The MedITNet Assessment Framework: Development and Validation of a Framework for Improving Risk Management of Medical IT Networks

Silvana Togneri MacMahon, Fergal McCaffery, Frank Keenan
Department of Computing & Mathematics
Dundalk Institute of Technology
Co Louth, Ireland
{silvana.macmahon, fergal.mccaffery, frank.keenan}@dkit.ie

Abstract

Medical devices are increasingly designed for incorporation into a hospital's IT network allowing devices to exchange critical information. However, connecting devices in this way can introduce risks potentially negating the benefits to patients. While the IEC 80001-1 standard has been developed to aid Healthcare Delivery Organisations (HDOs) in addressing these risks, HDOs often struggle to understand and implement the requirements. The MedITNet framework has been developed to allow HDOs to assess the capability of their risk management processes against the requirements of IEC 80001-1. MedITNet provides a flexible assessment framework enabling HDOs to gain a understanding of the requirements of the standard and to improve risk management processes by determining their current state and highlighting areas for improvement. This paper examines the challenges faced by HDOs in the risk management of medical IT networks and explains the components of the MedITNet framework and how the framework addresses these challenges. The use of Action Design Research (ADR) in the development and validation of MedITNet are also discussed focusing on a pilot implementation of the assessment method and expert review of the overall framework. The changes to the framework and its components as a result of the validation process are also discussed.

Keywords

Risk Management, Medical IT networks, IEC 80001-1, Action Design Research

INTRODUCTION

Health IT systems and medical devices are increasingly being called upon to share network resources, with devices being placed onto hospitals IT networks.[1]. Interoperability of medical devices can provide a number of benefits in patient care [2-4]. However, in order to realize the benefits of interoperable medical devices fully, medical devices must be placed onto IT networks in a way that ensures that the safe operation of the device is not impacted [5].

This section examines the challenges faced by HDOs in the risk management of medical IT networks and how MedITNet addresses these challenges. Section 1 presents a brief description of the components of the MedITNet framework. Section 2 details how ADR was used to both develop MedITNet and ensure its utility in addressing the identified challenges. To provide examples of the use of ADR, Section 3 focuses upon the development and validation of the assessment questions which form part of the assessment method within MedITNet. Section 4 describes the final stage of validation of MedITNet using expert review. Section 5 examines the improvements to the framework as a result of the validation performed as part of the ADR process and finally the conclusions of the paper are presented in the final section.

The recent downturn in the global economy has led to an increased focus on interoperability of medical devices as a means of ensuring that a high standard of care is provided to the patient while reducing the cost of care [2, 6, 7]. The potential benefits of the use of interoperable medical devices and health information technology, such as electronic health records, has resulted in government incentives to promote their meaningful use [8, 9]. In addition, the prevalence of chronic conditions such as diabetes has resulted in a move away from acute episodic care. This move has resulted in 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 [3, 10-13]. Due to their utility in the management of chronic disease, the number of networked medical devices in use has increased and continues to increase [14-16].

Networked medical devices provide a number of benefits such as 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 [17, 18]. As a result of these benefits, medical IT networks have become a critical, integral component of the medical system [19]. However, while networked medical devices provide benefits 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 [16, 20-22]. Proprietary networks are being used less with medical devices being designed to be placed onto the hospitals general IT network meaning that medical device manufacturers no longer have control over the configuration of the network [23]. This complexity can lead to risks which result in unintended consequences which are 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 [1, 24]. These risks can result in the incorrect and degraded performance of the medical device [25, 26] compromising patient safety, effectiveness and the security of the IT network.[27-29]. For example, placing a medical device onto an IT network in which the device has not previously been tested could result in incorrect data being captured in the patients electronic health record. This in turn could result in mis-diagnosis and in the incorrect treatment being administered compromising the patients safety.

IEC 80001-1:2010 [30] was developed as a step towards addressing the risks associated with placing a device onto an IT network. The standard outlines the roles, responsibilities and activities to be carried out

in the management of these risks. However, HDOs face challenges when implementing the requirements of this standard [31]. These challenges include the following:

- HDOs vary in size and in terms of the capability of their risk management processes [19, 32]
- HDOs provide care in different regulatory environments meaning that the implementation of the requirements of the standard will vary depending on the regulation of the region in which the HDO provides care.
- Effective performance of risk management activities requires interaction between different stakeholder groups to understand the context of the HDO and manage identified risks accordingly [20, 33].
- HDOs may be unprepared for the organisational changes that are required to facilitate this level of interaction among stakeholders [16] who typically operate in silos [3].

These challenges make the requirements of the standard confusing and difficult to implement. These difficulties in implementing the requirements of the standard highlighted the need for the development of an assessment framework which would provide HDOs with a flexible approach to assessing the capability of their current risk management processes relating to medical IT networks while enabling communication among stakeholders groups and allowing HDOs to implement the requirements of the standard. While the approach to the development and validation of various components have been published previously e.g. the PRM and PAM[34-36] and the Assessment Method [37, 38] as well as experiences in implementing the assessment method [39], this paper examines how the MedITNet framework was developed to address these challenges by using the ADR process to combine the findings from the expert review of the framework as described in [40] and examines how this was combined with learnings from a pilot implementation of the assessment method in order to develop the framework and validate its utility for use in a specific HDO context and across a range of contexts.

The following section of this paper describes the MedITNet framework which was developed in order to assist HDOs in addressing the challenges associated with implementing the requirements of IEC 80001-1 and to provide a means to assess the capability of risk management processes in order to provide a foundation for the improvement of the risk management of medical IT networks.

1. THE MEDITNET FRAMEWORK

The MedITNet assessment framework consists of three components: a Process Reference Model (PRM), a Process Assessment Model (PAM) and an Assessment Method. Each of these components is described briefly in this section.

The PRM contains 14 processes, each of which is concerned with a different aspect of the life cycle risk management approach as outlined in IEC 80001-1. The PRM and PAM components of MedITNet have been developed in compliance with the requirements of ISO/IEC 15504-2 [41, 42]. This standard outlines requirements for “performing process assessment as a basis for use in process improvement and capability determination” [43]. Compliance with the requirements of this standard, ensures that the requirements of IEC 80001-1 are expressed at a process level which enables the use of the PRM, regardless of the geographical location of the HDO, for assessment of the requirements of the IEC 80001-1 standard, regardless of the regulations which apply to the implementation of these requirements. The processes within the PRM are described in terms of the purpose of performing the process and the outcomes which will be achieved as a result of performing the process. The processes which are contained in the PRM and PAM are illustrated in Figure 1 [42]. Figure 1 also illustrates the risk management stakeholders who must feed into the risk management processes throughout the lifecycle of the medical device. This includes risk management stakeholders from within the HDO or Responsible Organisation such as clinicians, IT and clinical engineers,as well as those that are external to the HDO

such as medical device manufacturers and providers of other IT technology. The processes address various planning, policy and implementation aspects of risk management. For example, the PRM and PAM contain processes for risk management planning or event management.

The descriptions of the 14 processes in the PRM are extended in the PAM to include base practices and work products allowing an assessment to be performed. Base practices are the activities which are performed in order to contribute to the achievement of the process purpose while work products are artifacts which are used in, or produced as a result of the execution of a process.

In addition to the PRM and PAM, MedITNet also contains an assessment method. The assessment method provides a consistent and repeatable approach to the performance of an assessment. The assessment method consists of seven stages during which the assessment scope is defined; focus group interviews are conducted with risk management stakeholders in order to make an assessment of the capability of the risk management processes. Following the interviews, a findings report is generated and presented to the HDO. The assessment method also contains an initial set of assessment questions to be used during the interviews. The questions allow for an assessment of each of the base practices defined in the PAM to be performed. The assessment questions can be used in their current form or can be tailored to take into account the context of the HDO. For example assessment questions can be used to take into account the scale and maturity of the HDO or to assess the implementation of specific requirements of IEC 80001-1 in terms of specific regulations applicable to the HDO. This ensures a flexible approach to assessment. The use of focus groups, which include internal and external risk management stakeholders, ensures that the required level of communication among risk management stakeholders is achieved. The following section describes the rationale for the use of ADR in the development and validation of the components of MedITNet.

[Insert Figure 1 – Silvana Togneri MacMahon]

Figure 1 – IEC 80001-1 Process Map

2. USE OF ACTION DESIGN RESEARCH IN THE DEVELOPMENT OF MEDITNET

ADR is a specific approach within the broader Design Science Research (DSR) paradigm. DSR is characterized by Hevner et al. [44, p.77] as follows: “In the design-science paradigm, knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artifact”. The focus of DSR is to address real-world challenges and solve authentic problems [45]. DSR is particularly useful in addressing “wicked problems” that is problems which cannot be easily understood and solved without considering the development of a solution [46] due to the involvement of the perspective of multiple stakeholders [47]. DSR has been used previously in the development of ISO/IEC 15504-2 compliant assessment models [48] and in the development of a Healthcare IT maturity model [49].

A number of approaches to DSR have been outlined all of which involve some elements of the following: identification of the problem; design of the solution; followed by its evaluation [50]. The evaluation of design artifacts can be conducted in a number of ways including the use of Action Research (AR) [50]. This approach led to the development of the ADR approach by Sein et al. [51], building on the work of Cole et al. [52]. While Cole et al. highlight the similarities between AR and DR and show how the criteria from one may be applied to the other through sequencing and interleaving of activities, Sein et al. advocate ADR as a new approach in the DSR where building, intervention and evaluation of the designed artifacts occur concurrently. Sein et al. describing the ADR process as “*as containing the inseparable and inherently interwoven activities of building the IT artifact, intervening in the organization, and evaluating it concurrently”*. ADR has been used in the development of the components of the MedITNet framework.

The use of ADR in the development of MedITNet was chosen as ADR provides a means to develop an artifact, in this case each of the components of MedITNet, which address a class of problems, in this case the challenges which are experienced by HDOs in the risk management of medical IT networks. The ADR approach allowed for the development of a framework which does not assume a "concrete client" [53] but is suitable to be tailored for use in the varying context of different HDOs. Sein et al. outline a number of steps and principles in the ADR process.These steps and principles are illustrated in Figure 2. Each of these steps and principles are discussed in the context of the application of the ADR approach in the development and validation of the MedITNet components and the overall MedITNet framework.

[Insert Figure 2 – Silvana Togneri MacMahon]

Figure 2 – ADR Steps and Principles – Adapted from Sein et al.

2.1 Phase 1 - Problem Formulation

The Problem Formulation stage of the ADR approach contains two principles: Practice-Inspired Research and Theory-Ingrained Artifact. In this stage of the process, the researcher investigates the identified problem. This is achieved through interaction with experts in the problem area in the form of "practitioners" and "end users". During this phase of the research, the researcher secured commitment from the experts for the duration of the research. Firstly, Practice-Inspired Research is conducted as a means to viewing field problems. This is then supplemented with the principle of the Theory-Ingrained Artifact where existing theories are considered for use in the development of the design artifact.

During the development of MedITNet both of these principles were used during the Problem Formulation stage of the research process. A literature review was conducted into the challenges which are faced by HDOs in the risk management of medical IT networks. The identified challenges were then validated through the use of focus group sessions within a HDO. These sessions were conducted in two stages. The focus group sessions centered on gaining an understanding of the context in which the specific HDO performs risk management activities and of the challenges reported by HDOs in the implementation of the requirements of the IEC 80001-1 standard.

Stage 1 of the focus group session concentrated on providing an overall understanding of the IEC 80001-1 standard from a HDO perspective. Each section of the standard was taken in turn and discussed. Two main concerns were highlighted by participants during this phase of the discussion. The first concern related to the placement of overall responsibility for risk management of the Medical IT network with the HDO. Participants were worried about the impact for the HDO and how they could judge their own conformance with the standard. The second concern related to the appointment of a Medical IT Network Risk Manager as required by the standard. Give current budgetary constraints such a role would require identifying an appropriately qualified person within the existing hospital staff who has appropriate experience of risk management, while also having an appropriate knowledge of system engineering, clinical workflows, relevant interoperability standards and the ability to engage with all relevant stakeholders.

Stage 2 of the focus group session investigated the current approach to the risk management within the HDO.. This stage informed the development and evaluation of MedITNet which takes place during Phase 2. During this stage it was confirmed that a robust approach is adopted for the risk management of the medical IT networks within the HDO with little downtime being experienced. The examination of current approach to risk management allowed a comparison to be made between the practical approach being taken within the HDO and the theoretical approaches outlined in the reviewed literature.

The literature review combined with the Practice-Inspired Research conducted during the focus group sesssions revealed that, while IEC 80001-1 can be used to address the identified challenges, HDOs may struggle to apply the requirements of the standard to their organisational context and may be unprepared for the organisational changes that implementation of the standard may require [16].

In addition the literature review revealed similarities between the IEC 80001-1 standard and Service Management standards [54-56] and examined the approach to the development of assessment models for these standards. As a result of the literature review in the broader area of process assessment standards, MedITNet was developed in compliance with the requirements of ISO/IEC 15504-2:2003 [41] and ISO/IEC TR 24774:2010 [57] using the TIPA transformation process. The TIPA transformation process is a goal oriented requirements engineering technique which allows for the transformation of a set of requirements into process assessment models which are compliant with the requirement of these standards [58]. The identification of these theories for the development of the proposed design artifact is consistent with the principle of a Theory-Ingrained Artifact.

2.2 Phase 2 - Building, Intervention and Evaluation

The Building, Intervention and Evaluation (BIE) phase of the ADR process contains three principles: Reciprocal Shaping; Mutually Influential Roles; and Authentic and Concurrent Evaluation. The principle of Reciprocal Shaping recognises that the design artifact is shaped by the organisational context in which it is used. In turn, the use of the design artifact shapes the design of the artifact by informing the design theories used in its development during the iterative BIE phase. The ADR process also emphasises the importance of mutual learning between the researcher and research participants in the principle of Mutually Influential Roles. The researcher provides insight into theoretical approaches while research participants provide insight into the practical application of the proposed theories. ADR differs from other DSR approaches in that evaluation is not a separate phase of the research process that follows building. This is embodied in the principle of Authentic and Concurrent Evaluation which advocates that design decisions are based on the ongoing evaluation of the artifact. Each of these principles is discussed in the context of the components of MedITNet. MedITNet was developed in two stages. The first stage focused on the development of the PRM and PAM while the second stage focused on the development of the assessment method.

The findings from the Problem Formulation Phase of the research were used to inform the development of the initial version of the PRM and PAM. Following their development, the PRM and PAM were subject to evaluation through expert review. The PRM and PAM were subject to review by two separate groups of “practitioners”. An iterative approach to the review was taken with each group reviewing the PRM and PAM twice. The feedback from each review was incorporated into the next version of the model. Firstly, the PRM and PAM were subject to review by members of IEC SC62A and ISO TC215 Joint Working Group 7 (JWG7). JWG7 was responsible for the development of the IEC 80001-1 standard and as such reviewed the PRM and PAM for their ability to assess against the requirements of the standard. In addition, the PRM and PAM were reviewed by experts in the development of similar ISO/IEC 15504-2 compliant assessment models (this group is referred to as SPICE in Figure 3). The focus of this review was on ensuring that the developed PRM and PAM were consistent with the requirements in terms of the development of PRMs and PAMs as expressed in the relevant process assessment standards. Where feedback from the two groups conflicted, each group was recognised for their own area of expertise and the feedback was addressed accordingly.

This approach to the BIE phase using practitioners is consistent with the principles of the BIE phase. Practitioners bring knowledge of the context in which the MedITNet PRM and PAM will be used and influence the design principles used in their development accordingly. Practitioners also provide feedback of the practical application of the chosen design theories, in this case the utility of the

development of an ISO/IEC 15504-2 compliant PRM and PAM for use by HDOs in assessment of their risk management processes. The use of an iterative *approach also facilitates the principle of Authentic and Concurrent Evaluation of the PRM and PAM.*

Stage 2 of the development of MedITNet focused on the development of the remaining component of MedITNet, the assessment method, and was performed concurrently with stage 1. As with Stage 1, the principles associated with the BIE phase of the ADR process are used. Development of the initial version of the assessment method was based on the findings from the literature review combined with the finding of the Practice-Inspired Research. In addition, a set of assessment questions was developed which formed part of the assessment method. The approach to the development of these questions is discussed in Section 5. The assessment method was subject to two forms of review. Similar to the PRM and PAM, the assessment method was reviewed by "practitioners" in the form of members of JWG7 to ensure that the assessment adequately addressed the requirements outlined in IEC 80001-1. In addition, a pilot implementation of the assessment method in a HDO was also performed. The pilot implementation within the HDO ensured that the assessment method, while performing an assessment of a process outlined in the MedITNet PRM and PAM, was suited for use by the "end user", in this case risk management stakeholders from within the HDO. The process used in the pilot implementation was Risk Analysis and Evaluation Process. This is the main process concerned with the performance of risk management activities. An assessment of this process can provide information about the capability of the overall risk management processes. The performance of risk analysis and evaluation activities requires discussion of other organisational processes which facilitate the performance these activities. For example, discussion of risk analysis and evaluation activities can provide insight into the risk management policy in place in the HDO and the allocation of resources to risk management activities. This approach builds on the BIE principles used in Stage 1. The pilot implementation places the assessment method in the context in which it will be used and feedback gathered during its use is incorporated into the next iteration of the assessment method. This is consistent with the principles of: Reciprocal Shaping where use of the assessment method influences design decisions about its next iteration; Mutually Influential Roles where end-users provide feedback on the practical application of the chosen design theories and; Authentic and Concurrent Evaluation where the assessment method is built and evaluated, while intervening in the HDO and improving risk management processes. The performance of the BIE phase of the ADR process can also provide insight into the problem which is under investigation which can then provide insight into the appropriateness of the chosen design. In this way, phases 1 and 2 of the ADR process are performed iteratively. Figure 3 illustrates the iterative Problem Formulation and BIE phases in the development of MedITNet.

[Insert Figure 3 – Silvana Togneri MacMahon]

Figure 3 – Iterative "Problem Formulation" and "Building, Intervention and Evaluation" Phases of the ADR Process (Adapted from Sein et al.)

2.3 Phase 3 - Reflection and Learning

While phases 1 and 2 of the ADR process are being performed iteratively, phase 3 is also being performed concurrently and contains a single principle: Guided Learning. The principle of Guided Learning means that the designed artifact not only contains the features of the original design but will also be shaped by the influence of the organisational context of the artifact using an iterative approach where feedback gathered during the BIE phase is incorporated into the next version of the artifact. This has certainly been the case in the development of MedITNet. MedITNet forms the basis of a technical report aimed at facilitating HDO self assessment against the requirements of IEC 80001-1. The original version of the technical report contained the PRM and PAM only as the assessment method had not yet been developed. This version of the technical report was circulated to members of JWG7 who reported

that the length of the technical report was too long which would impact its adoption due to the constraints on the resources within the HDO. To address this, the technical report was restructured prior to being re-circulated to members of JWG7. The new version contained the newly developed assessment method in the main body of the technical report. The assessment questions, sample assessment documentation and the PRM and PAM were moved to the annexes of the technical report. The PRM and PAM were also greatly reduced in size with relevant text from the ISO/IEC 15504 family of standards being removed but with references provided. This facilitated the dual purpose of the technical report. The first focused allowing HDOs to use the assessment method as provided in the TR to perform an initial assessment of compliance with the requirements of the standard. The second provided a means for tailoring of the assessment method, to account for the context of the HDO by reference to the PRM and PAM and to facilitate the performance of an assessment of the capability of risk management processes. Following the performance of the first three phases of the ADR process, Phase 4 is performed.

2.4 Phase 4 - Formalisation of Learning

The final phase of the ADR process contains a single principle: Generalised Outcomes. This phase moves away from the highly situated nature of the ADR process to a conceptual move where the findings from the ADR process are expressed in terms of generalised outcomes. Sein et al. contend that this conceptual move happens on three levels: (1) generalisation of the problem instance, (2) generalisation of the solution instance, and (3) derivation of design principles from the design research outcomes [51, p.44]. Each of these principles is discussed in the context of the generalisation of the learning from the development of MedITNet.

The first level in the generalisation of findings examines the problem instance in order to generalise the learning. In the case of MedITNet the generalisation of the problem instance was performed in a number of ways. Firstly, a literature review was performed to examine the challenges which are experienced by HDOs in the risk management of medical IT networks. A focus group sessions with risk management stakeholders confirmed that the identified challenges were consistent within the challenges experienced by the HDO in question. The context of the HDO was also examined. The HDO is a large teaching hospital which operates a category 2b network as defined in Table C.1 of IEC 80001-1. This category is described as follows:

> *Medical and non-Medical Devices incorporated by one Medical Device manufacturer and Medical and non- Medical Devices incorporated by other Medical Device manufacturers as well as non- Medical Devices and applications interconnected on a shared IT-Network by a 3rd party*[1].

The pilot implementation in the HDO resulted in an improvement in the Risk Analysis and Evaluation Processes within the HDO. In addition, the overall risk management of the medical IT network was improved showing the utility of MedITNet in this type of HDO.

The second level of generalisation looks as the generalisation of the solution instance. As in the first stage, the literature review identified the challenges which are faced by HDOs in the risk management of medical IT networks. The literature review revealed that although HDOs provide care in differing regulatory environments, the challenges which are faced are similar regardless of the location in which care is provided. To ensure that MedITNet addressed the identified common challenges, expert review of the components of MedITNet by members of JWG7 was performed. Members of JWG7 have been identified by member bodies as experts in their field and are representative of the risk management stakeholders as identified in IEC 80001-1. Members include representatives from various departments within HDOs such as clinical engineering, IT and management. Medical device manufacturers and

[1] Previous definitions of system categories in Table C.1 note that a 3rd party may be a hospital.

providers of other information technology solutions are also represented. The process of expert review by this group and the use of their feedback in the development and refinement of MedITNet ensured that MedITNet is suitable for tailoring for usage across a number of HDO contexts. In addition, the definition of the requirements of IEC 80001-1 at a process level, consistent with the requirements of ISO/IEC 15504-2, ensures that the requirements can be applied regardless of the context which is the intent of the IEC 80001-1 standard.

The final level in the generalisation of learnings ensures that the design principles from the ADR process are understood and communicated. While ISO/IEC 15504-2 compliant process assessment models have been developed for Service Management standards, which are similar to IEC 80001-1 in their lifecycle approach, no such model had been developed for use in this domain prior to this research. During the focus group sessions in the Practice-Inspired Research, it was revealed that risk management stakeholders found the IEC 80001-1 standard to be "new" in its approach in that it places the responsibility for the risk management of the network with the HDO. While medical device manufacturers are familiar with the use of standards in the development of medical devices [59, 60], HDOs are not as familiar and may struggle to implement the requirements of IEC 80001-1. The presence of a model such as MedITNet has been identified as essential in increasing adoption of IEC 80001-1 in assisting HDOs in addressing the challenge of understanding and implementing the requirements of the standard. This was revealed during a focus group session which was performed by selected expert members of JWG7. This session focused on validating the overall MedITNet framework and is discussed in more detail in Section 6. This level of generalisation of learnings also calls for the dissemination of the results of the research. MedITNet has been published as *ISO/TR 80001-2-7: Application of risk management for IT networks incorporating medical devices –Application Guidance – Part 2 – 7: Guidance for Healthcare Delivery Organisations (HDOs) on how to self-assess their conformance with IEC 80001-1* [61]. The following section discusses the approach taken in the development of the assessment questions which form part of the assessment method.

3. DEVELOPMENT AND VALIDATION OF THE ASSESSMENT METHOD QUESTIONS

As part of the assessment method component of MedITNet, a set of assessment questions was developed which can be used by HDOs to perform an assessment of their risk management processes related to medical IT networks [38]. As the questions perform an assessment of the capability of the base practices as outlined in the MedITNet PAM, the questions can be used as written or can be tailored to the context of the HDO and the scope of the assessment. In order to develop the assessment questions, the ADR approach was utilised with the researcher working closely with representatives from the HDO in the development of the assessment questions. This approach was taken as it allowed the perspective of different risk management stakeholders to be considered. Focus group interviews were used during some phases of the question development which also allowed the use of focus group interviews during an assessment to be trialled.

This section presents the approach that was taken to the development of the questions and outlines how this approach may also be useful to HDOs when performing a self assessment using MedITNet.

The initial phase of the question development focused on the development of questions to assess the base practices of the Risk Analysis and Evaluation Process. This process would later be used in the pilot implementation of the assessment method as mentioned previously. Focus group participants in the initial question development session had previously been involved in the Practice-Inspired Research and as such were familiar with the IEC 80001-1 standard and the approach being taken in the development of

MedITNet. In order to develop the assessment questions, participants were asked to complete six steps as follows:

1. Review the base practice;
2. Formulate an initial question(s);
3. Review the base practice in the context of the standard;
4. Review the base practice with reference to a "real" implementation of the practice;
5. Review/reformulate the question to assess the degree to which the base practice has been implemented;
6. Rephrase the question(s) to ensure fewest questions are used to assess the base practice.

Using these steps participants were encouraged to review the base practice before formulating the initial question(s). Having formulated the question participants are then asked to review the base practice in the context of the standard. Participants were encouraged to consider how the base practice formed part of the process under consideration and how the Risk Analysis and Evaluation process formed part of the overall risk management process. Following this review, participants were asked to think of "real" examples of medical IT network projects that had taken place in the HDO where the base practice under consideration had been implemented. Participants were then asked to revisit the initial question(s) and rephrase as necessary based on the understanding gained during the review process. Finally, participants were asked to review the question(s) to ensure that the fewest number of questions were used to assess the base practice. The researcher participated in this process acting as moderator during the focus group and providing clarifying aspects of the requirements of the standard as required. These steps were also used in the development of the assessment questions for the remaining 13 processes. These questions were also developed with input from HDO end users.

The steps outlined above may also assist HDOs when performing an assessment. These steps were recognized by focus group participants as being useful to HDOs for use in the tailoring of assessment questions for their own context. Participants suggested that reviewing the base practices and considering examples of the implementation of base practices during previous network projects may help in understanding how the requirements can be applied in their specific HDO context. This approach also facilitates the rephrasing of assessment questions to assess how the base practices are implemented while ensuring that regulatory requirements are met. Expert reviewers of MedITNet as described in Section 6 also noted that it is only through consideration of the requirements of IEC 80001-1 in the context of their own HDO that implementers of the standard could begin to understand the requirements in a way that would be difficult to gain by simply reading the standard, the associated technical reports and other material on the subject.

3.1 VALIDATION OF THE ASSESSMENT METHOD QUESTIONS – PILOT IMPLEMENTATION

In order to ensure that the assessment method questions were suited for use in performing an assessment of the capability of the risk management processes related to medical IT networks, a pilot assessment was performed using a focus group session. The assessment focused on a Clinical Information System (CIS) currently being used in the Intensive Care Unit (ICU) The focus group was attended by the Principal Physicist, a Physicist/Clinical Engineer, the Clinical Informatics Manager, the IT Deputy Operations Manager, a Technical Support Engineer, an IT Department Representative and two Nurses from the ICU. All participants of the assessment are members of a multi-disciplinary project team which meets on a weekly basis to discuss the risk management of the ICU CIS and other networked systems within the HDO. The researcher performed the role of the lead assessor while a second member of the research group performed the role of the second assessor. The assessment was performed against the requirements of the Risk Analysis and Evaluation Process.

Prior to the commencement of the focus group, the Principal Physicist provided an introduction to the standard and its specific impact in the context of the HDO. This introduction was followed by a presentation by the researcher to provide participants with an understanding of the IEC 80001-1 standard, process assessment concepts, the work completed to date within the study and the scope and benefits of the assessment and the approach that would be taken to performing the assessment. Participants were encouraged to ask questions and to discuss examples of their previous experience in relation to risk management processes.Fourteen questions related to the Risk Analysis and Evaluation process were posed to the focus group participants. Based on the assessment, a number of weaknesses in the risk management process were highlighted and a number of recommendations were provided. These recommendations are shown in *Table 1*. These recommendations were compiled into a findings report following the assessment which was then issued to the HDO.

3.2 Implementation of Recommendations

This section discusses the implementation of the recommendations presented in Table 1. The implementation of recommendations was discussed in a focus group held 9 months after the assessment.

The assessment made a number of recommendations in terms of the deployment of risk management resources. These recommendations included: recommendation 1, which advises the continued use of the multi-disciplinary team and that members of multi-disciplinary team continue to be made aware of their responsibilities in relation to the risk management of the medical IT network; recommendation 2 which suggests that all stakeholder groups continue to be represented in the multi- disciplinary team; and finally, recommendation 3 which advises that the position of the medical IT network risk manager be formalised.

As a result of the assessment, the importance of the multi-disciplinary team in terms of the risk management of the medical IT network has been highlighted within the HDO. Following the assessment the future procurement of new systems will result in the convening of a multi-disciplinary team. In addition, there will be documented responsibilities, in terms of the risk management of the medical IT network, for each member of the multi-disciplinary team.

Also, since the assessment, a minimum representation of risk management stakeholder groups is required in order for the multi-disciplinary team to be convened. The team must consist of the following: IT department representatives; the clinical lead in the unit in which the system will be used; clinical informatics representatives; and the CE team. The Clinical Informatics role has been established in the HDO since the assessment. The team also includes nurses or allied health professionals who take an active role as both system trainers and system administrators on a day to day basis once the system is operational. These are the minimum requirements in terms of teammembership in order for decisions on risk management of the medical IT network to be made. Other risk management stakeholders will attend the multi-disciplinary team meetings as required.

The role of the medical IT network risk manager is being resourced as part of the procurement of new medical IT network systems within the HDO as a part time role. However, as a result of the assessment, the responsibilities related to the medical IT network risk management component of the role will be defined in a way which is consistent with the requirements of IEC 80001-1. The creation of this role has been agreed by the Principal Physicist with Top Management following the reporting of recommendation 3 which advised that this role be formalised.

Responsibility agreements, in the form of service contracts, had been established prior to the assessment and were operating well between the HDO and their medical device suppliers. Recommendation 4 advised that the performance of responsibility agreements be monitored. The CE team advised that the responsibility agreements in place continue to operate well. As a result of the recommendation made during the assessment, the HDO is examining the possibility of developing a process for the review and

drafting of service contracts/responsibility agreements to ensure consistency in the development of service contracts among different manufacturers.

Recommendation 5 advised the continuing use of the multi-disciplinary team to ensure that the link between the risk management process and other processes in the HDO is maintained. Linking risk management with other processes within the HDO ensures that risk management can be performed effectively as an awareness of other processes within the HDO can highlight addtional risks. The use of the multi-disciplinary team is ongoing and improvements have been implemented regarding the management of the team. Recommendation 6 advised that the project best practices be used in the day to day management of risks. This has occurred with the focus on risk being more proactive, outside of projects, than was the case prior to the assessment. Ongoing service activities on the network are planned in advance and the focus is on minimising risk.

Recommendation 7 suggested that risk management processes be reviewed at regular intervals. In the HDO, risk management processes are reviewed when the multi-disciplinary team are prompted to do so when a change to the system occurs. There is no scheduled interval after which risk management processes are reviewed. Participants in the focus group reported that a review of risk management processes is prompted by a change to the system. In addition to the pilot implementation, the assessment questions were also reviewed by members of JWG7 as part of the review of framework. This was followed by a review of the overall MedITNet framework by a group of expert reviewers from JWG7. The results of this review are discussed in the following section.

Recommendation 8 suggested that a risk management policy be documented in the HDO. While no documented risk management policy has been put in place in the HDO since the assessment, the CE team have reported to Top Management within the HDO, the importance of the risk management processes in managing the risks associated with the medical IT networks. The assessment findings have been reported to Top Management, as has the need to resource a medical IT Network Risk Manager. The need for an “overarching” risk management policy sponsored by Top Management is recognised by risk management stakeholders within the HDO. Despite the absence of a risk management policy, the CE team confirmed that the documenting of risk management activities has improved since the assessment and that, as more risks are identified, the level of risk management documentation which is required for the context of the HDO is becoming more clear. The HDO Top Management had agreed to resource a medical IT network risk manager as part of a data analytics role. This role will be resourced to manage two new CIS’s which are currently in the process of being procured. The findings from the assessment have been reported to Top Management and an assessment of risk management processes was undertaken prior to the commencement of a new medical IT network risk management project.

Recommendation 9 suggested that risk acceptability criteria should be documented as part of the overall risk management policy. The CE team report that despite an improvement in this area, risk acceptability criteria have not yet been established and documented. However, significant improvements have been made in the discussion of the estimation of risk. Despite this, the CE team struggle with estimating risk in the way that is suggested in IEC 80001-1 based on a function of probability and severity.Estimation of risk in the HDO is focused on the severity of the impact on patient care. Risks that are identified by the CE team tend to be high severity and while the probability of occurrence generally cannot be accurately determined, probability is generally considered to be low. Informal types of risk acceptability criteria, which are not documented, are used to determine acceptability of risks on a case by case basis. Acceptability of risks is determined based on the potential impact to the patient, both in terms of patient safety and also in terms of the potential impact to the patient if the effectiveness of the network is not maintained. The CE team recognise the need to establish risk acceptability criteria and report that there is

greater awareness among the multi-disciplinary team of the need to estimate risk and determine if the level of risk is acceptable since the assessment.

The last recommendation made during the assessment suggested that a risk management policy be established which balances the key properties of the network with the mission of the HDO. As no risk management policy currently existed, no attempt had been made to balance the key properties of the network with the mission of the HDO. However, the CE team have reported the results of the assessment to Top Management and have communicated the need for the establishment of a risk management policy for medical IT networks which is consistent with the overall risk management policy of the HDO.

4. EXPERT REVIEW OF MEDITNET

The use of the ADR approach in the development and validation of the component part of MedITNet have been discussed in the previous sections of this paper. The latest version of MedITNet (incorporating feedback from all previous phases of the BIE process) was then subject to review by a select group of experts from JWG7. This formed the final stage of validation of MedITNet as illustrated in Figure 3.

This phase of the ADR process is discussed in depth in [40] and focused on the following areas:

1. The utility of the assessment framework (MedITNet) within the IEC 80001-1 family of standards;
2. The usability of the assessment framework for self-assessment of risk management processes within a Healthcare Delivery Organisation;
3. The scalability and generalisability of the assessment framework;
4. The coverage of the requirements of IEC 80001-1 by ISO/TR 80001-2-7;
5. Suggestions for improvements to the assessment framework.

The findings from the expert review in each of these areas will be discussed briefly in the remainder of this section.

4.1 Utility of MedITNet

Experts reported that the assessment framework benefits the IEC 80001-1 family of technical reports being based on ISO/IEC 15504 principles; it allows HDOs to have an objective measurement of the capability of risk management processes. Experts also noted that the format of the framework using the assessment questions gives an understanding to HDOs which is not gained by simply reading the standard. Experts reported that having to answer a set of questions requires HDOs to think about what they do in terms of IEC 80001-1 and how they will implement it within the HDO in practical terms.

One expert who had performed a trial assessment using MedITNet advised that HDO Top Management, are primarily focused on the “ultimate value proposition of safer, more effective, more secure technology usage versus 80001 requirements”. The expert reported that Top Management within the HDO recognised the benefit of having “an industry standard against which they could evaluate their own policies, procedures, competencies and deployed technology, and the use of improvement plans to provide an executable strategy for improving”.

One expert commented that having access to such a standard “ should have a huge impact for adoption, because it provides the basis for evaluation and maturity models, creation of improvement plans, and thus a path to realizing the benefits of 80001.

4.2 Usability of MedITNet for Self Assessment

Experts reported that it is difficult to say how “suitable” the framework is for performing and assessment of risk management processes as the suitability is determined by the level of maturity of the HDO who are using the framework. One expert, who had used the model in a trial assessment, found the framework to be “well formed” but noted that specific questions had to be adapted based on the maturity

of the HDO involved in the assessment and the scope of the assessment and in some cases based on the care context of the technology being assessed.

Experts also noted that the ease of use of the assessment framework is dependent on the maturity level of the HDO and the awareness, knowledge and skill of the person performing the self-assessment. It was noted that the intent of the Assessment Method is to be tailored to the specific context in which it is being used and that the intent of the document is to be a starting point rather than used as presented. This tailoring may present challenges when a self-assessment is being performed in a HDO at a lower maturity level. Experts advised that the suitability of the assessment framework will be better understood when more feedback is received from HDOs of varying types.

Experts also noted that while the measurement scale used in ISO/IEC 15504 is useful for determining the capability level of a process, experts commented that a maturity framework identifying which parts of IEC 80001-1 are more fundamental would be useful. This would provide a valuable implementation roadmap in terms of what parts of the standard should be implemented first and then be built upon to achieve a higher maturity level.

4.3 Generalisability and Scalability of MedITNet

Experts confirmed that, as the assessment framework is based on an assessment at a process level, it is suitable for use in HDOs of varying sizes. Experts suggested that tailoring of the Assessment Method may be required based on the expertise within the organisation with more tailoring required for smaller organisations with less specific expertise in this area.

Experts similarly confirmed that the assessment framework, due to its definition on a process level, is suitable for use in different locations and different regulatory frameworks. Experts who have been involved in using the assessment framework to perform an assessment confirmed that the information provided was sufficient to allow the Assessment Method to be tailored to the specific context in which it was to be used.

4.4 MedITNet Coverage of the Requirements of IEC 80001-1

Traceability from the requirements is maintained from the standard to the outcomes in the PRM, which are then phrased as base practices within the PAM. The questions in the Assessment Method are used to assess the capability of the base practices. While this traceability to each requirement has been maintained during the study, experts noted that a simple and easily understandable mapping of questions to IEC 80001-1 requirements would be helpful. It has been suggested that this traceability should be provided in order to increase the usefulness of the technical report.

Experts also advised that not all references had been checked but the references were generally thought to be correct. References to the other technical report in the IEC 80001-1 family of standards were provided in the Assessment Method as guidance.

4.5 Suggestions for Improvements to MedITNet

In addition to providing feedback on MedITNet, participants were given the opportunity to provide highlight weaknesses in the framework or make suggestions for its improvement. Experts did not note any problems with the assessment framework but suggested that further implementations were required to fully judge its utility. It was suggested that feedback should be sought from use of the assessment framework in different contexts and on different sized projects. For example, a large HDO implementation of a small project and vice versa. Experts remarked that this future use of the framework would not only highlight improvements that may be made to the framework but would also provide insight into needed revisions of the IEC 80001-1 standard.

5. IMPROVING MEDITNET FOLLOWING THE PILOT ASSESSMENT AND EXPERT REVIEW

The goal of the use of the ADR process is to validate the framework and highlight areas for improvement which will facilitate the frameworks use in a specific context and also across a range of contexts. The pilot implementation combined with review by JWG7 provided insight into the utility of the assessment framework in addressing the challenges experienced by HDOs in implemeting the requirement of the standard as outlined in the introduction to this paper. This section examines the strengths of the framework in addressing these challenges and also examines the changes to the framework resulting from the pilot implementation and the review of the framework by JWG7.

The pilot assessment showed that the assessment method was suited for use in a specific context, in this case, a large teaching hospital in Ireland. The pilot implementation showed that the use of the assessment questions opened a discussion of risk management that resulted in a common understanding of the principles of risk as outlined in the standard. The use of focus group interviews with different risk management stakeholders provided a greater understanding of the context of the HDO. The discussion of risk examined the context of the HDO in terms of the size of the HDO, the mission of the HDO and the regulations with which the HDO must comply. The use of focus group interviews also facilitated the required level of communication among risk management stakeholders and allowed the HDO to define a process to ensure that this level of communication was maintained. Participants agreed that a greater level of communication among risk management stakeholders was achieved as a result of the assessment.

While the pilot assessment provided insight into the utility of the assessment method in a specific context, the generalisability of the framework in its ability to be used across a range of contexts was an important objective of this research. Validation by JWG7 focused on ensuring the utility of the overall framework across a range of contexts. The combination of the use of the pilot implementation and the review by JWG7 ensured that both requirements were addressed. For example, the initial set of assessment questions which were developed with assistance from the focus group participants in the HDO were later found to be too context specific and were later reformulated to be more closely based on the base practices outlined in the PAM. This change was made based on the use of the questions during the pilot implementation and based on subsequent feedback on the framework from JWG7 in order to provide a basline set of questions that could be used across a range of contexts.

The pilot implementation and the review by JWG7 also resulted in changes to the structure of the MedITNet framework and the resultant technical report – ISO TR 80001-2-7. Feedback from both highlighted the pressure on resources with HDOs and outlined the need for a framework that was structured in a way that was flexible and lent itself both to an initial lightweight approach to assessment which could then be tailored for use by HDOs aty higher capability levels. This resulted in the framework being structured so that the assessment method was presented first. This meant that a HDO could use the assessment questions as detailed in the technical report, without reference to the PRM and PAM, to perform an initial “baseline” assessment of risk management processes related to medical IT networks. HDOs operating at a higher capability level where the focus was on improving the capability of risk management processes or those operating in a specific regulatory context could use the PRM and PAM processes and practices to tailor the assessment framework to their specific context.

The ADR approach leveraged both review by various risk management stakeholders reqpresenting HDOs in a number of context through JWG7 and the feedback provided by a pilot implementation in a specific HDO context. While this approach revealed the utility of the framework and its ability to be used in varying context, it was noted during the expert review of the framework that a lot will be learned about the suitability of the framework based on future implementations across varying contexts. MedITNet has now been published as ISO TR 80001-2-7 and the authors continue to interact with

JWG7 to gain feedback on how the framework is being used and may be improved. The use of the fraework has also provided some feedback for the improvement of the IEC 80001-1 standard which is currently being revised.

CONCLUSIONS

MedITNet is a flexible assessment framework which can be used by HDOs to assess the capability of their risk management processes. In order to ensure the utility of MedITNet across varying HDO contexts, ADR was used in the development and validation of the assessment framework. The iterative approach used enabled the combination of expert review by practitioners in the area with the pilot implementation of components of MedITNet by end users in the HDO context. The overall use of ADR in the development and validation of MedITNet has been discussed in this paper. In addition, examples of the use of ADR in the development of assessment questions and during the expert review of MedITNet have been discussed. The MedITNet framework is scheduled for publication as technical report in the IEC family of standards.

The development of MedITNet provides a standardised and repeatable approach to the assessment of the capability of risk management processes related to medical IT networks. An assessment can highlight areas of weakness in the risk management process, and therefore, can be used as a foundation upon which improvements to the process can be made. By improving risk management processes, HDOs can place medical devices onto their IT network and ensure that risks to the safety, effectiveness and security of the device and network are mitigated. This enables the potential benefits associated with networked medical devices to be realized such as reduced cost, reduction in adverse events and improvements to patient safety.

Acknowledgements – This research is supported by the Science Foundation Ireland Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by Science Foundation Ireland under a co-funding initiative by the Irish Government and European Regional Development Fund),and by Lero - the Irish Software Research Centre (http://www.lero.ie) grant 10/CE/I1855 & 13/RC/20194.

REFERENCES

[1] T. Cooper, Y. David, and S. Eagles, *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks*: AAMI, 2011.

[2] West Health Institute, "The Value of Medical Device Interoperability - Improving patient care with more than $30 billion in annual health care savings," 2013.

[3] Institute of Medicine. (2001). *Crossing the Quality Chasm: A New Health System for the 21st Century*. Available: https://download.nap.edu/catalog.php?record_id=10027

[4] President's Council of Advisors on Science and Technology (PCAST), "Report to the President - Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward," Executive Office of the President, Ed., ed, 2010.

[5] M. Logan and B. Patel, "Medical Device Interoperability - A Safer Path Forward " AAMI, Arlington, VA2012.

[6] A. Hamilton, R. Nau, R. Burke, S. Weinstein, C. K. B. Dlatt, S. Fiore, *et al.*, "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 University2011.

[7] I. Lee, G. J. Pappas, R. Cleaveland, J. Hatcliff, B. H. Krogh, P. Lee, *et al.*, "High-confidence medical device software and systems," *Computer*, vol. 39, pp. 33-38, 2006.

[8] N. Milenkovich. (March 15, 2013, 16/07/2013). *OCR issues new HITECH regulations* Available: http://drugtopics.modernmedicine.com/drug-topics/news/drug-topics/health-system-news/ocr-issues-new-hitech-regulations

[9] Centers for Medicare & Medicaid Services, "42 CFR Parts 412, 413, 422 et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule ", Health and Human Services Ed., ed, 2010.

[10] E. H. Wagner, "The role of patient care teams in chronic disease management," *BMJ: British medical journal*, vol. 320, p. 569, 2000.

[11] E. H. Wagner, B. T. Austin, C. Davis, M. Hindmarsh, J. Schaefer, and A. Bonomi, "Improving chronic illness care: translating evidence into action," *Health affairs*, vol. 20, pp. 64-78, 2001.
[12] C. Hoffman and D. Rice, "Chronic care in America: A 21st century challenge," *Princeton, NJ: The Robert Wood Johnson Foundation*, 1996.
[13] A. Soceanu, A. Egner, and F. Moldoveanu, "Towards Interoperability of eHealth System Networked Components," in *Control Systems and Computer Science (CSCS), 2013 19th International Conference on*, 2013, pp. 147-154.
[14] J. Comstock. (2013, 23/01/2014). *14M networked medical devices to ship by 2018*. Available: http://mobihealthnews.com/28295/14m-networked-medical-devices-to-ship-by-2018/
[15] Agency for Healthcare Research and Quality (AHRQ), "Health IT for Improved Chronic Disease Management," Department of Health and Human Services, Ed., ed, 2013.
[16] M. Castañeda, "Connecting devices and data on the healthcare network," *Biomedical Instrumentation & Technology*, vol. 44, pp. 18-25, 2010.
[17] J. Goldman and S. Whitehead, "Advancing the Adoption of Medical Device "Plug-and-Play" Interoperability to Improve Patient Safety and Healthcare Efficiency," 2010.
[18] K. K. Venkatasubramanian, S. K. S. Gupta, R. P. Jetley, and P. L. Jones, "Interoperable Medical Devices - Communication Security Issues," *IEEE Pulse*, vol. Sept/Oct 2010, 2010.
[19] R. Hampton and R. Schrenker, "What Does IEC 80001-1 Mean to You?," *24x7 - Technology and Service Solutions for Biomeds*, 2011.
[20] S. R. Rakitin, "Networked Medical Devices: Essential Collaboration for Improved Safety," *AAMI.org*, 2009.
[21] S. Loughlin and J. S. Williams, "The top 10 medical device challenges," *Biomedical Instrumentation & Technology*, vol. 45, pp. 98-104, 2011.
[22] T. Mehta and C. Mah, "Auto-Provisioning of Biomedical Devices on a Converged IP Network," *Biomedical Instrumentation & Technology*, vol. 43, pp. 463-467, 2009.
[23] T. Gee. (2008, 27/1/2012). *Medical Device Networks Trouble Industry*. Available: http://medicalconnectivity.com/2008/12/18/medical-device-networks-trouble-industry/
[24] S. Eagles, "An Introduction to IEC 80001: Aiming for Patient Safety in the Networked Healthcare Environment," *IT Horizons*, vol. 2008, 2008.
[25] National Cybersecurity and Communications Integration Center, "Attack Surface: Healthcare and Public Health Sector," ed, 2012.
[26] D. Talbot. (2012, Computer Viruses Are "Rampant" on Medical Devices in Hospitals. *MIT Technology Review*. Available: http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/
[27] J. Graham and C. Dizikes, "Baby's death spotlights safety risks linked to computerized systems," in *Chicago Tribune*, ed, 2011.
[28] J. Shuren, "Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup - Testimony of Jeffrey Shuren, Director of FDA's Centre for Devices and Radiological Health," ONC, Ed., ed, 2010.
[29] S. Eagles, "IEC 80001: An Introduction," 80001-1 Experts,, Presentation from 19th Annual NCBA ConferenceSeptember 13, 2012 2012.
[30] IEC, "IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities," ed. Geneva, Switzerland: International Electrotechnical Commission, 2010.
[31] F. J. Hegarty, S. T. MacMahon, P. Byrne, and F. McCaffery, "Assessing a Hospital's Medical IT Network Risk Management Practice with 80001-1," *Biomedical Instrumentation & Technology*, vol. 48, pp. 64-71, 2014.
[32] T. Cooper and K. Fuchs, "The Wireless Challenge - Technology Risk Assessment In Healthcare Facilities," *Biomedical Instruments and Technology*, vol. May/June 2013, 2013.
[33] M. Janssen and R. Schrenker, "Guidelines From 80001: Maintaining a Medical IT Network," *Biomedical Instrumentation & Technology*, vol. 45, pp. 295-299, 2011/07/01 2011.
[34] S. T. MacMahon, F. McCaffery, S. Eagles, F. Keenan, M. Lepmets, and A. Renault, "Development of a Process Assessment Model for assessing Medical IT Networks against IEC 80001-1," presented at the Software Process Improvement and Capability Determination (SPICE) 2012, Mallorca, Spain, 2012.
[35] S. T. MacMahon, F. McCaffery, and F. Keenan, "Transforming Requirements of IEC 80001-1 into an ISO/IEC 15504-2 Compliant Process Reference Model and Process Assessment Model," presented at the European Systems and Software Process Improvement and Innovation Conference, Dundalk, Co Louth, Ireland, 2013.
[36] S. T. MacMahon, F. Mc Caffery, and F. Keenan, "Towards a Process Assessment Model for IEC 80001-1," presented at the Healthinf 2013, Barcelona, Spain, 2013.
[37] S. T. MacMahon, F. Mc Caffery, and F. Keenan, "The Approach to the Development of an Assessment Method for IEC 80001-1," presented at the Software Process Improvement and Capability Determination, SPICE 2013, Bremen, Germany, 2013.

[38] S. T. MacMahon, F. McCaffery, and F. Keenan, "Development of the MedITNet Assessment Method - Enabling Healthcare Delivery Organisation Self Assessment against IEC 80001-1," in *First International Conference on Fundamentals and Advances in Software Systems Integration (FASSI 2015)*, Venice, Italy, 2015.
[39] F. Hegarty, S. T. MacMahon, and P. Byrne, "Experience gained in applying IEC80001-1 principles to a Medical IT Network supporting a Clinical Information Systems," *Medical Physics Journal International,*, vol. 1, p. 193, September 2013 2013.
[40] S. T. MacMahon, F. Mc Caffery, and F. Keenan, "Development and Validation of the MedITNet Assessment Framework: Improving Risk Management of Medical IT Networks," presented at the International Conference on Software and System Process (ICSSP), Tallinn, Estonia, 2015.
[41] ISO/IEC, "ISO/IEC 15504-2:2003 - Software engineering — Process assessment — Part 2: Performing an assessment," ed. Geneva, Switzerland, 2003.
[42] S. T. MacMahon, F. Mc Caffery, and F. Keenan, "Risk Management of Medical IT Networks: An ISO/IEC 15504 Compliant Approach to Assessment against IEC 80001-1," presented at the International Conference on Software and System Process (ICSSP), San Francisco, 2013.
[43] ISO. (2014, November 3rd). *The International Organization for Standardization*. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=37458
[44] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, pp. 75-105, 2004.
[45] A. Pascal, C. Thomas, and A. G. L. Romme, "Developing a Human-centred and Science-based Approach to Design: The Knowledge Management Platform Project," *British Journal of Management*, pp. n/a-n/a, 2012.
[46] H. W. Rittel and M. M. Webber, "Dilemmas in a general theory of planning," *Policy sciences*, vol. 4, pp. 155-169, 1973.
[47] J. Zimmerman, J. Forlizzi, and S. Evenson, "Research through design as a method for interaction design research in HCI," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2007, pp. 493-502.
[48] D. Tuffley, "Modelling Organisational Behavior with Process Reference Models," 2012.
[49] J. Kenneally, M. Curley, B. Wilson, and M. Porter, "Enhancing Benefits from Healthcare IT Adoption Using Design Science Research: Presenting a Unified Application of the IT Capability Maturity Framework and the Electronic Medical Record Adoption Model," in *Design Science: Perspectives from Europe*, ed: Springer, 2013, pp. 124-143.
[50] P. Offermann, O. Levina, M. Schönherr, and U. Bub, "Outline of a design science research process," in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 2009, p. 7.
[51] M. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," 2011.
[52] R. Cole, S. Purao, M. Rossi, and M. K. Sein, "Being proactive: Where Action Research meets Design Research," in *Proceedings of the Twenty-Sixth International Conference on Information Systems*, 2005, pp. 325-336.
[53] J. Iivari and J. Venable, "Action research and design science research–seemingly similar but decisively dissimilar," in *17th European Conference on Information Systems*, 2009, pp. 1-13.
[54] ISO/IEC, "ISO/IEC 20000-1:2011 - Information technology —Service management Part 1: Service management system requirements," ed. Geneva, Switzerland, 2011.
[55] ISO/IEC, "ISO/IEC 20000-2:2005 - Information technology -- Service management -- Part 2: Code of Practice," ed. Geneva, Switzerland, 2012.
[56] The Cabinet Office, "ITIL 2011 - Summary of Updates," ed. Norfolk, England: Crown Copyright, 2011.
[57] ISO/IEC, "ISO/IEC TR 24774:2010 - Systems and software engineering — Life cycle management — Guidelines for process description," ed. Geneva, Switzerland, 2010.
[58] B. Barafort, A. Renault, M. Picard, and S. Cortina, "A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000," presented at the SPICE Nuremberg, Germany, 2008.
[59] M. McHugh, F. McCaffery, and V. Casey, "Standalone software as an active medical device," in *Software Process Improvement and Capability Determination*, ed: Springer, 2011, pp. 97-107.
[60] Center for Devices and Radiological Health (CDRH), "Guidance for Industry and FDA Staff - Recognition and Use of Consensus Standards," CDRH, Ed., ed, 2007, p. 10.
[61] ISO, "ISO/TR 80001-2-7: 2015 Application of risk mangement for IT-networks incorporating medical devices -- Application guidance -- Part 2-7: Guidance for healthcare delivery organisations (HDOs) on how to self-assess their conformance with IEC 80001-1," ed. Geneva, Switzerland: International Organisation for Standardisation, 2015.

Table 1- Assessment Recommendations

Resources:

Resources for:	Assessment Result:	Recommendations	
Provision of adequate Resources	Adequate and appropriate resources to be employed in Multidisciplinary team	1.	Ensure resources continue to be aware of responsibilities and that equivalent resources are maintained.
Assignment of Qualified Personnel	Resources are adequately qualified to represent perspective of all risk management stakeholders	2.	Ensure all stakeholder groups are represented
Appointment of Medical IT Network Risk Manager	Role has been informally assumed by Clinical Engineering	3.	Formalise position as Medical IT Network Risk Manager
Enforcement of Responsibility Agreements	Responsibility agreements in place and functioning well	4.	Continue to monitor performance of responsibility agreements
Risk Management Process			
Risk Management Process:	**Assessment Result:**	**Recommendations**	
Clear Connection to other processes	Multidisciplinary team gives oversight of other processes	5.	Use of Multidisciplinary team gives connection to other processes and should be continued.
Ensuring continuing stability and effectiveness	Bring emphasis from project to on-going risk management	6.	Ensure project best practice, including assignment of responsibilities, is used in day to day risk management of the Medical IT Network.
Reviewing results at defined intervals	Not currently reviewed	7.	Develop a schedule for review and ensure results of risk management processes are reviewed at defined intervals.
Policies:			
Policies for:	**Assessment Result:**	**Recommendations:**	
Risk Management Process	No documented policy in place	8.	Document risk management policy
Risk Acceptability Criteria	No documented risk acceptability criteria	9.	Establish risk acceptability criteria. Identified risks should be evaluated against these criteria.
Balancing the three key Properties with the mission of the Responsible Organisation	Key properties are balanced on a case by case basis. No documented policy for balancing the key properties.	10.	Establish policy to balance key properties with mission of the Responsible Organisation.