Revising IEC 80001-1: Risk Management of Health Information Technology Systems

Silvana Togneri MacMahon[1], Todd Cooper[2], Fergal McCaffery[1]

[1] Regulated Software Research Centre, Department of Visual and Human Centred Computing, Dundalk Institute of Technology & Lero, Dundalk, Co. Louth, Ireland
{Silvana.MacMahon, Fergal.McCaffery}@dkit.ie
[2]Trusted Solutions Foundry, San Diego, California
{Todd@trustedsolutionsfoundry.com}

Abstract. IEC 80001-1 was published in 2010 and is now undergoing revision. Feedback gathered on the adoption of the standard has revealed a number of barriers that have impacted its adoption. The standard provides requirements related to the roles, responsibilities and activities that need to be performed for the risk management of medical IT networks. One reported barrier is a lack of drivers to motivate Top Management to implement the standard. In addition, there is a lack of alignment between IT and biomedical engineering departments within hopitals. Finally, the IEC 80001-1 standard was considered to be too complicated and complex to implement. This paper presents the barriers identified in the feedback and presents an approach to the revision of the standard as a process based standard following the structure outlined in ISO/IEC Directives Annex SL and aligned risk management standards as a means to overcome these barriers.

Keywords: IEC 80001-1, Risk Assessment, ISO 31000, Annex SL, Process Assessment, ISO 15224.

1 Introduction

There is an increased focus on ensuring that a high standard of care is provided to the patient while reducing the cost of care. This focus is due to the recent downturn in the global economy. One potential approach to achieving this goal is through the use of interoperable medical devices [1–3]. Governments recognising this potential have provided incentives to promote the meaningful use of interoperable medical devices and Health Information Technology (HIT), such as Electronic Health Records (EHRs) [4–6]. The increased prevalence of chronic conditions such as diabetes, which has resulted in a move away from acute episodic care, has led to increased use of interoperable medical devices. The management of chronic disease requires the establishment of an ongoing relationship between the patient and their care team facilitated by carefully designed care processes and requiring the support of

information technology [7–10]. The number of networked medical devices in use continues to increase as a result of this change, [11–13].

Benefits to patients identified through the use of networked medical devices include reducing the instances of adverse events improving patient safety, reducing the time spent by clinicians manually entering information, reducing redundant testing due to inaccessible information, improving patient care, reducing healthcare costs and ensuring comprehensive and secure management of health information [14, 15] resulting in medical IT networks becoming a critical, integral component of the medical system [16].

However, as medical devices increasingly interface with other equipment and hospital information systems the integration complexity of the systems is increased and this presents additional operational risks [13, 17–19]. Traditionally, when devices were placed onto a network, proprietary networks were used. Increasingly, medical devices are being designed to be placed onto the hospital's general IT network. There has been a move away from the use of proprietary networks as their use may limit the communication of the devices and therefore the potential benefits of connecting devices. This means that medical device manufacturers no longer exercise full control over the configuration of the network [20] with hospitals sourcing network components and devices from different manufacturers. This lack of control can lead to risks which result in unintended consequences outside the control of the medical device manufacturer as the placement of the device onto the hospital network creates a new system in which the device has not been validated [21]. These risks can result in the incorrect and degraded performance of the medical device [22, 23] compromising patient safety, effectiveness and the security of the IT network [24–27].

IEC 80001-1: *Application of risk management for IT-networks incorporating medical devices* [28] was published in 2010 to address the risks associated with the incorporation of a medical device into an IT network. This standard is now scheduled for revision. The revision of the standard will take into account feedback which has identified barriers to the adoption of the standard as well as the need to broaden the scope of the standard. This paper presents a proposed approach to the revision of the IEC standard and is structured as follows. Section 2 presents the results of the feedback gathered which identifies barriers to the adoption of the 2010 version of the IEC 80001-1 standard. Section 3 presents the proposed approach to the revision of the standard. Section 4 examines how the proposed approach addresses the identified barriers to adoption of the current version of the standard and, finally, section 5 presents the conclusions of the work and outlines future work in this area.

2 Barriers to the Adoption of IEC 80001-1: 2010

Prior to commencing work on the revision of the standard, feedback was gathered by the developers of the standard, International Electrotechnical Commission (IEC) Sub-Committee (SC) 62A – International Organization for Standardization (ISO) Technical Committee (TC) 215 Joint Working Group 7 (JWG7), to identify any barriers to its adoption in its current form. This feedback was gathered for use in

identifying an approach to the revision of the standard. The feedback was gathered through three case studies. These case studies examined the lessons learned from a number of projects which were conducted in which a Healthcare Delivery Organisation (HDO) attempted to implement IEC 80001-1. The projects were carried out in HDOs of varying sizes and in different geographical locations. The first case study was carried out in a large HDO based in the US who performed a pilot implementation of IEC 80001-1. The second was performed in a Cancer Therapy unit based in Austria targeting a full implementation of IEC 80001-1. The final case study was based on the experiences of a Health Service in Australia and it's experience in the implementation of IEC 80001-1 across a number of HDOs. Based on these case studies, the report on the feedback was compiled by JWG7 and identified 3 barriers to the adoption of the standards as follows:

- Lack of drivers to motivate Top Management to implement the IEC 80001-1 standard
- HDO Organizational challenges: Information Technology (IT) and Biomedical Engineering (BME) departments are not aligned
- The IEC 80001-1 standard is too complicated and complex to implement

Each of these barriers to adoption of the standard is discussed in the remainder of this section.

2.1 Lack of Drivers to Motivate Top Management

An issue which was identified during the case studies was that Top Management do not see the return on investment of implementing IEC 80001-1. This can cause issues in the adoption of the IEC 80001-1 standard as Top Management may be reluctant to provide the support and resources which are required in order to implement the standard. Comments from task group participants revealed that while participants felt that an argument can be made to say that implementing the standard increases patient safety, particpants also felt that this benefit has not as yet been quantified and so may be thought of as too abstract by Top Management. It was also reported that there is a correlation between a hopitals experience and their desire to perform risk management activities required under IEC 80001-1. Hospitals that have experienced incidents such as lost patient records or viruses are more likely to implement the requirements of the standard. This can lead to "fragmented motivations" for implementing the standard.

It was also reported that IT management lack knowledge of basic risk management concepts such as safety and reliability engineering and Failure Mode Cause and Effect Analysis (FMCEA). It was stated that "this resonates as the single largest impediment to 80001 adoption and needs clear and concise focus in the revision". This issue is also discussed in the context of HDO Organisational Challenges section of this paper. Additional perceived barriers to the implementation of the standard were the cost, complexity, lack of resources and/or skillsets. These barriers are directly related to the lack of information concerning the return on investment on implementation of the standard. This lack of information has recently been partially addressed by the publication of a white paper by the Association for the

Advancement of Medical Instrumentation (AAMI) which provides quantative information regarding the return on investment of implementing IEC 80001-1[29].

2.2 HDO Organisational Challenges

In addition to the challenges identified regarding Top Management support for adoption of the standard, an additional barrier was identified. There has been a move within hospitals to promote greater levels of communication between the clinical departments, which include clinicians, Management and BME, and the IT departments, which includes network administrators and network engineers. However, these departments still tend to operate in silos often leading to communication breakdowns between the two departments. The feedback indicated that, in general, IT do not understand clinical workflows or that network connectivity has become a crucial element of patient care. It is also reported that BMEs do not understand complex networking concepts. They "do not speak the same language".

IEC 80001-1: 2010 references a risk management standard for medical devices - ISO 14971 [30]. It should be noted that based on this feedback, the revised standard will now also reference ISO 31000 [31], a generic risk management standard. IT departments while familiar with the definition of risk within ISO 31000 are not familiar with the requirements of ISO 14971. Expanding the reference to include ISO 31000 will provide understanding of how to integrate the requirements of IEC 80001-1 within a HDOs larger risk management framework which includes many more objectives than safety, effectiveness and security, the key properties defined in IEC 80001-1.

2.3 IEC 80001-1: Too Complex and Complicated to Implement

The IEC 80001-1 standard was reported to be too complex and complicated to implement. Organisations reported that, the standard was too abstract and did not provide a means to tailor it to their needs, also it lacked guidance on how a stepwise approach may be taken to the implementation of the standard. While there is a technical report, ISO TR 80001-2-7 [32], which provides guidance on how to assess against the requirements of the standard and provides information on tailoring the assessment to a specific HDO context, it was reported that the top-level standard, IEC 80001-1, is dependent on the associated technical reports to provide guidance on various aspect of implementation of the standard. However, often the technical reports are either not available due to lack of awareness or do not provide sufficient guidance on implementation.

2.4 Conclusions from the Case Studies/ Lessons Learned Report

In order to address the barriers identified during the case studies, it was agreed that a process approach similar to that taken in ISO/TR 80001-2-7 should be taken in the revision of the standard. While this would provide an approach it does not fully

address the barriers to adoption identified during the lessons learned report. This research has focused of developing a proposed approach to the revision of the IEC 80001-1 as a process standard while addressing the identified barriers. This proposed approach is discussed in the remainder of this paper.

3 Proposed Approach for the Revision of IEC 80001-1

In determining the proposed approach for the revision of the standard, a review of the lessons learned was conducted to ensure that the approach to the revision would address these lessons and identified barriers to adoption. In addition, during the revision of the standard the scope of the standards is to be broadened. IEC 80001-1 focused on risk management of medical IT networks which were defined as an IT network that contained at least one medical device. However, this scope is to be broadened to include health software and health IT systems. This is consistent with the approach taken in IEC/CD 62304 [33] and IEC 82304: 2016 [34]. This revised scope was considered in determining the approach to the revision of the standard.

3.1 Determining the Approach to the Revision

In determining the approach to the revision of the standard, a number of standards and ISO directives were examined to assess their ability to address the lessons learned. These standards are examined in the remainder of this section prior to presenting the porposed approach to the revision of the standard.

BS EN 15224:2016
BS EN 15224: 2016 [35] is a sector specific quality management system standard for healthcare. The standard incorporates requirements from "EN ISO 9001:2105 with additional requirements, specifications and interpretations for healthcare. This standard is based on Annex SL of the ISO/IEC Directives, Part 1 – Consolidation ISO Supplement – Procedures specific to ISO [36].

Annex SL
Annex SL of the ISO Directives outlines requirements for the development of Management System Standards. The directive defines a management system standard as: "a set of interrelated or interacting elements of an organisation to establish policies and objectives and processes". Section S.9 of the Annex outlines the High level structure, identical core text and common terms and core definitions for use in Management Systems Standards. This high level structure is shown in Table 1.

Table 1. Annex SL High Level Structure

Clause :	***Title:***
Clause 1	Scope
Clause 2	Normative References
Clause 3	Terms and Definitions
Clause 4	Context of the Organisation
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance Evaluation
Clause 10	Improvement

ISO/TR 80001-2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

This technical report provides guidance to HDOs on how to assess confomance with the requirements of IEC 80001-1. ISO/TR 80001-2-7 uses a process approach and outlines the requirements of IEC 80001-1 in the form of a Process Reference Model (PRM), Process Assessment Model (PAM) and assessment method which can be used by HDOs to assess the capability of their risk management processes in relation to medical IT networks. The PRM and PAM within the technical report were developed in compliance with the requirements of ISO/IEC 15504-2:2003 Software engineering — Process assessment — Part 2: Performing an assessment [37, 38]. This standard outlines the requirements for the development of PRMs and PAMs and has susequently been replaced by the ISO/IEC 330XX series of standards.

The PRM and PAM were developed using the TIPA transformation process [39] which is a goal oriented requirements engineering technique which allows a set of requirements to be transformed into a PRM and PAM which is compliant with the requirements of ISO/IEC 15504-2. The transformation process was used firstly, as it had been used in the development of similar PRM and PAMs for service management standards [40]. These service management standards were identified as being similar to the IEC 80001-1 standard [41]. Secondly, this approach was used for developing a PRM and PAM that are compliant with the requirements of ISO/IEC 15504-2 allows for an assessment to be performed regardless of the regulatory requirements of the geographical location in which the HDO provides care and also allows for the assessment to be tailored to take into account the context of the specific HDO in which the assessment is being conducted.

ISO 31000 Risk Management

ISO 31000: 2009 Risk management – Principles and guidelines, provides principles, framework and a process for managing risk. It can be used by any organization in any domain regardless of its size or activity. This standard is currently being revised.

While the standard is not a management system standard, the revised version will follow the structure set out in Annex SL of the ISO Directives but also separates the sections into those which are concerned with the framework concerned with the implementation of risk management activities and those sections which are concerned withe the processes associated with risk management. As previously stated in this work, it has been agreed that the revised version of IEC 80001-1 must also be aligned with the revised version of the ISO 31000 standard.

3.2 The Proposed Approach to the Revision of IEC 80001-1

Having reviewed the standards above the following approach to the revision of the standard has been proposed. It is proposed that the standard should be revised i in accordance with the structure of Annex SL and in alignment with the revised version of ISO 31000. While the revised IEC 80001-1 will follow this structure, the standard will not be a management system standard.

Revising IEC 80001-1 in line with Annex SL

In order to determine if this approach would be possible, a high level mapping of the 14 processes from ISO/TR 80001-2-7 was performed against the structure for management system standards described in Annex SL (Table 1). The result of this mapping is shown in Table 2. It should be noted that as clauses 1 to 3 address Scope, Normative References, and Terms and Definitions respectively they have not been included in the mapping. All 14 processes within ISO/TR 80001-2-7 have been mapped to clauses 5 through 9 of Annex SL. As Clause 4 of annex SL addresses the context of the Organisation, it is expected that this section of the revised standard would provide guidance in terms of the the context in which the HDO provides care. This section will incorporate wording from or reference to IEC/TR 80001-2-4 which provides guidance on implementing the requirements of IEC 80001-1 in large and small responsible organisations. This section will also provide information in relation to how a stepwise approach may be used in order to implement the requirements of the standard. The stepwise approach would be facilitated by the development of an Maturity Model (MM) that would allow HDOs to take a stepwise approach to the implementation of the standard. Clause 10 of the revised standard would provide further guidance on the implementation of a stepwise approach to the implementation of the standard and would address this specifically in the context of improvement and movement to the next level of the maturity model in terms of implementing the standard.

Table 2. Mapping of ISO/TR 80001-2-7 processes to Annex SL High Level Structure

Clause :	***Title:***	***Notes:***
Clause 4	Context of the Organisation	Advice on understanding the context and tailoring Maturity Model – Stepwise Approach
Clause 5	Leadership	**Organizational Risk Management Process**
Clause 6	Planning	**Medical IT-Network Risk Management Process** **Medical IT-Network Planning Process**
Clause 7	Support	**Medical IT-Network Risk Management Process** **Risk Management Policy Process** **Medical IT-Network Documentation Process** **Responsibility Agreements Process**
Clause 8	Operation	**Risk Analysis and Evaluation** **Risk Control Process** **Residual Risk Process** **Change Release and Configuration Management Process** **Decision on how to apply Risk Management** **Go-Live**
Clause 9	Performance Evaluation	**Monitoring Process** **Event Management Process**
Clause 10	Improvement	The organisation shall continuously improve …. Refer back to MM and stepwise approach

In addition to structuring the revised standard in a manner that is consistent with the structure of annex SL, the proposed approach will also incorporate the development of a PRM, PAM, documented assessment process and MM. The development of these models would be facilitated through the use of the TIPA Transformation Process for Management System Standards. This transformation process allows for the development models for standards which are aligned with the structure outlined in Annex SL.This transformation process is discussed in the following section.

IEC 80001-1 as a Process Standard

Feedback gathered has also identified the value of adopting a process approach in the revision of the standard similar to the approach adopted in ISO/TR 80001-2-7. As previously discussed, the TIPA transformation process was used in the development of ISO/TR 80001-2-7 to ensure that the requirements of IEC 80001-1 could be transformed into a PRM and PAM that were compliant with the requirements of ISO/IEC 15504-2 (and ISO/IEC TR 24774 [42]). The developers of the TIPA transformation process have shown that the TIPA transformation process can be used in the development of PRMs and PAMs for Management System Standards [43]. The transformation process allows for compliance with ISO/IEC 33004:2015 [44]. ISO/IEC 33004:2015 sets out the requirements for process reference models, process assessment models, and maturity models and replaces ISO/IEC 15504-2 which has now been withdrawn.

Summary of the Proposed Approach to the Revision of the Standard

In order to revise the IEC 80001-1:2010 standard according to the proposed approach a number of steps are needed as follows:

- Firstly, using ISO/TR 80001-2-7 as a baseline (which contains the requirements of IEC 80001-1:2010 in the form of a ISO/IEC 15504-2 compliant PRM and PAM) the requirements expressed in the TR are reviewed in the context of the extended scope of IEC 80001-1.
- Additional requirements are incorporated into the draft revised standard to take account of the revised scope as required.
- All other existing technical reports aligned with IEC 80001-1 (IEC 80001-2-X) are reviewed for inclusion in the revised draft standard.
- Additional requirements form the technical reports are incorporated into the draft revised standard as appropriate. In some cases, it may be appropriate to make reference to the technical report rather than incorporating the requirements into the draft revised standard.
- Once all requirements have been identified for inclusion in the draft revised standard, the requirements should be structured according to the requirements of Annex SL, initially according to the high level mapping of ISO/TR 80001-2-7 processes to Annex SL.
- Using the TIPA transformation Process for Management System Standards a ISO/IEC 33004 compliant PRM, PAM and MM for the revised draft standard are developed.

The proposed approach to the revision of the IEC 80001-1 standard was presented to ISO TC215 JWG7 at a recent meeting in Hangzhou, China. While no concerns were raised regarding the proposed approach, the approach was further discussed at ISO TC215 JWG7 meetings in Belfast and Liverpool. During these discussions, members of JWG7 recognised the benefits of aligning with the structure outlined in Annex SL due to the alignment which this structure provides with existing management system standards. However, it was agreed that IEC 80001-1 should not be revised as a management system standard. Rather it has been agreed that the revised approach should follow the approach that has been adopted in the revision of ISO 31000 in that the standard will be restructured to follow the structure of Annex SL but will not be designated as a management system standard. In addition, it has been agreed that the approach of separating the sections into those related to the framework and those related to the process should also be adopted.

Revising IEC 80001-1 – ISO 31000 and Annex SL

Having agreed to the approach above the contents of IEC 80001-1: 2010 have been mapped to the structure of the current draft of the revised version of ISO 31000 which is itslef aligned with the structure outlined in Annex SL. The restructured content will be distributed to members of ISO TC215 JWG7 for review to ensure that the content have been moved to the appropriate section of the Annex SL structure. The reorganisation of the content has simplified some aspect of the standard. For example, the original version of the standard had references thoughout to how risk management activities should be documented where the structure of the revised standard allows all references to documentation to be maintained in a single section. The use of the strcuture used in the revised version of ISO 31000 allows for closer alignment between the two risk management standards. Table 3 shows a sample mapping detailing how the content from IEC 80001-1:2010 has been mapped to the

restructured content of the standard and how the section headings in the restructured version are aligned to the headings in the revised version of ISO 31000.

Table 3. Mapping of ISO DIS 31000 to IEC 80001-1 Reorganised Content to IEC 80001-1: 2010

ISO/DIS 31000		***IEC 80001-1 Content Reorganisation***		***IEC 80001-1: 2010***	
No:	***Heading:***	***No:***	***Heading:***	***No:***	***Heading:***
		n/a	Foreword	n/a	Foreword
		n/a	Introduction	n/a	Introduction
1	Scope	1.	Scope	1.	Scope
2	Normative references	2.	Normative References	n/a	No normative references in IEC 80001-1:2010
3	Terms and definitions	3.	Terms and Definitions	2	Terms and Definitions
4	Principles	4.	Principles	n/a	No principles in IEC 80001-1:2010
5	Framework	5.	Framework	n/a	Top Level Heading
5.1	General	5.1	General	3.2	Responsible Organization
5.2	Leadership and commitment	5.2	Leadership and Commitment	n/a	Top Level Heading
5.2.1	General	5.2.1	General	4.1	Overview
5.2.2	Integrating risk management	5.2.2	Integrating Risk Management	n/a	No IEC 80001-1 content linked to this section
5.3	Design	5.3	Design/Planning	n/a	No IEC 80001-1 content linked to this section
5.3.1	Understanding the organization and its context	5.3.1	Understanding the Organisation and its Context	n/a	No IEC 80001-1 content linked to this section Text from ISO TR 80001-2-7 or IEC TR 80001-2-4 could be included here or new text added
5.3.2	Articulate risk management commitment(s)	5.3.2	Articulate Risk Management Commitment	3.3 3.4 3.5 3.6	Top Management Responsibilities Medical IT Network Risk Manager Medical Device Manufacturer(s) Providers of other information technology

4 How the Proposed Approach Addresses the Identified Barriers to Adoption

Section 2 outlined the barriers to adoption of the IEC 80001-1:2010 standard. In summary, the barriers identified were as follows:

- Lack of drivers to motivate Top Management to implement the IEC 80001-1 standard;
- HDO Organizational challenges: Information Technology (IT) and Biomedical Engineering (BME) departments are not aligned;
- The IEC 80001-1 standard is too complicated and complex to implement

This section reviews each of the identified barriers and examines how the proposed approach addresses each of the barriers.

4.1 Lack of Drivers to Motivate Top Management

Adoption of IEC 80001-1 requires sponsorship by Top Management by allocation of budgets and resources to support the implementation of the standard. The proposed approach is revising the standard following the structure of Annex SL. Other management system standards which also follow the annex SL structure such as ISO 9001:2015 [45] and BS EN 15224:2016 allow for certification against the requirements of the standard. Standards development organisations have published statistics regarding the return on investment of implementing standards such as ISO 9001 [46]. By revising IEC 80001-1 in alignment with Annex SL, a similar approach may be taken to determine the return on investment of implementing IEC 80001. This will involve leveraging Top Managements familiarity with the return on investment of implementing standards such as ISO 9001 and may allow a path to certification against IEC 80001-1 in the future. This approach would also facilitate the integration of the requirements of the revised IEC 80001-1 standard with existing ISO 9001 processes (if previously implemented).

4.2 HDO Organisational Challenges

The second barrier to adoption which was identified was that IT and BME departments often operate in silos. IT do not understand clinical workflows and BME do not understand complex networking concepts. This issue was also identified during pilot implementations of ISO TR 80001-2-7 [47]. Using a structure based on Annex SL and ISO 9001 may aid in providing a common language between BME and IT. By basing the revision of the standard on a structure that both BME and IT may be familiar with, through implementation of BS EN 15224:2016 and ISO 9001 respectively, this may allow BMEs to discuss clinical aspects of networked medical devices in a way that is more understandable to IT and vice versa. By incorporating requirements from the technical reports into the revision of the standard, this will ensure that visibility of technical reports is provided. This will provide guidance on

the implementation of the requirements and ensure that the standard is not “high level”, a criticism which is sometimes made regarding BS EN 15224:2016.

4.3 IEC 80001-1: Too Complex and Complicated to Implement

Feedback also revealed that the IEC 80001-1:2010 standard was felt to be both too complex and complicated to implement. Another barrier to adoption which was identified was the lack of a stepwise approach to implementation of the standard. These barriers are addressed in the proposed approach. Firstly, Annex SL simplifies the overall structure of the standard. This is illustrated in Table 2 which shows how 14 processes from ISO/TR 80001-2-7 can be mapped to the five clauses of Annex SL. Secondly, Annex SL allows information to be provided in relation to understanding the organisational context of the HDO and to provide guidance as to how this should be considered in the implementation of the standard. Thirdly, using the TIPA transformation process for management system standards allows for the development of a PRM, PAM and MM for the revised IEC 80001-1 standard. The PRM and PAM can be used to facilitate an assessment of the capability of a HDOs risk management process against the requirements of the revised standard while the OOM can facilitate a stepwise approach to the implementation of those requirements.

5 Conclusions and Future Work

This paper outlines a proposed approach to the revision of the IEC 80001-1:2010 standard. The proposed approach focuses on the revision of IEC 80001-1 as following the structure as defined in Annex SL of the ISO Directives and aligned with the structure of the draft revised version of ISO 31000. In addition, the proposed approach will allow for the revision of IEC 80001-1 as a process standard by using the TIPA transformation process for Management System Standards to develop an ISO/IEC 33004 compliant PRM, PAM and MM which will allow for an assessment of capability of risk management processes related to health software and health IT systems to be performed. The development of the MM will allow for a stepwise approach to the implementation of the requirements of the standard which takes into account the context of the HDO in which care is being provided.

This paper also examined the barriers to adoption of the IEC 80001-1 standard and examined how the proposed approach to the revision of the standard addresses these barriers. The proposed approach may improve Top Management sponsorship of the implementation of the standard and increase management willingness to allocate the necessary budgets and resources to allow for implementation of the standard. Top Management understand the return on investment of implementing ISO 9001, which also follows Annex SL structure. Structuring the revised standard according Annex SL may allow for similar measures of return on investment to be developed. Using the Annex SL structure may address issues around the use of different language in the discussion of risk allowing for greater communication around the area by leveraging an understanding of and integration with existing standards. Revising the standard in this way will simplify the structure of the standard and make implementation of the

standard less complex. The alignment of the revised standard with the structure of the draft version of the revised ISO 31000 standard will aloow for closer alignment of these standards and will allow risk management processes which are related to health information technology systems to be integrated with more generic risk management processes within the HDO. This will allow risk management processes to take into account the wider context of risk management within the HDO. In addition, through inclusion of text from or reference to the associated technical reports will provide additional guidance on the implementation of the standard. Implementation will also be simplified by using a stepwise approach to implementation as defined in the proposed MM.

Following feedback from JWG7, the proposed approach to the revison of the standard has been agreed and the standard will be revised on this basis. The focus of the revision of the standard is not to establish the revised version of IEC 80001-1 as a management system standard in its own right but rather to follow the structure of Annex SL in an approach that is similar to that which has been adopted in the revision of the ISO 31000 standard. This approach allows the standard to be revised in alignment with the more generic risk management processes outlined in ISO 31000 while providing domain specific processes rleated to the risk management of helath information technology systems. Taking this approach allows for these domain specific processes to be integrated with generic risk management processes which may already be in place within the HDO. The revision will focus on addressing the extended scope of the standard and the identified barriers to adoption. This paper has examined how the outlined approach to the revision will address the barriers to adoption which have been identified in this paper. All research outputs will be validated through the standard community within JWG7 and also through pilot implementation within a HDO. The standard community will validate the research outputs to ensure that the barriers to adoption are addressed while the pilot implementation, while addressing these barriers, will focus specifically on ensuring that the identified organisational barriers are addressed.

The focus of the revised standard is to ensure that, while chronic illnesses increase and health information technology systems become more complex and ubiquitous, the key properties of these systems continue to be protected and remain safe, produce the intended outcome for the patient, and that data and system assests remain secure.

Acknowledgments. This research is supported by Science Foundation Ireland through Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 13/RC/2094.

References

1. West Health Institute: The Value of Medical Device Interoperability - Improving patient care with more than $30 billion in annual health care savings. (2013).
2. Hamilton, A., Nau, R., Burke, R., Weinstein, S., Dlatt, C.K.B., Fiore, S., Conyers, J.L.: Summary of the August 2011 Symposium on the Role and Future of Health Information Technology in an Era of Health Care Transformation. The George Washington University (2011).
3. Lee, I., Pappas, G.J., Cleaveland, R., Hatcliff, J., Krogh, B.H., Lee, P., Rubin, H., Sha, L.: High-confidence medical device software and systems. Computer (Long. Beach. Calif). 39, 33–38

(2006).
4. Milenkovich, N.: OCR issues new HITECH regulations , http://drugtopics.modernmedicine.com/drug-topics/news/drug-topics/health-system-news/ocr-issues-new-hitech-regulations.
5. Centers for Medicare & Medicaid Services: 42 CFR Parts 412, 413, 422 et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, http://www.gpo.gov/fdsys/pkg/FR-2010-07-28/pdf/2010-17207.pdf, (2010).
6. Centers for Medicare & Medicaid Services: EHR Incentive Programs, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms.
7. Institute of Medicine: Crossing the Quality Chasm: A New Health System for the 21st Century, https://download.nap.edu/catalog.php?record_id=10027, (2001).
8. Wagner, E.H.: The role of patient care teams in chronic disease management. BMJ Br. Med. J. 320, 569 (2000).
9. Wagner, E.H., Austin, B.T., Davis, C., Hindmarsh, M., Schaefer, J., Bonomi, A.: Improving chronic illness care: translating evidence into action. Health Aff. 20, 64–78 (2001).
10. Hoffman, C., Rice, D.: Chronic care in America: A 21st century challenge. Princeton, NJ Robert Wood Johnson Found. (1996).
11. Comstock, J.: 14M networked medical devices to ship by 2018, http://mobihealthnews.com/28295/14m-networked-medical-devices-to-ship-by-2018/.
12. Agency for Healthcare Research and Quality (AHRQ): Health IT for Improved Chronic Disease Management, http://healthit.ahrq.gov/ahrq-funded-projects/emerging-lessons/health-it-improved-chronic-disease-management, (2013).
13. Castañeda, M.: Connecting devices and data on the healthcare network. Biomed. Instrum. Technol. 44, 18–25 (2010).
14. Whitehead, S.F., Goldman, J.M.: Getting Connected for Patient Safety How Medical Device "Plug-and-Play" Interoperability Can Make a Difference. Patient Saf. Qual. Healthc. (2008).
15. Venkatasubramanian, K.K., Gupta, S.K.S., Jetley, R.P., Jones, P.L.: Interoperable Medical Devices - Communication Security Issues. IEEE Pulse. Sept/Oct 2, (2010).
16. Hampton, R., Schrenker, R.: What does IEC 80001-1 mean to you?, http://www.24x7mag.com/2011/01/what-does-iec-80001-1-mean-to-you/, (2011).
17. Rakitin, S.R.: Networked Medical Devices: Essential Collaboration for Improved Safety. AAMI.org. (2009).
18. Loughlin, S., Williams, J.S.: The top 10 medical device challenges. Biomed. Instrum. Technol. 45, 98–104 (2011).
19. Mehta, T., Mah, C.: Auto-Provisioning of Biomedical Devices on a Converged IP Network. Biomed. Instrum. Technol. 43, 463–467 (2009).
20. Gee, T.: Medical Device Networks Trouble Industry, http://medicalconnectivity.com/2008/12/18/medical-device-networks-trouble-industry/.
21. Eagles, S.: An Introduction to IEC 80001: Aiming for Patient Safety in the Networked Healthcare Environment. IT Horizons. 2008, (2008).
22. National Cybersecurity and Communications Integration Center: Attack Surface: Healthcare and Public Health Sector, (2012).
23. Talbot, D.: Computer Viruses Are "Rampant" on Medical Devices in Hospitals, http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/, (2012).
24. Graham, J., Dizikes, C.: Baby's death spotlights safety risks linked to computerized systems, http://articles.chicagotribune.com/2011-06-27/news/ct-met-technology-errors-20110627_1_electronic-medical-records-physicians-systems, (2011).
25. Shuren, J.: Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup - Testimony of Jeffrey Shuren, Director of FDA's Centre for Devices and Radiological Health, http://www.cchfreedom.org/pr/Health IT Deaths - FDA jeffrey Shuren.pdf, (2010).
26. Eagles, S.: IEC 80001: An Introduction. 80001-1 Experts, (2012).
27. Cooper, T., David, Y., Eagles, S.: Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks. AAMI (2011).
28. IEC: IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities, (2010).
29. Association for the Advancement of Medical Instrumentation: Health IT risk management. ,

Arlington, Virginia (2017).
30. ISO: ISO 14971:2007 - Medical Devices - Application of Risk to Medical Devices, (2007).
31. ISO: ISO 31000:2009 Risk management -- Principles and guidelines, (2009).
32. ISO: ISO/TR 80001-2-7: 2015 - Application of risk management for IT-networks incorporating medical devices -- Application guidance -- Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1. (2015).
33. IEC: IEC/CD 62304 Health software -- Software life cycle processes, https://www.iso.org/standard/71604.html?browse=tc.
34. IEC: IEC 82304-1:2016 Health software -- Part 1: General requirements for product safety. (2016).
35. British Standards Institute: BS EN 15224:2016 Quality management systems. EN ISO 9001:2015 for healthcare. (2016).
36. ISO/IEC: ISO/IEC Directives, Part 1 Consolidated ISO Supplement — Procedures specific to ISO - Annex SL, (2015).
37. ISO/IEC: ISO/IEC 15504-2:2003 - Software engineering — Process assessment — Part 2: Performing an assessment, (2003).
38. MacMahon, S.T., McCaffery, F., Keenan, F.: Transforming Requirements of IEC 80001-1 into an ISO/IEC 15504-2 Compliant Process Reference Model and Process Assessment Model, (2013).
39. Barafort, B., Betry, V., Cortina, S., Picard, M., St Jean, M., Renault, A., Valdés, O., Tudor, P.R.C.H.: ITSM Process Assessment Supporting ITIL : Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification. Van Haren, Zaltbommel, Netherlands (2009).
40. Barafort, B., Renault, A., Picard, M., Cortina, S.: A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000, (2008).
41. MacMahon, S.T., McCaffery, F., Eagles, S., Keenan, F., Lepmets, M., Renault, A.: Development of a Process Assessment Model for assessing Medical IT Networks against IEC 80001-1, (2012).
42. ISO/IEC: ISO/IEC TR 24774:2010 - Systems and software engineering — Life cycle management — Guidelines for process description, (2010).
43. Cortina, S., Mayer, N., Renault, A., Barafort, B.: Towards a process assessment model for management system standards. Commun. Comput. Inf. Sci. 477, 36–47 (2014).
44. ISO/IEC: ISO/IEC 33004:2015 Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models. (2015).
45. ISO: ISO 9001: 2015 Quality management systems -- Requirements, (2015).
46. British Standards Institute: BSI's ROI tool - Calculate your Return On Investment with ISO 9001, http://roi.bsigroup.com/.
47. Hegarty, F.J., MacMahon, S.T., Byrne, P., McCaffery, F.: Assessing a Hospital's Medical IT Network Risk Management Practice with 80001-1. Biomed. Instrum. Technol. 48, 64–71 (2014).