaged that this would lead to safer and more efficient software design and developed device. It was also desirable that the resulting RM framework would satisfy the regulatory requirements of other regulatory bodies (if applicable). Therefore, the focus and content of the resulting framework could not be restricted to just FDA and BSI guidance documents.

1.

In order to understand and define the scope of the RMCM, it was important that the authors gained both a broad and deep understanding of the concepts of RM in both the MD domain and the software engineering community. The approach adopted was to perform an extensive literature review of existing regulatory guidance papers, industry guidance papers and standards which govern the MD software industry as well as SPI models from other industry sectors. This in turn provided a solid and proven foundation upon which the model could be based.

4.1. Structure of RMCM

The RMCM does not dictate a software lifecycle model. It assumes the existence of software phases common to industry standard lifecycle models. The phases include requirements management, design and development, verification and validation, release, maintenance and post production. Neither quality nor safety can be integrated into software as a final step in the software development process. MD companies must take an approach which integrates hazard management and risk analysis into the entire software lifecycle. This should begin at the requirements phase and continue through to product retirement. The approach taken must clearly demonstrate that serious consideration was given to all possible hazards posed by MD software. It must put in place appropriate risk reduction and mitigation techniques.

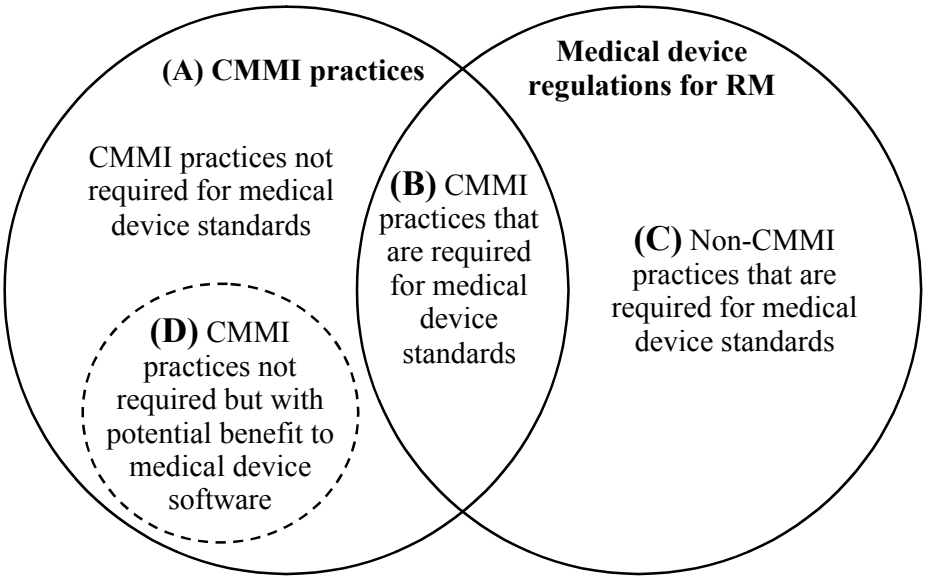
The RMCM has been designed to be flexible in that relevant elements of the model may be adopted as required to provide the most significant benefit to the business. The model is based on the CMMI® and the regulations used to extend the CMMI® framework are those of the FDA, ISO:14971, GAMP 4 and the ANSI/AAMI/IEC:62304 standard (IEC:62304) (MD software – Software life cycle processes) (ANSI/AAMI/IEC 2006). EN 6061-1-4 (BS EN 2000) was also considered for the RMCM, to establish if there was additional knowledge within the standard which would complement the model. Such information has been highlighted by the authors during the discussion of the models sub-practices in the subsequent sections.

The RMCM contains an assessment method that provides a means of assessing the software engineering capability for the RM process area in relation to MD software (both application and embedded software). The RMCM is being developed as a foundation upon which to promote SPI practices into the RM process adopted by MD companies. This is an attempt to improve the effectiveness and efficiency of RM within MD companies through investigating the mapping of MD regulatory guidelines against

2.

the CMMI® RM process area. The mappings between the MD regulatory guidelines and the CMMI® specific practices for the RM process result in the RMCM being composed of a number of goals and practices. Goals and practices may be either generic (relating to the entire organisation) or specific (relating directly to the RM process). The RMCM determines what parts of the CMMI® RM process area (i.e. part A of Figure 1) are required to satisfy MD regulations (i.e. part B of Figure 1).

The RMCM also investigates the possibility of extending the CMMI® process areas with additional practices that are outside the remit of CMMI®, but are required in order to satisfy MD regulatory guidelines (i.e. part C of Figure 1). Additionally, the RMCM provides MD companies with the opportunity to incorporate practices from the CMMI® that are not required in order to achieve regulatory compliance but that would greatly enhance their RM process if they were included (i.e. part D of Figure 1).



A- CMMI® Practices that are not mandatory for MD standards.
B- CMMI® Practices that are required for MD standards.
C- Non-CMMI® Practices that are required for MD standards.
D- CMMI® Practices that are not mandatory for MD standards – but if performed could contribute to the safety of the MD software or enhance the company's RM practices

Figure 1. Composition of the RMCM.

RMCM will help companies to measure their organisational RM capability and to track their progression against the following SPI capability levels:

1.

- **RMCM Level Med** – Companies must demonstrate that they satisfy the goals and perform the practices required to meet the requirements of the various MD regulatory guidelines and standards associated with RM. This will involve performing some practices, which the CMMI® views as generic, although not to the extent of fulfilling any generic goals.
- **RMCM Level 0** – Insufficient practices have been performed to satisfy the requirements of Level Med.
- **RMCM Level 1** - Companies must demonstrate that they satisfy RMCM level Med and the CMMI® capability level 1 goal of performing the CMMI® RM base practices.
- **RMCM Level 2** – Companies must demonstrate that they satisfy RMCM level 1 and additionally perform CMMI® RM Advanced Practices, as well as the CMMI® capability level 2 generic goal of institutionalising a Managed Process.
- **RMCM Level 3** - Companies must demonstrate that they satisfy RMCM level 2 and additionally the CMMI® Generic Goal to Institutionalise a Defined Process (CMMI® Generic Goal 3) for the RM process area.
- **RMCM Level 4** – Companies must demonstrate that they satisfy RMCM level 3 and additionally the CMMI® Generic Goal to Institutionalise a Quantitatively Managed Process (CMMI® Generic Goal 4) for the RM process area.
- **RMCM Level 5** - Companies must demonstrate that a process area satisfies RMCM level 4 and additionally the CMMI® Generic Goal to Institutionalise an Optimising Process (CMMI® Generic Goal 5) for the RM process area.

Section 5 details a mapping of the MD standards and guidelines (these shall be referred to as MD regulations throughout the paper) to the CMMI® for the RMCM. This will demonstrate what CMMI® goals and practices are required in order to satisfy MD regulations for RM. Software development within MD companies could be improved by incorporating other CMMI® practices that are not required to achieve MD compliance. Details are provided in relation to how additional sub-practices (not included in the CMMI®) may be added where necessary to satisfy MD regulatory guidelines. RM goals and practices have to be performed to satisfy each of the RMCM capability levels.

2.

5. RMCM Goals, Practices and Sub-practices

In this section we identify the goals that exist within the RMCM. Tables will be used to illustrate the complete list of the RMCM practices and sub-practices for a particular goal. The tables also specify the RMCM capability level associated with each sub-practice. Sub-practices that are displayed in bold italics in the tables are not present in the CMMI® but are required in order to fulfil MD regulatory requirements.

The RM process area has three specific goals (SG):

- **SG1: Prepare for RM**
- **SG2: Identify and Analyse Risks**
- **SG3: Mitigate Risks**.

For each of these goals to be achieved, it is necessary for a number of specific practices (SP) to be performed.

5.1. SG1: Prepare for RM

In order to fulfil **SG1: Prepare for RM** the specific practices of *Determine Risk Sources and Categories*; *Define Risk Parameters*; and *Establish a RM Strategy* must be performed. (For a more complete description of these sub-practices please refer to the RM process area section within the CMMI® (SEI 2006)). Table 1 provides the complete list of the RMCM sub-practices and their associated capability level for preparing for RM.

Table 1. RMCM Sub-practices for Specific Goal 1 Preparing for RM

RMCM Sub-Practice Number	Sub-Practice	Source	RMCM Level
Practice: Determine Risk Sources and Categories			
1	Determine risk sources	CMMI RM SP1.1-1 sub-practice 1, ISO:14971 4.2, IEC:62304 7.1.1 & 7.1.2	Med
2	Determine risk categories	CMMI SP1.1-1 sub-practice 2	Med
3	***Determine software hazards***	***IEC:62304 7.1, ISO:14971 4.3 and CDRH***	***Med***
4	***Include failure in the OTS software as a potential hazard***	***IEC:62304 7.1.2 (c) & 7.1.3***	***Med***
5	***Include hardware failures as a potential hazard***	***IEC:62304 7.1.2 (d)***	***Med***
Practice: Define Risk Parameters			
6	Define consistent criteria for evaluating and quantifying risk likelihood and severity levels	CMMI RM SP1.2-1 sub-practice 1, IEC:62304 4.3, ISO:14971 4.4	Med
7	Define thresholds for each risk category	CMMI RM SP1.2-1 sub-practice 2, ISO:14971 D.3.2	Med
8	Define bounds on the extent to which thresholds are applied against or within a category	CMMI RM SP1.2-1 sub-practice 3, ISO:14971 D.3.3	Med
Practice: Establish a RM Strategy			

1.

9	Establish a RM Strategy	CMMI RM SP1.3-1, IEC:62304 5.1.7, ISO:14971 3.1	Med
10	***Define the scope of the strategy and include those life-cycle phases for which the strategy is applicable***	***ISO:14971 3.4(a)***	***Med***
11	***Define the policy for determining acceptable risks***	***ISO:14971 3.4(d)***	***Med***
12	***Include a verification plan and activities as part of the strategy***	***ISO:14971 3.4(e) and 6.3***	***Med***
13	***Outline the allocation of responsibilities***	***ISO:14971 3.4(b)***	***Med***
14	***Outline the requirements for reviewing the RM activities***	***ISO:14971 3.4(c)***	***Med***
15	***The RM strategy should include OTS***	***IEC:62304 7.1.3***	***Med***
16	***Post-production queries and bugs be should analysed***	***ISO:14971 9, IEC:62304 9.2(b) and CDRH***	***Med***

Table 2 summaries the mapping of the MD RM regulations against specific goal 1 of the CMMI® RM process area (**Prepare for RM**). It may be observed that 10 MD specific sub-practices will have to be performed in addition to all the CMMI® RM practices and sub-practices in order to satisfy the MD guidelines of this goal. However, the CMMI® specific goal 1 for RM would be fully satisfied by following guidelines required to adhere to MD regulations.

Table 2: Summary of RMCM Specific Goal 1 – Prepare for RM

Practice	**RMCM Sub-Practice Numbers**	**CMMI® Sub-practices**	**CMMI® Sub-practices required to meet regulatory requirements**	**Additional Sub-practices required to meet regulatory requirements**
Determine Risk Sources & Categories	1 – 5	2	2	3
Define Risk Parameters	6 – 8	3	3	0
Establish RM process	9 –16	1	1	7
Total	**1 - 16**	**6**	**6**	**10**

5.1.1. Determine risk sources & categories

Table 2 illustrates that the RMCM practice for determining risk sources and categories items consists of 2 sub-practices that are required by both the CMMI® and the MD regulations (i.e. Level Med in table 1), plus 3 new sub-practices that are required by the MD regulations but not by the CMMI® (i.e. Level ***Med*** in table 1).

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 1): Sub-practices 1 & 2.* Determining the potential sources of risk and categorising them as activities that are required by both the CMMI® and the MD guidelines (see table 1).

2.

However, the MD regulations require additional information in relation to factors that could result in software hazards. FDA guidelines recommend focusing upon safety as a primary source of risk. Other typical sources of risk that the MD guidelines recommend focusing upon are: cost, integrity and security. FDA guidelines also note that risk may be initiated by human factors, hardware faults, software faults, integration errors and environmental conditions. MD guidelines also recommend that all potential causes and sequences of events that could result in a hazard should be documented.

Risks should be organised into related groups as this will assist with consolidating sub-practices in risk mitigation plans. A number of factors may be considered when determining risk categories. FDA guidelines advise similar factors to those recommended by the CMMI®, such as categorising risk for an entity, as well as for major components, subsystems, software, electronics and lifecycle stages. For example, FDA regulations stress that it is important to define risk-related functions when analysing requirements and to monitor this ongoing source of risk throughout the lifecycle process as requirements change. Additionally, IEC:62304 specifies that each safety requirement in the software be uniquely identifiable and traceable to risk mitigation measures (see section 5.2.1).

Sub-practices required by the MD regulations but NOT by the CMMI® *(see Table 1)**:***

Three additional MD specific sub-practices as defined in IEC:62304 were added in order to provide full coverage of the MD regulations. These are as follows:

Sub-practice 3. The MD regulations identify hazard management as part of RM and request that hazards should be identified that could be the direct result of software failure or for which software implements a control measure. Hazards should be identified from both normal and incorrect use of the software device and should be considered for patients, operators, service personnel, bystanders and the environment. EN 60601-1-4 recommends that the method used for hazard identification should be documented in the RM file (IEC 1985).

Sub-practice 4. The MD regulations specify that OTS (Off-The-Shelf) software must be considered as a potential source for failure of MD software. IEC:62304 specifically requires that where software of unknown provenance (SOUP) is used in the MD software, that any published SOUP anomaly list be evaluated to determine if any new hazards could be introduced as a result of the known anomalies.

1.

Sub-practice 5. The MD regulations detail that hardware failures should be considered as a potential source of software failures.

5.1.2. Define risk parameters

Table 2 illustrates that the RMCM practice for defining risk parameters consists of 3 sub-practices that are required by both the CMMI® and the MD regulations. Therefore the MD guidelines demand similar effort and rigour to those demanded by CMMI® and a company satisfying MD regulations would also satisfy the specific practice for defining risk parameters.

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 1)**:***

Sub-Practice 6. It is important to identify criteria that may be used for comparing risks and enabling risks to be prioritised. ISO:14971 guidelines identify parameters for the severity of harm (should the risk occur) and the likelihood of the occurrence for quantifying risk. These criteria may be acceptable in the instance where a hardware failure may lead to a corresponding software failure and the likelihood can be reasonably estimated. However, IEC:62304, states that for software, if a hazard could arise from the failure of the software, the probably of such a failure shall be assumed to be 100 percent. Software safety is broken into three classes A, B and C. Class A represents a software item where failure would not result in injury or damage to health, B could result in non-serious injury and C could result in death or serious injury. All software items are assigned a classification and all software items within a system are assumed to inherit the system's safety class until they themselves have been evaluated. Any unclassified software items assume a class level C. Many of the software lifecycle activities and associated tasks within IEC:62304 are directly linked to these software classifications.

Sub-Practice 7. The MD company must define thresholds against which all identified risks shall be measured.

Sub-Practice 8. In terms of developing software for medical devices the parameter values for 'severity of harm' are very important and are defined and justified by the sponsor. The degree of detail and effort involved in RM and control should be in line with the 'severity of the resulting consequences' (should failure happen). Therefore most effort should be devoted to handling risks that have a 'severity of harm' level of major (Class C). As safety is of primary importance companies must ensure that

2.

medical devices are produced that satisfy acceptable levels of risk and that this is not based upon probability.

5.1.3. Establish RM strategy

Table 2 illustrates that the MD regulations are more stringent in terms of what constitutes a RM strategy and therefore additional sub-practices (other than those detailed in the CMMI®) will have be included within this practice in order to fulfil the objectives of RMCM. For example, the FDA guidelines specify that a strategy should include: *potential sources of risk; appropriate techniques for risk analysis of software, electronics, biomaterials etc., such as fault tree analysis, failure modes and effects analysis; risk criteria, parameters and thresholds; risk control methods; & activities used to monitor the risks and whether risk controls were successful* (FDA Regulations 2006). Table 1 demonstrates that the RMCM practice for establishing a RM strategy consists of one sub-practice that is required by both the CMMI® and the MD regulations (i.e. Level Med), and 7 sub-practices that are required by the MD regulations but not by the CMMI® (i.e. Level ***Med***).

Sub-practice required by BOTH the CMMI® and the MD regulations *(see Table 1)**:***

Sub-Practice 9. Establishing a RM strategy involves establishing and maintaining a strategy to be used for RM. Both CMMI® and the FDA require companies to have a RM strategy that is used to define risk analysis and control activities, which should be documented. EN 60601-1-4 adds that if the plan/strategy changes during the course of development, a record of the changes shall be kept. MD guidelines require that a RM strategy is adopted and request that MD manufacturers document: an analysis of intended use of MD and software, a description of each identified risk; the severity level of the risk; the source of the risk; the risk control methods used and how they were implemented; tests used to confirm the success of the risk method used; and the severity level after the risk control method has been implemented.

Sub-practices required by the MD regulations but NOT by the CMMI *(see Table 1)**:***

Sub-Practice 10. To satisfy ISO:14971, the life-cycle phases for which the RM plan is applicable, should be identified and described within the plan.

Sub-Practice 11. To satisfy ISO:14971, before a risk is deemed acceptable, it must be measured against a pre-defined acceptability policy, which should be outlined by the

1.

RM plan. MD standards do not define acceptable levels and instead leave the decision to the MD manufacturer, who in turn must document their decision using existing standards, comparable levels of risk from devices in use, medical references and clinical study references where available.

Sub-Practice 12. To satisfy ISO:14971, the verification plan and activities should be included as part of the RM plan.

Sub-Practice 13. To satisfy ISO:14971, those responsible for the various RM and control activities should also be identified.

Sub-Practice 14. To satisfy ISO:14971, the plan should also cover the requirements for reviewing the RM activities.

Sub-Practice 15. To satisfy IEC:62304, the RM plan should cover (Off-the-shelf) OTS software.

Sub-Practice 16. ISO:14971, IEC:62304 and the FDA guidelines recommend that post-production queries and bugs should be analysed to safeguard against a risk scenario arising post-release that was not originally considered during development.

5.2. SG2: Identify and Analyse Risks

In order to fulfil SG2: **Identify and Analyse Risks** the following specific practices have to be performed: *Identify risks; & Evaluate, categorise, and Prioritise risks (see Table 3).*

Table 3: RMCM Sub-practices for Specific Goal 2 : Identifying and Analysing Risks

RMCM Sub-Practice Number	Sub-Practice	Source	RMCM Level
Practice: Identify risks			
17	***Include a description of the intended use and any foreseeable misuse***	***ISO: 14971 4.2***	***Med***
18	Identify the risks associated with the cost, schedule, and performance in all appropriate product lifecycle phases	CMMI RM SP2.1-1 sub-practice 1	1
19	Review environmental elements that may impact the project	CMMI RM SP2.1-1 sub-practice 2	1
20	Review all elements of the work breakdown structure as part of identifying risks to help ensure that all aspects of the work effort have been considered	CMMI RM SP2.1-1 sub-practice 3	1
21	Review all elements of the project plan as part of identifying risks to help ensure that all aspects of the project have been considered	CMMI RM SP2.1-1 sub-practice 4	1
22	Document the context, conditions, and potential consequences of the risk	CMMI RM SP2.1-1 sub-practice 5, ISO:14971 4.4	Med
23	***Provide risk traceability: Identify risk traceability from the device level down to the specific cause within the software***	***IEC:62304 7.3.3, ISO: 14971 3.5 and CDRH***	***Med***
24	Identify the relevant stakeholders associated with each risk	CMMI RM SP2.1-1 sub-practice 6	1

2.

25	***At least one trained individual directly involved in the software development, with both relevant MD and RM knowledge shall participate in the RM activity to ensure that risks are adequately addressed. This person(s) shall be identified on the report along with the date of the analysis***	***ISO: 14971 3.2, 3.3 and 3.4(b)***	***Med***
Practice: Evaluate, categorise, and prioritise risks			
26	Evaluate the identified risks using the defined risk parameters	CMMI RM SP2.2-1 sub-practice 1, ISO:14971 5	Med
27	Categorise and group risks according to the defined risk categories	CMMI RM SP2.2-1 sub-practice 2, ISO:14971 5	Med
28	Prioritise risks for mitigation	CMMI RM SP2.2-1 sub-practice 3, ISO:14971 5	Med
29	***The results of all the RM activities should be recorded and maintained in a RM file***	***ISO: 14971 3.1***	***Med***

Table 4 summaries the mapping of the MD RM regulations against specific goal 2 **(Identify and Analyse Risks)** of the CMMI® RM process area. It may be observed that in order to satisfy the MD regulations that not all of sub-practices of this CMMI® goal will have to be performed. However, in order to satisfy the objectives of the RMCM 4 additional sub-practices had to be added (Table 3). Table 3 also illustrates that specific goal 2 of the CMMI® will not be satisfied by following the MD regulations (i.e. performing only the RMCM level Med sub-practices) as only 4 of the 9 CMMI® sub-practices associated with this CMMI® goal are required for RMCM level Med.

Table 4: Summary of RMCM Specific Goal 2 – Identify and Analyse Risks

Practice	**RMCM Sub-Practice Numbers**	**CMMI® Sub-practices**	**CMMI® Sub-practices required to meet regulatory requirements**	**Additional Sub-practices required to meet regulatory requirements**
Identify Risks	17 - 25	6	1	3
Evaluate, categorise and prioritise risks	26 - 29	3	3	1
Total	**17 - 29**	**9**	**4**	**4**

5.2.1. Identify risks

Table 3 includes the complete list of RMCM sub-practices for identifying risks. From mapping the MD regulations against the CMMI® for identifying risks, it was discovered that unlike the specific goal 1 practices, not all of the CMMI® sub-practices are required in order to achieve MD compliance (i.e. 5 of the 6 CMMI® sub-practices are at level 1). However, the MD regulations request additional information in relation to usage, traceability and the participation of a software development team member in the RM activity. Therefore, additional MD specific sub-practices are required in order to achieve the objectives of the RMCM. Table 4 illustrates that the RMCM practice for

1.

identifying risks consists of 1 sub-practice that is required by both the CMMI® and the MD regulations (i.e. Level Med), 3 sub-practices that are required by the MD regulations but not by the CMMI (i.e. Level ***Med***), and 5 sub-practices that are required by the CMMI® but not by the MD regulations (i.e. Level 1).

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 3):*
Sub-Practice 22. Identified risks should be documented. However prior to identifying the risks, ISO:14971 requires all characteristics that could affect safety to be documented. The acceptable level of residual risk will depend upon the intended purpose of the MD. The documentation should include a description of the identified risk (details of the context and conditions) and the severity of the risk (potential consequences) should it occur.

Sub-practices required by the MD regulations but NOT by the CMMI *(see Table 3):*
Sub-Practice 17. To satisfy ISO14971, MD companies should assess the effect the risk will have upon patients, operators, bystanders, service personnel and the environment.
Sub-Practice 23. ISO:14971, IEC:62304 and the FDA guidelines recommend that, as development progresses through the software development lifecycle, the status of existing risks should be updated and new risks should be identified. Risks should be identified for all predictable instances and follow established procedures, starting at the requirements stage of the lifecycle. MD regulations also request that the documentation should identify traceability from the device level down to the specific cause in the software and also provide traceability from the risk analysis, evaluation, implementation, and verification down to the final assessment of the acceptability of residual risks.

Sub-Practice 25. ISO:14971 specifies management must provide an adequate provision of qualified resources. Those performing risk analysis should possess knowledge and experience of the MD, its intended use and RM techniques. Additionally, records of these qualifications should be maintained for future compliance inspection. The risk report should contain the identity of the person and organization that carried out the risk analysis along with the date of the analysis. The IEC:62304 and ISO:14971 requirements are not as comprehensive as CMMI® as they do not specify that each risk

2.

is assigned an owner. Therefore, a separate sub-practice is added to RMCM to reflect both IEC:62304 and ISO:14971 guidelines.

Sub-practices required by the CMMI® but NOT by the MD regulations *(see Table 3)**:***

Sub-Practice 18. Many factors that contribute to risk such as cost, integrity, security and safety should be considered.

Sub-Practice 19. In addition to identifying software related issues, risks should also be identified for hardware faults and integration issues. The CMMI® acknowledges that it is important to review areas that are outside the scope of the project for risks.

Sub-Practices 20&21. The CMMI® requires that all elements of both the work breakdown structure and the project plan should be reviewed to ensure that all aspects of the work effort and project are considered. There is no necessity to review the work breakdown structure and the project plan in order to achieve MD compliance for RM.

Sub-Practices 24. The CMMI® requires that stakeholders should be associated with each risk so that individuals are assigned responsibility for risks. However, this is not necessary for MD regulatory compliance.

5.2.2. Evaluate, categorise, prioritise risks

Table 3 includes the complete list of RMCM sub-practices and associated capability levels for evaluating, categorising and prioritising risks. From mapping the MD regulations against the CMMI® for this practice, we noted that the MD regulatory requirements exceed those of the CMMI®, as ISO:14971 additionally requests that the results of all the RM sub-practices should be recorded and maintained in a RM file. Therefore, in order to fulfil the objectives of the RMCM one extra sub-practice is required in addition to those demanded by CMMI® (see table 3). A company fulfilling MD regulations would also satisfy the CMMI® requirements for this practice. Table 3 illustrates that the RMCM practice for evaluating, categorising and prioritising risks consists of 3 sub-practices that are required by both the CMMI® and the MD regulations (i.e. Level Med), and 1 sub-practice that is required by the MD regulations but not by the CMMI® (i.e. Level ***Med***).

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 3):*

Sub-Practice 26. Parameters defined in the RM strategy are used to evaluate identified risks. MD companies adhering to FDA guidelines are required to determine risk using

the parameters of "severity of harm" (should the risk occur) and the "likelihood of occurrence". Emphasis is placed on the "severity of harm" parameter, as it may not always be possible to accurately estimate the software failure rate (which is directly related to the "likelihood of occurrence" parameter).

Sub-Practice 27. There is a necessity to group risks according to defined risk categories (e.g. entity, components/subsystems, software etc.) to assist risk handling.

Sub-Practice 28. As a project may have multiple risks, it is important that risks are prioritised so that the highest priority risks receive the most attention and effort. MD guidelines specify that risks should be prioritised according to the severity of the resulting consequences and that the amount of effort devoted to creating design solutions that reduce or eliminate the risk should be based upon the value of this parameter. GAMP 4 combines the risk classification with the probability of detection to further prioritise the risk. The probability of detection is broken out into three levels: "low" where the detection of the fault condition is perceived to be unlikely, "medium" where detection is reasonably likely and "high" where detection of the fault is very likely. The logic is that risks that are not easily detected, are the most vulnerable. Therefore, they become higher priority and should be dealt with first. For example, a medium level risk with a low probability of detection would be deemed high priority due to the low detection rate. In contrast, a medium level risk with a high probability of detection would be a low priority risk. By focussing on the higher priority areas first, the quality of the system is improved by reducing the overall probability of failure.

Sub-practices required by the MD regulations but NOT by the CMMI (see Table 3):

Sub-Practice 29. ISO:14971 requests that the results of all the RM activities should be recorded and maintained in a RM file. EN 60601-1-4 suggests that a RM summary file should also be created to summarise the RM activities. The RM summary file contains each identified hazard, its initiating cause, mitigation techniques used to control risk and an evaluation of effectiveness of the risk controls. Because the RM file will already contain this information, the summary report is seen by the authors as useful but not a necessity and as such has not been highlighted as a separate sub-practice.

2.

5.3. SG3 Mitigate Risks

In order to fulfil SG3: **Mitigate Risks** the following specific practices have to be performed: *Develop Risk Mitigation Plans & Implement Risk Mitigation Plans (see Table 5).*

Table 5: RMCM Sub-Practices for Specific Goal 3: Mitigate Risks

RMCM Sub-Practice Number	Sub-Practice	Source	RMCM Level
Practice: Develop Risk Mitigation Plans			
30	Determine the levels and thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation or contingency plan	CMMI RM SP3.1-1 sub-practice 1, ISO:14971 6.5 & 7	Med
31	Identify the person or group responsible for addressing each risk	CMMI RM SP3.1-1 sub-practice 2	1
32	Determine the cost-to-benefit ratio of implementing the risk mitigation plan for each risk	CMMI RM SP3.1-1 sub-practice 3	1
33	***Develop mitigation plans for all risks***	***CDRH Guidelines (Supersedes CMMI RM SP3.1-1 sub-practice 4)***	***Med***
34	***Develop contingency plans for all risks***	***CDRH Guidelines (Supersedes CMMI RM SP3.1-1 sub-practice 5)***	***Med***
35	***Add software risk control measures to the software requirements document***	***IEC:62304 7.2.2***	***Med***
36	***Identify segregation between software items essential to risk control and show how segregation is effective***	***IEC:62304***	***Med***
37	***Mitigations should be verified***	***ISO: 14971 6.3 and IEC:62304 7.3.1***	***Med***
38	***Results of the verification should be documented***	***ISO: 14971 and IEC:62304 7.3.1***	***Med***
Practice: Implement Risk Mitigation Plans			
39	Provide a method for tracking open risk-handling options when monitored risks exceed the defined thresholds	CMMI SP3.2-1 sub-practice 2, ISO:14971 3.5, 6.7 & A.2.3.5	Med
40	Invoke selected risk-handling options when monitored risks exceed the defined thresholds	CMMI SP3.2-1 sub-practice 3, ISO:14971 6.1 to 6.7	Med
41	Establish a schedule or period of performance for each risk-handling activity that includes the start date and anticipated completion date	CMMI SP3.2-1 sub-practice 4	1
42	Provide continued commitment of resources for each plan to allow successful execution of the risk-handling activities	CMMI SP3.2-1 sub-practice 5, ISO14971 3.2 & 3.3	Med
43	Collect performance measures on the risk-handling activities.	CMMI SP3.2-1 sub-practice 6, ISO14971 3.2	Med

Table 6 summarises the mapping of the MD RM regulations against CMMI® specific goal 3 (**Mitigate Risks**). It may now be determined that in order to satisfy MD regulations that not all of sub-practices of this CMMI® goal will have to be performed. However, in order to satisfy the objectives of RMCM, 6 additional sub-practices had to

1.

be added to ensure the safety element of the MD regulations is captured. Table 5 illustrates that specific goal 3 of the CMMI® will not be satisfied by following the MD regulations (i.e. performing only the RMCM level Med sub-practices) as only 5 of the 8 CMMI® sub-practices associated with this CMMI® goal are required for RMCM level Med and 2 are superseded by more comprehensive MD practices 33 and 34 respectively.

Table 6: Summary of RMCM Specific Goal 3 – Mitigate Risks

Practice	RMCM Sub-Practice Numbers	CMMI® Sub-practices	CMMI® Sub-practices required to meet regulatory requirements	Additional Sub-practices required to meet regulatory requirements
Develop Risk Mitigation Plans	30 – 38	3	1	6
Implementing Risk Mitigation Plans	39 – 43	5	4	0
Total	**30 – 43**	**8**	**5**	**6**

5.3.1. Develop risk mitigation plans

Table 5 includes the complete list of RMCM sub-practices and associated capability levels for developing risk mitigation plans. From mapping the MD regulations against the CMMI® for this practice, it was discovered that both IEC:62304 and ISO:14971 request additional sub-practices to those specified by the CMMI®. These are: *mitigations should be verified* and *the results of the mitigation verification should be documented*. Therefore, 2 additional MD specific sub-practices were added in order to ensure that the MD RM regulations are adhered to through adopting RMCM. This practice also differed from the previous practices in that two of the CMMI® sub-practices are not applicable to the RMCM. Unlike CMMI®, the FDA requires that risk mitigation plans and contingency plans be developed for all risks. Therefore, it was necessary to add another 2 sub-practices (*developing mitigation for all risks* and *developing contingency plans for all risks)*. The introduction of these sub-practices therefore overrules the more lightweight CMMI® sub-practices as they refer to individual and selected risks whereas the new sub-practice refers to all risks. Table 6 illustrates that developing risk mitigation plans consists of 1 sub-practice that is required by both the CMMI® and the MD regulations, 4 sub-practices that are required by the CMMI® but not by the MD regulations, and 4 sub-practices that are required by the MD regulations but not by the CMMI®.

2.

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 5):*

Sub-Practice 30. Based upon FDA guidelines the aim of risk mitigation within a MD company is to reduce the severity of the risk, the likelihood of the occurrence, or both. Ideally the risk would be eliminated or the severity reduced to a minor level of severity. All residual risk is measured against the criteria defined earlier in the RM strategy. If the criteria are not met, then further risk reducing control measures may be applied. If the criteria are met, then it is still the responsibility of the sponsor of the project to describe and justify any residual risk. ISO:14971 states that if the residual risk is unacceptable and no additional control measures will reduce the risk further, then a risk/benefit analysis must be performed to justify whether the intended use outweighs the residual risk. The evaluation and corresponding data and literature should be included in the RM file. Consequently, the acceptable level of residual risk depends upon the intended purpose of the MD. ISO:14971 also requires that the "overall residual risk" for the device be assessed to decide if the overall residual risk is acceptable. This should be documented in the RM file along with any associated data and relevant literature.

Sub-practices required by the CMMI® but NOT by the MD regulations *(see Table 5)**:***

Sub-Practice 31. The CMMI® requires an individual or a group to be given responsibility for addressing each risk; this is not specified in MD software guidelines.

Sub-Practice 32. There is no specific MD guideline requesting that a cost-benefit analysis has to performed for each risk as compliance with MD safety regulations and not cost is the most important factor.

Sub-practices required by the MD regulations but NOT by the CMMI *(see Table 5)**:***

Sub-Practice 33. Even though the CMMI® requires an overall mitigation plan to be in place for each project there is a difference in the thoroughness of the plan. In the case of the CMMI®, risk mitigation plans may not have to be produced for each risk (SEI 2006: RM SP 3.1-1, sub-practice 4). In order to comply with MD guidelines the manufacturer has to produce a risk control method that will eliminate or reduce the risk to be as low as possible. Risk mitigation plans should be developed for all risks. Therefore, it is necessary to add another sub-practice as follows: *developing mitigation plans for all risks*.

1.

Sub-Practice 34. The CMMI® requests that contingency plans are produced for only selected risks (SEI. 2006: RM SP3.1-1, sub-practice 5). However, as MD guidelines deal with safety, the initial approach is to only permit a product to be manufactured if it is safe and the remaining risk will not result in injury to the patient, operator, and or bystander. In terms of a contingency plan for such risks, the MD guidelines recommend using protective measures that do not involve user interaction or supplying warning labels, or alternatively a combination of both. It is therefore necessary to add another sub-practice as follows: *developing contingency plans for all risks*.

Sub-Practice 35: IEC:62304 requires that any system requirements related to the control of risks must be added to the requirements document.

Sub-Practice 36: IEC:62304 requires that the MD manufacturer identifies segregation between software items, as this is essential for effective risk control .

Sub-Practices 37 & 38. The IEC:62304 and ISO:14971 guidelines request additional sub-practices to those specified by the CMMI®. These are: *mitigations should be verified* and *the results of the mitigation verification should be documented*. Therefore additional sub-practices have to be added to RMCM.

5.3.2. Implementing risk mitigation plans

Table 5 includes the complete list of RMCM sub-practices and associated capability levels for developing risk mitigation plans. Both the MD regulatory guidelines and the CMMI® require that adequate resources and training must be provided for areas within the software quality domain such as RM. ISO:14971 specifies that the results of the RM activities should be reviewed at defined intervals to check the suitability and effectiveness of the RM process. The CMMI® also specifies that performance measures for risk handling activities are established but adds that a schedule should be produced for resolving each risk. This is not mandated within the MD regulations and is therefore labelled as a level 1 sub-practice.

Table 5 illustrates that the RMCM practice for implementing risk mitigation plans consists of 4 sub-practices that are required by both the CMMI® and the MD regulations (i.e. Level Med), and 1 sub-practice that is required by the CMMI® but not by the MD regulations (i.e. Level 1).

2.

Sub-practices required by BOTH the CMMI® and the MD regulations *(see Table 5)**:***

Sub-Practice 39. Both FDA guidelines and the CMMI® require that risks be monitored throughout a project. In fact, to comply with MD regulations, a software company is required to demonstrate that all risks may be traced throughout the lifecycle process and illustrate the mitigation of risks to an acceptable level.

Sub-Practice 40. Both FDA guidelines and the CMMI® require a method to be provided for tracking risk items to closure or to an acceptable level. FDA guidelines specify a number of control methods that may be used either individually or concurrently. The first preference control method is to eliminate the risk or reduce the risk by safe design or redesign. The second preference is to reduce the risk by introducing protective measures within the device itself or manufacturing process that do not require any user action. The third method is to reduce the risk by providing adequate user information (e.g. warnings) and training. This is the least preferable method, as it requires intervention on the part of the MD user. GAMP 4 also suggests further strategies which include: *modification of project strategies such as project structure and makeup, increasing testing* and *complete elimination of the risk driver by changing the expectations or requirements*.

The MD manufacturer is required to record the steps taken to eliminate or reduce a risk (e.g. methods adopted) and also record the results of the verification performed to check the effectiveness of the risk control measure. The manufacturer must indicate the severity level of the risk after the risk control method has been implemented and verified. Then a decision is made in relation to comparing the remaining severity level for each risk with the acceptance level associated with that risk. If the resultant risk severity level is not acceptable, then the risk control process will have to be performed again until the risk has been eliminated or the severity level of the risk is deemed acceptable. Additionally, the MD manufacturer is required to perform tests to determine if any new risks have been introduced during the risk control process. If such tests discover any new risks then the RM process will have to be followed for each of these risks. After all potential risks have been evaluated a final decision is made in relation to the safety of the MD.

Sub-Practice 42. Both FDA and CMMI® require that adequate resources and training be provided for areas within the software quality domain such as RM.

1.

Sub-Practice 43. ISO:14971 specifies that the results of the RM activities should be reviewed at defined intervals to check the suitability and effectiveness of the RM process.

Sub-practices required by the CMMI® but NOT by the MD regulations *(see Table 5)**:***
Sub-Practice 41. The CMMI® also specifies that performance measures for risk handling activities are established. Additionally, it requires that a schedule should be produced for resolving each risk.

5.4. Summary of the RMCM Specific Practices

Table 7 provides a summary of the 3 specific goals within the RMCM. There are 43 specific sub-practices of the RMCM. This consists of 23 CMMI® and 20 MD specific sub-practices. In order to satisfy the mandatory MD RM requirements, 35 of these sub-practices have to be adhered to (15 CMMI® and 20 MD specific sub-practices). Therefore level Med of the RMCM contains 35 sub-practices across 3 specific goals.

Table 7: Summary of the RMCM Specific Goals

Goal	RMCM Sub-Practice Numbers	CMMI® Sub-practices	CMMI® Sub-practices required to meet regulatory requirements	Additional Sub-practices required to meet regulatory requirements
Prepare for RM	1 – 16	6	6	10
Identify and Analyse Risks	17 – 29	9	4	4
Mitigate Risks	30 – 43	8	5	6
Total	**1 – 43**	**23**	**15**	**20**

5.5. Generic Goals and Practices

The CMMI® also identifies a number of generic goals and practices and these goals form the basis of the RMCM generic goals. At a fundamental maturity or capability level it is only necessary to perform the specific base practices. It is interesting to note that MD regulations with respect to RM often have a counterpart in the CMMI®. For RM the generic goals and practices for capability level 2 (***GG 2:*** **Institutionalise a Managed Process*)*** are*: GP 2.1 Establish Policy; GP 2.2 Plan the process; GP 2.3 Provide Resources; GP 2.4 Assign Responsibility; GP 2.5 Train People; GP 2.6 Manage Configurations; GP 2.7 Identify stakeholders; GP 2.8 M&C Process; GP 2.9 Evaluate Adherence;* and *GP 2.10 Review.*

The FDA regulations state that each manufacturer shall establish the appropriate responsibility, authority, and interrelation of all personnel who manage, perform, and

2.

assess work affecting quality. It also undertakes to ensure that all work is adequately resourced and that staff are trained. After mapping the MD RM regulations against the CMMI® generic goals, it may be determined that in order to satisfy MD regulations that not all of sub-practices of the CMMI® generic goals have to be performed. However, 6 out of the 10 practices for goal 2 have to be performed, but none of the practices for goals 3,4 or 5 are required in order to satisfy MD regulations. This gives a total of 41 required practices when combined with the 35 level Med practices from goal 1. Table 8 illustrates the goals and practices that have to be performed for each of the RMCM generic goals (GG).

Table 8: RMCM levels for the CMMI® Generic goals

Goal: GG1: Perform the Specific Practices			
Practice	**Activity Number**		
GP 1.1 Perform Base Practices	1 to 43 – see tables I, III & V		
Goal: GG2: Institutionalise a Managed Process			
Practice	**Activity Number**	**Source**	**RMCM Level**
GP 2.1 Establish Policy	44	CMMI	Med
GP 2.2 Plan the process	45	CMMI	Med
GP 2.3 Provide Resources	46	CMMI	Med
GP 2.4 Assign Responsibility	47	CMMI	Med
GP 2.5 Train People	48	CMMI	Med
GP 2.6 Manage Configurations	49	CMMI	2
GP 2.7 Identify stakeholders	50	CMMI	Med
GP 2.8 Monitor& Control the Process	51	CMMI	2
GP 2.9 Evaluate Adherence	52	CMMI	2
GP 2.10 Review	53	CMMI	2
Goal: GG3: Institutionalise a Defined Process			
GP 3.1 Establish a defined Process	54	CMMI	3
GP 3.2 Collect Improvement Information	55	CMMI	3
Goal: GG4: Institutionalise a Quantitatively Managed Process			
GP 4.1 Establish Quantitative Objectives for the Process	56	CMMI	4
GP 4.2 Stabilise Sub-process Performance	57	CMMI	4
Goal: GG5: Institutionalise an Optimising Process			
GP 5.1 Ensure Continuous Process Improvement	58	CMMI	5
GP 5.2 Correct Root Causes of Problems	59	CMMI	5

6. Results

Table 9 provides a summary of the specific and generic goals within the RMCM. This table illustrates that level Med of the RMCM contains 41 sub-practices. Additionally, only 21 of the 39 CMMI® RM sub-practices are included in the RMCM level Med. With respect to the specific goals and practices of the RM process area, it is clear that following the MD regulations will only partially meet the goals of this CMMI® process area, with only specific goal 1 being fully satisfied. As might reasonably be expected,

1.

there is little guidance provided within the MD regulations for the advanced practices of RM. Since failure to perform any specific practice implies failure to meet the specific goal, with respect to the CMMI®, it is clear, that the goals of RM within CMMI® cannot be obtained by satisfying the MD regulations during software development. However, the RMCM shows that 35 specific sub-practices would have to be performed in order to satisfy MD regulations and that only an additional 8 sub-practices would be required in order to satisfy all the CMMI® level 1 (or RMCM level 1) requirements. But is the opposite true, can meeting the CMMI® goals for RM successfully meet the MD software regulations? Meeting the goals of the RM process area by performing the CMMI® specific practices would not meet the requirements of the MD software regulations in this area as an additional 20 MD specific sub-practices had to be added to meet the objectives of RMCM. However, companies wishing to further improve their RM practices and fulfil all the RM goals and practices required by the CMMI® may adopt the 18 additional RMCM sub-practices.

Table 9: Summary of the RMCM Specific and Generic Goals

Goal	**CMMI® Activities**	**CMMI® Activities required to meet regulatory requirements**	**Additional Activities required to meet regulatory requirements)**
SG 1: Prepare for RM	6	6	10
SG 2: Identify and Analyse Risks	9	4	4
SG 3: Mitigate Risks	8	5	6
GG2: Institutionalise a Managed Process	10	6	0
GG3: Institutionalise a Defined Process	2	0	0
GG4: Institutionalise a Quantitatively Managed Process	2	0	0
GG5: Institutionalise an Optimising Process	2	0	0
Total	**39**	**21**	**20**

7. Conclusions and Future Work

This research has made a number of contributions. It has investigated how thorough current MD regulations are in relation to specifying what RM practices MD companies should adopt when developing software. This was achieved through performing a mapping between the MD regulations and the CMMI® guidelines for RM. We discovered that the guidelines specified in the MD regulations will at best, only partially meet the goals of this CMMI® process area. However, we cannot state that the CMMI®

2.

guidelines for RM are more thorough than those specified in the MD regulations as 20 additional sub-practices are required in order to satisfy the MD regulatory requirements associated within RM. We also identified the potential strengths and weaknesses of the CMMI® RM process area in the specific context of MD software.

Secondly, we developed a Risk Management Capability Model (RMCM) for the MD software industry. This model consists of 7 levels of capability. This model will assist MD companies to improve their existing RM practices and provide them with a pathway to achieving CMMI® certification which could provide them with an advantage in a competitive market-place.

As a result of this research three additional questions now require resolving. First, will MD companies react favourably to adopting the RMCM? Second, what impact will this model have upon RM practices and MD software quality, safety and reliability within the MD industry? Third, should similar SPI models be developed for other process areas that are pivotal to the development of MD software? We intend to address these three questions through performing further research.

To assist with this research we are currently progressing the development of the RMCM. Next, we plan is to trial this model within more MD companies. Our vision is to provide a complete SPI framework that is specifically tailored to the needs of the MD industry. This SPI framework will consist of a capability model for each process area that is relevant to the development of software within the MD software industry (RMCM will be one of these capability models). RMCM will support MD companies in pursuing a continuous SPI path that will produce more efficient software development and safer medical devices in compliance with regulatory requirements.

8. References

AAMI 2004, TIR32:2004, Medical device software risk management, http://marketplace.aami.org/eseries/scriptcontent/docs/Preview%20Files/TIR320412%20preview.pdf

AAMI 2005, New Guidance Offered on Software Risk Management, Vol. 40, No. 2. February 2005

ANSI/ AAMI 2001, Medical device software-Software life cycle processes, ANSI (American National Standard)/AAMI (Association for the Advancement of Medical Instrumentation) SW68:2001. http://www.techstreet.com/cgi-bin/detail?product_id=923487

ANSI/AAMI/IEC. 2006, ANSI/AAMI/IEC 62304:2006, Medical device software - Software life cycle processes Association for the Advancement of Medical Instrumentation, 19-Jul-2006 (replacement for SW68) http://www.techstreet.com/cgi-bin/detail?product_id=1277045, ISBN 1-57020-258-3

ANSI/AAMI/ISO:14971, 2007 , Medical devices – Application of risk management to medical devices.

Automotive SIG. 2005, The SPICE User Group Automotive Special Interest Group, *Automotive SPICE Process Reference Model*, 2005, available from http://www.automotivespice.com

1.

Bassen H., Silberberg J., Houston F., Knight W., Christman C., Greberman M.D., 1985, Computerized medical devices: Usage trends, problems and safety technology, In Proc. IEEE 7th Annual Conference Engineering in Medicine and Biology Society, pp. 180-185.

Bates D.W., Kuperman G.J., Rittenberg E., Teich J.M., Fiskio J. et al. 1999, "A randomized trial of a computer-based intervention to reduce utilization of redundant laboratory tests", The American Journal of Medicine, Volume 106, Issue 2, pp. 144-150, 1999.

Bovee M.W., Paul D. L., Nelson K. M., 2001, A Framework for Assessing the Use of Third-Party Software Quality Assurance Standards to Meet FDA Medical Device Software Process Control Guidelines", In: IEEE Transactions on Engineering Management, Vol. 48, No. 4, pp. 465-478.

BS/EN. 2000, BS EN 60601-1-4:2000, Medical Electrical Equipment, Part 1. General requirements for safety, http://engineers.ihs.com/document/abstract/THIIPAAAAAAAAAAA

Burton J., McCaffery F. & Richardson I. 2006, "A Risk Management Capability Model for use in Medical Device Companies", 4th Workshop on Software Quality, ICSE 2006 Shanghai, China, pp 3-8, 21st May 2006.

Cass A., and Volcker C. *2000* , SpiCE for SPACE: A method of Process Assessment for Space Projects, *SPICE 2000 Conference Proceedings*, http://www.synspace.com

Ciarkowski A.A. 2000, " FDA Regulatory Requirements for Medical Devices with Control Algorithms", Proceedings of the American Control Conference Chicago, Vol.5, pp. 3497-3500, Illinois June 2000

Crumpler E.S. & Rudolph H., 1997, FDA software policy and regulation of medical device software, Food Drug Law Journal, Vol. 52, pp. 511-516.

Eagles S., Murray J. 2001, Medical Device Software Standards: Vision and Status, http://www.devicelink.com/mddi/archive/01/05/002.html, May 2001.

Elahi B.J. 1993, "Safety & Hazard Analysis for Software Controlled Medical Devices, Proceedings of Sixth Annual IEEE Symposium on Computer-Based Medical Systems, pp.10 – 15, 13-16 June, 1993.

European Council. 1993, Council Directive 93/42/EEC Concerning Medical Devices, 14 June 1993. http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/meddevic.html

FDA Regulations. 2006, Code of Federal Regulations 21 CFR Part 820. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1

FDA/CDRH. 1999, Guidance for Off-the-Shelf Software Use in Medical Devices. http://www.fda.gov/cdrh/ode/guidance/585.pdf

FDA/CDRH. 2000, Guidance for Industry and FDA Premarket and Design Control Reviewers - Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management, July 18, 2000, http://www.fda.gov/cdrh/humfac/1497.html

FDA/CDRH. 2002, "General Principles of Software Validation; Final Guidance for Industry and FDA Staff", January 2002.

FDA/CDRH. 2005, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. http://www.fda.gov/cdrh/ode/guidance/337.pdf

FDA's Mission Statement 2007 - http://www.fda.gov/opacom/morechoices/mission.html

IEC. 1985, IEC 60812, Analysis technique for system reliability - Procedure for failure modes and effects analysis (FMEA), 1985.

ISO/IEC. 2003, ISO/IEC 15504, *Information Technology – Process Assessment – Part 5: An exemplar Process Assessment Model*, ISO/IEC JTC1/SC7, International Standards Organisation, October 2003.

ISPE. 2001, GAMP Guide for Validation of Automated Systems. GAMP 4, Dec 2001. http://www2.ispe.org/eseries/scriptcontent/orders/ProductDetail.cfm?pc=4BOUNDFUS

Johnson C.M., Johnson T.R., Zhang J. 2005, "A user-centered framework for redesigning health care interfaces", Journal of Biomedical Informatics, Vol. 38, Issue 1, pp.75–87, Feb 2005.

Kim P.T.H. 1993, FDA, *FDA and the Regulation of Medical Software,* Proceedings of Sixth Annual IEEE Symposium on Computer-Based Medical Systems, pp.1 – 6, 13-16 June 1993.

Kohn L., Corrigan J., Donaldson M., 2000, To Err is Human: Building a Safer Health System, National Academy Press.

Leveson N.G, Turner C. S, 1993, An investigation of the Therac-25 accidents, Computer, Vol. 26, No. 7, pp. 18-41, July 1993.

Mc Caffery F. & Coleman G. 2007, "The Need for a Software Process Improvement Model for the Medical Device Industry" – International Review on Computers and Software (I.R.E.C.O.S) Journal, Vol. 2, No. 1, pp. 10-15 Jan/Feb 2007.

Mc Caffery F., Donnelly P., McFall D. & D. Wilkie D. 2005, "Software Process Improvement for the Medical Industry". Chapter in Personalised Health Management Systems - The Integration of Innovative Sensing, Textile,

Information and Communication Technologies. Vol. 117 Studies in Health Technology and Informatics. Edited by: C.D. Nugent, P.J. McCullagh, E.T. McAdams and A. Lymberis, pp. 117-124., 2005, hardcover , ISBN: 1-58603-565-7, IOS Press.

Mc Caffery F., McFall D., Donnelly P. , Wilkie F.G. 2005a, *"Risk Management Process Improvement for the medical device industry"*. Proceedings of the International Conference on Software Development (SWDC-REK-2005), University of Iceland, 27th May - 1st June, 2005, in "Software Development" (*Edited by* Oddur Bendiktsson, Pekka Abrahamsson, Darren Dalcher, Ebba Thora Hvannberg, Rory O' Connor, Helgi Thorbergsson), University of Iceland Press & Engineering Research Institute (Reykjavik), ISBN 9979-54648-4, Pages 92-103

McDermid J. 1993, Issues in the development of safety-critical systems, In: F. Redmill and T. Anderson (eds) Safety-Critical Systems: Current Issues, Techniques and Standards (Chapman and Hall, London) pp. 16-43.

Munsey R. R., 1995, Trends and events in FDA regulation of medical devices over the last fifty years, Food Drug Law Journal, Vol. 50, pp. 163-177, 1995.

Munzer R.F. 1988, "FDA Rules for the Medical Device Engineer", Special Symposium on Maturing Technologies and Emerging Horizons in Biomedical Engineering, pp. 48-49, 4-7 Nov, 1988.

Rados C., 2003, Medical device Works to Reduce Preventable Medical Device Injuries. Medical device Consumer Magazine, July-August 2003. Accessed at: http://www.fda.gov/fdac/ features/2003/403_devices.html

Rudolph H. 2003, *Do we Need Medical Device Risk Management Certification?,* Medical Device & Diagnostic Industry. http://www.devicelink.com/mddi/archive/03/11/001.html

Sawyer D, Aziz KJ, Backinger CL, et al. 1996, Do it by Design: An Introduction to Hmnan Factors in Medical Devices. In: US Department of Health and Human Services, Public Health Service, Food and Drug Administration, Center for Devices and Radiological Health; 1996.

Sayre K., Kenner J., Jones P.L. 2001, *"Safety Models: An Analytical Tool for Risk Analysis of Medical Device Systems"*, Proceedings. 14th IEEE Symposium on Computer-Based Medical Systems (CBMS 2001), pp. 445 – 451, 26-27, July.

Schmuland C. 2005, *Value-Added Medical-Device Risk Management*, IEEE Transactions on Device And Materials Reliability, Vol. 5, No. 3, Page(s): 488-493, Sept 2005.

SEI. 2006, Capability Maturity Model® Integration for Development, Version 1.2 (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html, Technical Report CMU/SEI-2006-TR-008

Tang P.C., Patel V. 1994, "Major issues in user interface design for health professional workstations: summary and recommendations", Int. Journal of Biomedical Computing, Vol. 34, pp.139–48. 1994;

Theisen T.W., Neill C.J. 2004, *FDA Regulations and Auditing Practices for Software Suppliers at a Pharmaceutical Manufacturer*, SQP Vol.6, No. 4.

Tierney V.W., McDonald C.J., Martin D.K., Rogers M.P. 1987, "Computerized display of past test results effect on outpatient testing", Annals of Internal Medicine, Vol. 107(4), pp. 569–74, 1987.

US Department of Health and Human Services, 1992, Software related recalls for fiscal years 1983-91, CDRH, FDA,

US General Accounting Office 1997, Medical device reporting: Improvements needed in FDA's system for monitoring problems with approved devices, GAO/HEHS-97-21, http://www.gao.gov/archive/1997/he97021.pdf

Voas J., Miller K., Payne J. 1993, *A Software Analysis Technique for Quantifying Reliability in High-Risk Medical Devices,* Proceedings of Sixth Annual IEEE Symposium on Computer-Based Medical Systems, pp.64 – 69, 13-16 June.

Wallace D.R. and Kuhn D. R. 2001, Failure Modes in Medical Device Software: An Analysis of 15 years of Recall Data, National Institute of Standards and Technology (NIST), Int'l J. Reliability, Quality and Safety Eng., Vol. 8, no. 4.

Wood B.J. 1999, *Software Risk Management for Medical Devices*, Medical Device & Diagnostic Industry, Jan 1999. http://www.devicelink.com/mddi/archive/99/01/013.html

Risk Management Capability Model (RMCM) for the Development of Medical Device Software

Fergal Mc Caffery, John Burton & Ita Richardson
Lero – the Irish Software Engineering Research Centre
University of Limerick
Limerick, Ireland
Email: fergal.mccaffery@lero.ie, john.burton@ul.ie, ita.richardson@ul.ie

Acknowledgement.

This research is supported by the Science Foundation Ireland funded project, Global Software Development in Small to Medium Sized Enterprises (GSD for SMEs) grant number 03/IN3/1408C within Lero - the Irish Software Engineering Research Centre, University of Limerick (http://www.lero.ie).

Author Biographies

Dr. Fergal Mc Caffery, BSc, DPhil, PGCUT, is a senior research fellow with Lero - the Irish Software Engineering Research Centre. He has both an industrial and academic background. He has a degree in Computing and Information Systems, a DPhil in Intelligent Adaptive Multimedia Interfaces and a Postgraduate Certificate in University Teaching (all from the University of Ulster). His current research interests include the development of a software development framework for the medical device industry, software process improvement frameworks and assessments, and global software development.

John Burton, BSc, is the Principal Software Engineer for a Medical Device company. He possesses a degree in Computer Science and Information Systems from the University of Limerick, Ireland. He is currently pursuing a PhD from the University of Limerick. The primary focus of his research is software risk management within the medical device industry and the development of software process improvement models for this area. This research is supported and funded by Lero - the Irish Software Engineering Research Centre.

Dr. Ita Richardson, BSc, MSc, PhD, CPIM, CDipAF, MBCS, CEng is a senior lecturer in the Department of Computer Science and Information Systems at the University of Limerick. She is project leader on the Global Software Development for Small to Medium sized enterprises project, which is funded by Science Foundation Ireland and operates within Lero – the Irish Software Engineering Research Centre. Her research focuses on global software development and software process improvement and involves qualitative research with companies. Some of her post-graduate students are in full-time employment with software development companies

*** Author Photographs**


Dr Fergal Mc Caffery


John Burton


Dr Ita Richardson