

Development & Validation of an Assessment Method
for the International Standard IEC 80001-1

Lucy Ann Kiely

A dissertation submitted to the University of Dublin,
in part fulfillment of the requirements for the degree of
Master of Science in Health Informatics.

2014

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university.

Signed: _____

Lucy Ann Kielty

Date: _____

Permission to lend and / or copy

I agree that the Trinity College Library may lend or copy this dissertation upon request.

Signed: _____

Lucy Ann Kielty

Date: _____

Acknowledgements

The author would like to thank the following for their contribution and support in making this dissertation possible.

My Supervisor Mr Damon Berry for his excellent knowledge, expertise and encouragement. Thank you for sharing your knowledge and insights and introducing me to the arena of standards development & the National Standards Authority of Ireland (NSAI).

The MSc in Health Informatics Course Director Ms. Lucy Hederman for her commitment and enthusiasm for health informatics, opening our eyes to this emerging and extremely important area of healthcare. Thank you for making the course such a memorable and unforgettable experience.

All the course lecturers for their insight & considerable knowledge of health informatics & the excellent site visit facilitators for taking the time to demonstrate health informatics in action. The excellent, thought provoking and enjoyable lectures and site visits were much appreciated.

My classmates who offered guidance, friendship, support and encouragement particularly during the tough times. It was a privilege to have met you & shared this experience & I wish you all future success.

Silvana MacMahon for sharing her knowledge on ISO standards and facilitating my involvement in the Technical Report (IEC/ISO TR 80001-1-2-7) for the International Standard IEC 80001-1.

Ms Chrissie Keane for facilitating my involvement in International standards development in Ireland.

My friends who encouraged & supported me along the way, Thank you.

My work colleagues who participated in this study, generously giving of their valuable time & without whom this study would not have been possible.

My Husband Lorenzo, for his love, patience and understanding in putting up with my disappearing acts to the computer room to complete assignments and of course this thesis, thank you for helping me to complete this MSc.

Summary

The increasing use of medical devices incorporated into the IT-network creates a medical IT-network with additional risks to patient safety. The standard IEC 80001-1 (IEC 2010) addresses risk management of medical IT networks, however implementation has been slow, due to lack of an assessment method.

This study aimed to contribute to the development and validation of an assessment method for IEC 80001-1 (IEC 2010), to enable healthcare organisations to assess their processes and conformance. Additionally, this research intended to raise awareness of the standard and improve risk management processes related to medical IT-network modification.

The assessment method (containing a question set) was developed and used in the context of a medical IT-network modification project in a healthcare organisation. The feedback and findings were used to refine the question set.

The practical output of this study includes the developed assessment method which has been incorporated into a technical report (ISO/IEC TR 80001-2-7) for IEC 80001-1 due for publication in 2014. Additionally, the assessment tool used was accepted by study participants for use in future medical IT-network modification projects increasing the likelihood of further IEC 80001-1 (IEC 2010) implementations.

The findings showed that while participants used standards, none had used IEC 80001-1 (IEC 2010). No formal risk management resources were assigned to the project. Many risk management processes were undertaken informally, there was no formal risk management plan or process and documentation was mainly informal (meeting minutes). The assessment identified strengths, weaknesses, opportunities and threats in the risk management processes of the medical IT-network project. There was improved communication and collaboration among risk management stakeholders and increased knowledge and awareness of the standard among participants following the assessment.

Implementation of recommendations arising from the assessment resulted in improvements in risk management of the medical IT-network leading to increased patient safety. This study has contributed to International standards development work related to risk management of medical IT-networks. The study has raised awareness of the standard IEC 80001-1 among risk management stakeholders and improved risk management processes at the study site.

Table of Contents

Declaration	I
Permission to lend and / or copy.....	II
Acknowledgements.....	III
Summary	IV
Table of Tables.....	XIII
Table of Figures.....	XIV
Glossary of Terms	XV
List of Abbreviations	XXIV
Chapter 1 Introduction.....	26
1.1 Introduction	26
1.2 Background & Significance of this Study.....	26
1.2.1 Motivation	27
1.3 Research Question.....	27
1.4 Research Aim.....	28
1.5 Research Objectives.....	28
1.6 Outline of the Research	29
1.7 Outline of the Dissertation.....	30
1.8 Summary	31
Chapter 2 Literature Review.....	32
2.1 Introduction	32
2.2 Medical Devices – Definition & Types	33
2.3 Medical Devices & ICU.....	34
2.4 Development of POCT Devices.....	35
2.4.1 Impact of POCT in ICU	35
2.4.2 POCT Connectivity/ Interoperability in ICU	36
2.5 Medical Devices & Interoperability	36
2.6 Medical IT-networks & Risk.....	37

2.7	Risk Management of Medical IT-networks	39
2.8	International & National Regulatory & Standard Organisations	40
2.8.1	International Regulatory & Standard Organisations	40
2.8.2	National Regulatory and Standards Organisations	41
2.9	Standards Development Process & Contribution of this Study	42
2.10	Standards	44
2.10.1	Benefits of Standards	44
2.10.2	Medical Device Manufacturer & IT Standards	45
2.10.3	Healthcare Domain Standards	46
2.10.4	POCT Standards.....	47
2.11	IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) - History & Purpose	48
2.11.1	Outline of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010)	49
2.11.2	IEC 80001-1 Technical Reports (TRs).....	50
2.11.3	CE-IT Collaboration & IEC 80001-1 Implementation	51
2.11.4	IEC 80001-1 (IEC 2010) Implementation Process.....	52
2.11.5	IEC 80001-1 (IEC 2010) Implementation Research	53
2.11.6	The Need for an Assessment Method for IEC 80001-1 (IEC 2010)	54
2.12	Summary	56
Chapter 3 Research Design & Methodology		57
3.1	Introduction	57
3.2	Research Approach, Design & Methodology	58
3.2.1	Research Approach	58
3.2.2	Research Design.....	59
3.2.3	Research Paradigm, Design & Methodology of this Study & Justification for choice	60
3.3	Sampling.....	62
3.4	Data Collection Methods	62
3.4.1	Development of Data Collection Instruments, Purpose & Use	63

3.5	Data Analysis Methods	65
3.6	Methodology Overview	65
3.6.1	Step 1: Perform Literature Review.....	67
3.6.2	Step 2: Develop question set & guidance.....	67
3.6.3	Step 3: Identify the Medical IT-network Modification Project to be the focus of the assessment.....	67
3.6.4	Step 4: Identify the subset of questions & associated guidance appropriate to the identified IT-network modification project.....	68
3.6.5	Step 5: Validate subset of questions & ensure all processes are represented.....	68
3.6.6	Step 6: Develop the Questionnaire.....	68
3.6.7	Step 7: Provide an overview of the Standard IEC 80001-1 (IEC 2010) Process Assessment.....	68
3.6.8	Step 8: Perform the assessment using the subset of questions	68
3.6.9	Step 9: Post Assessment Questionnaire Distribution/Completion.....	69
3.6.10	Step 10: Assessment Analysis	69
3.6.11	Step 11: Prepare a Findings Report.....	69
3.6.12	Step 12: Questionnaire Analysis	69
3.6.13	Step 13: Refinement of the assessment question set.....	69
3.6.14	Step 14: Individual Interview Schedule Development	69
3.6.15	Step 15: Individual Interview Data Collection.....	69
3.6.16	Step 16: Individual Interview Analysis.....	69
3.6.17	Step 17: Project Review Post Go-Live.....	70
3.6.18	Step 18: Review the findings in light of the published literature	70
3.8	Submission of revised question set to Technical Committee 62A - ISO/IEC TR 80001-2-7 (Committee draft) (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014)	70
Chapter 4 Research Implementation.....		72
4.1	Introduction	72
4.2	Research Implementation: Step by Step.....	72

4.2.1 Step 1: A literature review was undertaken	74
4.2.2 Step 2: Development of a question set & guidance based on the base practices for all processes in the IEC 80001-1 PAM (MacMahon <i>et al.</i> , 2013).	74
4.2.3 Step 3: Identification of the Medical IT-network Modification Project for the Assessment.....	74
4.2.4 Step 4: Identification of the subset of questions & associated guidance appropriate to the proposed IT-network modification project	75
4.2.5 Step 5: Validation of subset of questions for use in the assessment.....	76
4.2.7 Step 7: Provision of an overview of IEC 80001-1 (2010) & Process Assessment.....	76
4.2.8 Step 8: Performance of an assessment of the risk management processes involved in a medical IT-network modification project	76
4.2.9 Step 9: collection of feedback on the assessment questions via a questionnaire.....	78
4.2.10 Step 10: Assessment Analysis using SWOT analysis & thematic analysis.....	78
4.2.11 Step 11: Preparation of assessment findings report.....	79
4.2.12 Step 12: Questionnaire Analysis	79
4.2.13 Step 13: Refinement of question set.....	79
4.2.14 Step 14 Development of the individual interview schedule.....	79
4.2.15 Step 15: Conduction of individual interviews - data collection	79
4.2.16 Step 16: Individual interview Analysis.....	80
4.2.17 Step 17: Conduction of a project review post go-live for any unexpected consequences	80
4.2.18 Step 18: Review of the findings in light of the published literature.	80
4.3 Submission of question set to Technical Committee 62A for ISO/IEC TR 80001-2-7	81
4.4 Summary	81
Chapter 5 Data Analysis & Findings	82
5.1 Introduction	82
5.2 Assessment Analysis	82
5.3 Assessment Findings.....	82
5.3.1 SWOT Analysis Findings.....	82

5.3.2 Thematic analysis Findings	91
5.4 Questionnaire Analysis	91
5.5 Questionnaire Findings	91
5.5.1 Demographics	91
5.5.2 Standards	92
5.5.3 Pre-assessment Presentation	94
5.5.4 Assessment - Standard 80001-1 (International Electrotechnical Commission (IEC) 2010)	97
5.6 Validation of assessment questions	100
5.7 Individual Interviews Analysis	101
5.8 Individual Interview Findings	102
5.8.1 Feedback on Findings Report	102
5.8.2 Review & Allocation of Recommendations	103
5.8.3 Thematic Analysis of Interviews	103
5.9 Summary	103
Chapter 6 Discussion of Findings	105
6.1 Introduction	105
6.2 Discussion of Findings	105
6.2.1 Use of standards	105
6.2.2 Risk Management Resources	106
6.2.3 Documentation of Risk Management Activities	107
6.2.4 Risk management processes	108
6.2.5 Communication / Collaboration	109
6.2.6 IEC 80001 Assessment Method - Validation	109
6.2.7 Assessment against IEC 80001-1- Timing	110
6.3 Achievement of Objectives	111
6.3.1 Research Objective 1: To contribute to the development of the assessment criteria questions in ISO/IEC TR 80001-2-7 (ISO & IEC 2014)	111
6.3.2 Research Objective 2: To validate the developed question set	111

6.3.3 Research Objective 3: To develop a set of recommendations to address any weaknesses identified during the assessment.....	111
6.3.4 Research Objective 4: To validate recommendations arising from the assessment of the IT-network modification project	112
6.3.5 Research Objective 5: To utilise the assessment feedback to refine the criteria question set that is part of the output of this work	112
6.3.6 Research Objective 6: To raise awareness of the standard among healthcare stakeholders.....	112
6.3.7 Research Objective 7: To improve risk management processes related to a medical IT-network modification project	112
6.4 Choice & Implementation of Methodology	112
6.5 Choice of Medical IT-network Modification Project.....	113
6.6 Study Impact	114
6.6.1 Local Impact.....	114
6.6.2 International Impact - Standards Development Contribution.....	115
6.7 Limitations of this Study	115
6.8 Future Work	115
6.8.1 Capability / compliance level measurement	115
6.8.2 Survey of hospitals to determine use of standards and in particular level of awareness and use of IEC 80001-1 (2010)	116
6.8.3 Standards Development Potential	116
6.9 Reflection	117
6.10 Summary.....	117
Chapter 7 Summary & Conclusion	118
7.1 Summary.....	118
7.2 Conclusions	120
References.....	121
Appendices.....	132
Appendix A ISO Standard Development Process.....	132

Appendix B Sample Process from IEC 80001-1 PAM	133
Appendix C Methodology Overview – Detailed Description of Steps to be undertaken.....	134
Appendix D Information Pack for Participants	139
Appendix D.1 Participant Information Sheet	139
Appendix D.2 Informed Consent Form	142
Appendix D.3 Focus Group Assessment Interview Schedule	144
Appendix D.4 Post Assessment Questionnaire	145
Appendix D.5 Focus Group Assessment Interview Questions	148
Appendix E Individual Interview Schedule	151
Appendix F Individual Interview Transcripts (see enclosed CD).....	151
Appendix G Ethics Approval from the School of Computer Science & Statistics (SCSS)	152
Appendix H Permission to Access Participants from Corporate Management & Heads of Department.....	154
Appendix H.1 Permission to access Hospital Staff (Approval of Designated Research Activity Proposal Pages 1-7).....	154
Appendix H.2 Permission to access IT & MPBE staff	160
Appendix H.3 Permission to access Laboratory staff	161
Appendix H.4 Permission to access Intensive Care Unit staff.....	162
Appendix I Hospital Information Sheet & Consent from Corporate Management.....	165
Appendix I.1 Hospital Information Sheet.....	165
Appendix I.2 Hospital Consent Form Signed	169
Appendix J Assessment Questions & Guidance Document (Assessment Tool)	170
Appendix K Pre-Assessment Presentation	176
Appendix L Assessment Findings Report	180
Appendix M Revised Question set & Guidance	185
Appendix N Recommendations Review Post Go-live	191
Appendix O NSAI Acknowledgement of ISO TR 80001-2-7 Comment Review Submission ..	193
Appendix P Standard Operating Procedure (SOP) RapidPoint 500 POCT ABG Analysis Procedure.....	194

Appendix Q SWOT Analysis Tables	195
Appendix Q.1 SWOT Analysis - Strengths	195
Appendix Q.2 SWOT Analysis – Weaknesses	197
Appendix Q.3 SWOT Analysis – Opportunities.....	198
Appendix Q.4 SWOT Analysis - Threats	199
Appendix R Hazards & Potential Problems (POCT ABG Analysis).....	200
Appendix S IEC 80001-1 Focus Group Assessment Transcript (see enclosed CD).....	206
Appendix T Questionnaire Question 12 Additional Comments	207
Appendix U Recommendations from Findings Report	208
Appendix V Allocation of Recommendations from Findings Report	210

Table of Tables

Table 1 Glossary of Terms	XXIII
Table 2 Abbreviations	XXV
Table 3 Research Objectives.....	29
Table 4 Key properties of a medical IT-network (International Electrotechnical Commission (IEC) 2010)	49
Table 5 IEC 80001-1 PAM Processes (Mac Mahon <i>et al.</i> 2013).....	55
Table 6 IT-Network Modification Project Personnel & Role Description.....	77
Table 7 Individual Interview Participants.....	80
Table 8 Roles of Questionnaire Respondents.....	92
Table 9 Types of standards used by respondents.....	93
Table 10 Additional Information missing from the pre- assessment presentation.....	96
Table 11 Roles of Interviewees.....	102
Table 12 Feedback on the Findings Report from Interviewees.....	102
Table 13 Sample Process from IEC 80001 PAM.....	133
Table 14 Review of Implementation of Recommendations Post Go-Live.....	192
Table 15 SWOT Analysis - Strengths	196
Table 16 SWOT Analysis – Weaknesses	197
Table 17 SWOT Analysis – Opportunities.....	198
Table 18 SWOT Analysis - Threats	199
Table 19 Hazards & Potential Problems with POCT ABG Analysis.....	205
Table 20 Additional Comments or suggestions	207
Table 21 Recommendations from Assessment Findings Report	209
Table 22 Which recommendations will you take ownership of?	210

Table of Figures

Figure 1 Outline of Dissertation.....	30
Figure 2 Medical Devices in ICU.....	34
Figure 3 IEC Standard Development Stages (International Electrotechnical Commission (IEC) 2014a)	43
Figure 4 Methodology Overview	66
Figure 5 Research Implementation Steps	73
Figure 6 Number/percentage of respondents that had used standards previously.	92
Figure 7 Level of Awareness of IEC 80001-1.....	94
Figure 8 Clarity of the Pre-Assessment Presentation	94
Figure 9 The pre-assessment provided enough information on IEC 80001-1	95
Figure 10 The pre-assessment presentation provided enough information on process assessment.	95
Figure 11 The pre-assessment presentation could have provided additional information.....	96
Figure 12 The assessment questions were clear & easy to understand.	97
Figure 13 The Assessment questions adequately addressed risk management processes.	98
Figure 14 Participating in the assessment increased my knowledge & understanding of IEC 80001-1	98
Figure 15 I can use my increased knowledge & understanding of IEC 80001-1.....	99
Figure 16 I feel participating in the assessment has informed me of the risk management activity requirements of the standard.	99
Figure 17 The assessment method seemed appropriate.....	100
Figure 18 ISO Standard Development Process	132

Glossary of Terms

The glossary of terms is listed in Table 1 below.

Term	Definition
Arterial Blood Gas (ABG) Analysis	Analysis of arterial blood usually performed at the point of care. Blood gas analysis measures whole blood Ph, gases [partial carbon dioxide pressure (pCO ₂), partial oxygen pressure – (pO ₂)], electrolytes (e.g. potassium, sodium, chloride, calcium), metabolites (e.g. glucose & lactate), hematocrit, co-oximetry and total haemoglobin (Leino & Kurvinen 2011)
Analysers	Analysers are in-vitro medical devices used to perform analysis. They are used in both laboratories and at the point of care. The results are printed and / or transmitted to a clinical information system, electronic health record or laboratory information system.
Analyser Printout	The date & time of the analysis, patient details (name, medical record number, date of birth) and results of the analysis are issued on the analyser printout (paper record).
Clinical Information System (CIS)	A Clinical Information System is a computer application that enables electronic recording, storage, & retrieval of clinical information relating to patients. The CIS can include electronic prescribing and it can be interfaced with other hospital systems.
Conworxs	Conworxs is the company that supplies the data manager integration engine called Poccelerator which is a component of the point of care testing (POCT) analyser network configuration). Poccelerator has the capability

Term	Definition
	to integrate all POCT devices and link them to the laboratory information system / patient administration system used at the study site.
Data & Systems Security	Data & Systems Security Is defined as an operational state of a Medical IT-network in which information assets (data and systems) are reasonably protected from degradation, of confidentiality, integrity and availability (International Electrotechnical Commission (IEC) 2010)
Design Research	Design research also referred to as design experiments originated in the 1990s as a methodological approach to study educational interventions. The goal of design research is to determine how designed artefacts behave under different conditions. The approach involves progressive refinement of the design based on evaluations in the real world (Collins <i>et al.</i> 2004).
Effectiveness	Effectiveness in the context of the standard IEC 80001-1 is defined as the ability to produce the intended result for the patient and the responsible organisation (International Electrotechnical Commission (IEC) 2010).
Epistemology	Epistemology is concerned with the nature of knowledge and how knowledge is obtained (Liamputtong 2013).
Electronic Health Record (EHR)	An electronic record of health related information that conforms to nationally agreed interoperability standards, and can be created, managed, and reviewed by authorised personnel across healthcare locations, is

Term	Definition
	known as an electronic health record (EHR) (U.S. Department of Health & Human Services (DHHS) Office of the National Coordinator for Health Information Technology 2008).
Electronic Patient Record (EPR)	A collection of health information for a specific patient stored in digital format in one organisation (Hayrinen <i>et al.</i> 2008). The EPR in use in the study site incorporates information on patient care episodes, electronic orders (laboratory/radiology), referrals, results and clinical documentation.
FMEA	Failure Mode & Effects Analysis is a process analysis method to identify causes and effects of failure conditions of processes (Goddard 2000).
Go-Live	The transition of the medical IT-network to the “live” environment (International Electrotechnical Commission (IEC) 2010).
Health Information and Quality Authority (HIQA)	HIQA are an independent authority established by the government and responsible for driving quality, safety and accountability in health and social services in Ireland. They develop and publish standards, monitor compliance with standards, carry out health technology assessments, publish health and social care service delivery performance statistics and carry out investigations (Health Information & Quality Authority (HIQA) 2012b).
Intensive Care Unit (ICU)	ICU also referred to as critical care unit is a specialised department in a hospital focused on the delivery of intensive care medicine to critically ill patients.

Term	Definition
International Standard	An International Standard which is a standard adopted by an International standards organization and made available to the public (International Electrotechnical Commission (IEC) 2014b).
Interoperability:	Interoperability is the ability to share patient information among health information systems by authorised users (Thede & Sewell 2009).
Information Technology (IT) Network	A system or systems made up of communicating nodes and transmission links to provide physically linked or wireless transmission between specified communication nodes (International Electrotechnical Commission (IEC) 2010).
Laboratory Information System (LIS)	Computerised information system for recording, storage, and retrieval of laboratory test results, and associated patient demographic details.
Medical Device	<p>The Medical Device Directive (MDD) 93/42/EEC (1993) as amended by the Directive 2007/47/EC (2007) defines a medical device as “an instrument, apparatus, appliance, software, or material used for the:</p> <ul style="list-style-type: none"> • diagnosis, prevention, monitoring, treatment or alleviation of disease, injury or handicap • Investigation, replacement or modification of anatomy/physiological process and • control of conception <p>without using pharmacological, immunological</p>

Term	Definition
	or metabolic means". (European Parliament & the Council of the European Union 2007; European Parliament & the Council of the European Union 1993).
Medical Device Interoperability	Medical device interoperability is the ability of medical devices, clinical information systems or their components to communicate with each other in order to safely fulfil an intended purpose (AAMI-FDA 2012).
Medical Information Technology (IT) Network	An IT-network incorporating at least one medical device (International Electrotechnical Commission (IEC) 2010).
National Standards Authority of Ireland (NSAI)	The National Standards Authority of Ireland is Ireland's official standards body. They are the national certification authority for CE Marking providing a certification service to enable businesses demonstrate conformance to applicable standards (National Standards Authority of Ireland (NSAI) 2013).
Ontology	Ontology refers to an understanding of what exists in terms of what is reality (Cormack 2000). Phenomenology advocates that reality changes according to people's experiences and the social context of the situation (Cormack 2000).
Patient Identification (ID)	Patient ID refers to patient identification barcode addressograph label which can be used to enter patient details into the POCT ABG analyser via a scanner. These patient details are also found on the patient identity band which also includes the barcode.

Term	Definition
Patient Administration System (PAS)	A Patient Administration system records details of patient care episodes – admission, transfer, discharge & clinic appointments.
Point of Care Testing (POCT)	Point of care testing (POCT) or near-patient testing is defined as “testing that is performed near or at the site of a patient with the result leading to possible change in the care of the patient” (ISO 22870 definition 3.1) (International Organization for Standardization (ISO) 2006). Common locations include intensive care units, emergency departments, theatre, bedside and general practice clinics. Common tests include: blood gas & blood glucose (sugar), urinalysis.
Point of Care Testing (POCT) Arterial Blood Gas (ABG) Analysis	Testing of arterial blood at or near the bedside measuring PH, gases, electrolytes, metabolites, haemoglobin. POCT ABG analysers are common in intensive care units.
Process	A process is defined as “a set of interrelated or interacting activities which transforms inputs into outputs” (ISO 9000 definition 3.7.6) (International Standardisation Organisation (ISO) 2005).
Process Assessment	Process assessment is defined as “a disciplined evaluation of an organizational unit’s processes against a Process Assessment Model” ISO/IEC 15504-1 Definition 3.29 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2004). The International standard for performing a process assessment is outlined in ISO/IEC 15504-2 (International

Term	Definition
	Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003).
Process Assessment Model (PAM)	A Process Assessment Model (PAM) is a “model suitable for the purpose of assessing process capability based on one or more Process Reference Models” ISO/IEC 15504-1 Definition 3.30 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003).
Process Reference Model (PRM)	A Process Reference Model (PRM) is a reference source of process definitions and descriptions required for the scope of the model. The process descriptions include the purpose, objectives and the outcomes for successfully accomplishing the process purpose (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003).
RapidComms	RapidComms is the software in the POCT analysers implemented at the study site that interacts with Poccelerator the data manager for POCT devices on the IT-network.
Responsible Organisation	Entity accountable for the use and maintenance of a medical IT-network (International Electrotechnical Commission (IEC) 2010).
Responsibility Agreement	One or more documents that together fully define the responsibilities of all relevant stakeholders (International Electrotechnical Commission (IEC) 2010).

Term	Definition
Risk	Risk is a combination of the probability of occurrence of harm and the severity of that harm (International Organization for Standardization (ISO) 2007a). In the context of this thesis we are primarily concerned with risk to the patient but also to the operator, other persons, other equipment and the environment.
Risk Management	Risk management is the “systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring risk” (ISO 14971 Definition 2.22) (International Organization for Standardization (ISO) 2007a).
Risk Management Process	The risk management process involves identifying hazards and how they can occur, determining the risk posed by each hazard, evaluating whether that risk is acceptable, and identifying and implementing control measures to reduce unacceptable risks (Cooper <i>et al.</i> 2011).
Safety	Safety is defined as freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment (International Electrotechnical Commission (IEC) 2010).
Specimen	Blood, body fluids or tissue sent to the laboratory for analysis.
Standard	A Standard is a document, established by consensus and approved by a recognized body, which provides for common and repeated use,

Term	Definition
	rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given situation (International Electrotechnical Commission (IEC) 2014b).
Staff Identification (ID)	All personnel are issued with a staff photograph identification badge which contains a barcode. The details on the ID badge can be input manually on the POCT analyser or entered by scanning the barcode using a scanner.
Transcription Errors	Errors made when manually inputting data such as results from a POCT analyser printout into the electronic patient record in the clinical information system or inputting the result into the wrong patient electronic patient record in the clinical information system.
UPSs	UPSs – uninterruptible power supplies used to maintain power to critical systems in the event of a power outage.

Table 1 Glossary of Terms

List of Abbreviations

Abbreviations

AAMI	Association for the Advancement of Medical Instrumentation
ABG	Arterial Blood Gas
BP	Base Practices
BS	British Standard
CE	Clinical Engineering
CIS	Clinical Information System
EHR	Electronic Health Record
EPR	Electronic Patient Record
FMEA	Failure Mode & Effects Analysis
HIQA	Health Information & Quality Authority
HIT	Health Information Technology
ICU	Intensive Care Unit
ID	Identification
IEC	International Electrotechnical Committee
IMB	Irish Medicines Board
IMDRF	International Medical Device Regulator’s Forum
ISO	International Organization for Standardization
IS	International Standard
IT	Information Technology
IVD	In Vitro Diagnostic Medical Device
JWG	Joint Working Group
LIS	Laboratory Information System
MD	Medical Device
MDM	Medical Device Manufacturer

Abbreviations

MPBE	Medical Physics & Bioengineering
NSAI	National Standards Authority of Ireland
PAS	Patient Administration System
PAM	Process Assessment Model
PC	Personal Computer
POCT	Point of Care Testing
PRM	Process Reference Model
QC	Quality Control
RCA	Root Cause Analysis
SaMD	Software as a medical device
SC	Sub Committee
ST-PRA	Sociotechnical Probabalistic Risk Assessment
TC	Technical Committee
TR	Technical Report
TS	Technical Specification
UPS	Uninterrupted power supply
US DHHS FDA	United States Department of Health and Human Services Food & Drug Administration

Table 2 Abbreviations

Chapter 1 Introduction

1.1 Introduction

Intensive care medicine relies heavily on technology to support the diagnosis, monitoring and treatment of critically ill patients. However, despite this, approximately one patient in every 5 or 6 patients (18% - 19%) will not survive an admission to intensive care (The Irish Critical Care Trials Group 2008; Kaukonen *et al.* 2014). This is partly due to the critical nature of their illness; however risks to patient safety and adverse events causing patient harm can also be contributing factors (Cook *et al.* 2011). Numerous patient safety reports have been published to tackle this problem (Institute of Medicine 2000; Department of Health & Children (DOHc) 2008). The *Sentinel Alert* of the Joint Commission advocates the need to consider patient safety and prevention of adverse events in light of the increasing use of technology in healthcare (The Joint Commission 2008). Also of particular concern, is the increasing use of medical devices which are incorporated into the information technology (IT) network creating a medical IT-network with associated risks to patient safety (Eagles 2008). This is especially pertinent in technology rich intensive care units (ICUs) where critically ill patients are especially vulnerable. The use of technology is supposed to benefit the patient and not contribute to their early demise!

To address this issue of patient safety risks from networked medical devices, the International Standard International Electrotechnical Committee (IEC) 80001-1 "*Application of Risk Management for IT-networks Incorporating Medical Devices: Part 1: Roles, Responsibilities and Activities*" (International Electrotechnical Commission (IEC) 2010) was published. This standard outlines the roles, responsibilities and activities for managing risks related to incorporating medical devices onto the IT-network and if implemented, will improve patient safety (International Electrotechnical Commission (IEC) 2010). This standard is the focus of this study and will be described in detail in Chapter 2.

1.2 Background & Significance of this Study

There is limited literature relating to the implementation of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). A possible reason for this is a lack of awareness of the standard among healthcare organisations. Another contributing factor is the lack of an assessment method (MacMahon *et al.* 2012) to assess risk management processes against the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). In order to address the need to assess how effectively these risk management processes were being carried out and facilitate identification of areas for improvement, a Process Reference Model (PRM) and a Process

Assessment Model (PAM) were developed in line with the standard IEC 15504 “Software Engineering - Process Assessment - Part 2” (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003) by (MacMahon et al. 2013b). Once validated and approved by the International Organization for Standardization (ISO) the PRM and PAM will be incorporated into the IEC 80001-1 (2010) family of standards (MacMahon et al. 2013b). The validated IEC 80001-1 PAM will be used to inform the development of an assessment method. The assessment method guarantees a standard approach to assessment procedures by defining; roles and responsibilities in the assessment, the scope of the assessment and the questions to be utilised to establish the capability levels related to undertaking each process (MacMahon et al. 2013b). This study seeks to contribute to this current work in this field by undertaking refinement and validation of the assessment method developed.

1.2.1 Motivation

The researcher is a clinical informatics manager responsible for the clinical information system (CIS) in the ICUs of a large academic teaching hospital. The CIS includes interfaces to numerous medical devices and hospital systems. Recent awareness of IEC 80001-1 “*Application of Risk Management for IT-networks Incorporating Medical Devices: Part 1: Roles, Responsibilities and Activities*” (International Electrotechnical Commission (IEC) 2010) highlighting the importance of risk management for medical IT-networks has emphasised the need to consider the added risks to patient safety from networked medical devices. I believe it is likely that health informatics managers may not be aware of this standard and its implications for CISs incorporating medical devices. The increasing numbers and types of devices being added to the medical IT-network and the increasing use of CISs in ICUs means that this standard is now more applicable than ever.

This study presents an opportunity to raise awareness of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) among healthcare personnel involved in CISs, medical devices and IT-networks. This raised awareness coupled with implementation of the standard may result in improved risk management of medical IT-networks. The study also provides a unique opportunity to contribute to a technical report in the International family of standards IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

1.3 Research Question

How can a healthcare organisation assess their compliance with the requirements of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010)?

1.4 Research Aim

The aim of this research is to contribute to the development and validation of an assessment method for the International standard IEC 80001-1 *“Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, Responsibilities and Activities* (International Electrotechnical Commission (IEC) 2010).

1.5 Research Objectives

The objectives of the research and means of achieving same are outlined in Table 3.

	Objective	Methods
1.	To contribute to the development of the assessment criteria questions in ISO/IEC TR 80001-2-7 for all risk management processes related to medical IT-networks.	Assessment criteria question development workshop.
2.	To validate the developed question set.	Perform an assessment of current risk management processes prior to the implementation of an IT-network modification where IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) has been determined to be applicable.
3.	To develop a set of recommendations to address any weaknesses identified during the assessment.	Recommendations will be included in the assessment findings report.
4.	To validate recommendations arising from the assessment of the IT-network modification project.	Review of recommendations by assessment participants to obtain agreement that the recommendations are valid and that they could/would implement.
5.	To utilise the assessment feedback to refine the criteria question set that is part of the output of this work.	Assessment feedback will be collected via a post assessment questionnaire and the criteria question set will be amended accordingly.
6.	To raise awareness of the standard among healthcare stakeholders.	Participants will be provided with a summary of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) prior to the assessment & a questionnaire will measure

		their level awareness.
7.	To improve risk management processes related to a medical IT-network modification project.	Perform a SWOT analysis of the assessment findings, draft a findings report & implement identified recommendations.

Table 3 Research Objectives

1.6 Outline of the Research

This research study will include these steps:

- Undertake a literature review to inform the design and methodology of the study.
- Develop a question set which includes: question guidance based on the base practices for all 14 processes in the IEC 80001-1 PAM (MacMahon *et al.* 2012).
- Identify the subset of questions and associated guidance that are appropriate to the proposed IT-network modification project.
- Validate the subset of questions.
- Perform an assessment of the risk management process involved in a medical IT-network modification project.
- Obtain feedback on the assessment questions via a questionnaire.
- Refine question set based on the feedback from the assessment – Design Research.
- Analyse the assessment results using SWOT and thematic analysis.
- Prepare a findings report which includes a SWOT analysis and recommendations to improve risk management processes.
- Validate recommendations with assessment participants through individual interviews.
- Implement recommendations where possible to improve the risk management processes.
- Conduct a project review post go-live for any unexpected consequences.
- Submit revised question set to TC 62A for ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014).
- Review the findings in light of the published literature.

1.7 Outline of the Dissertation

This dissertation is divided into the following sections:

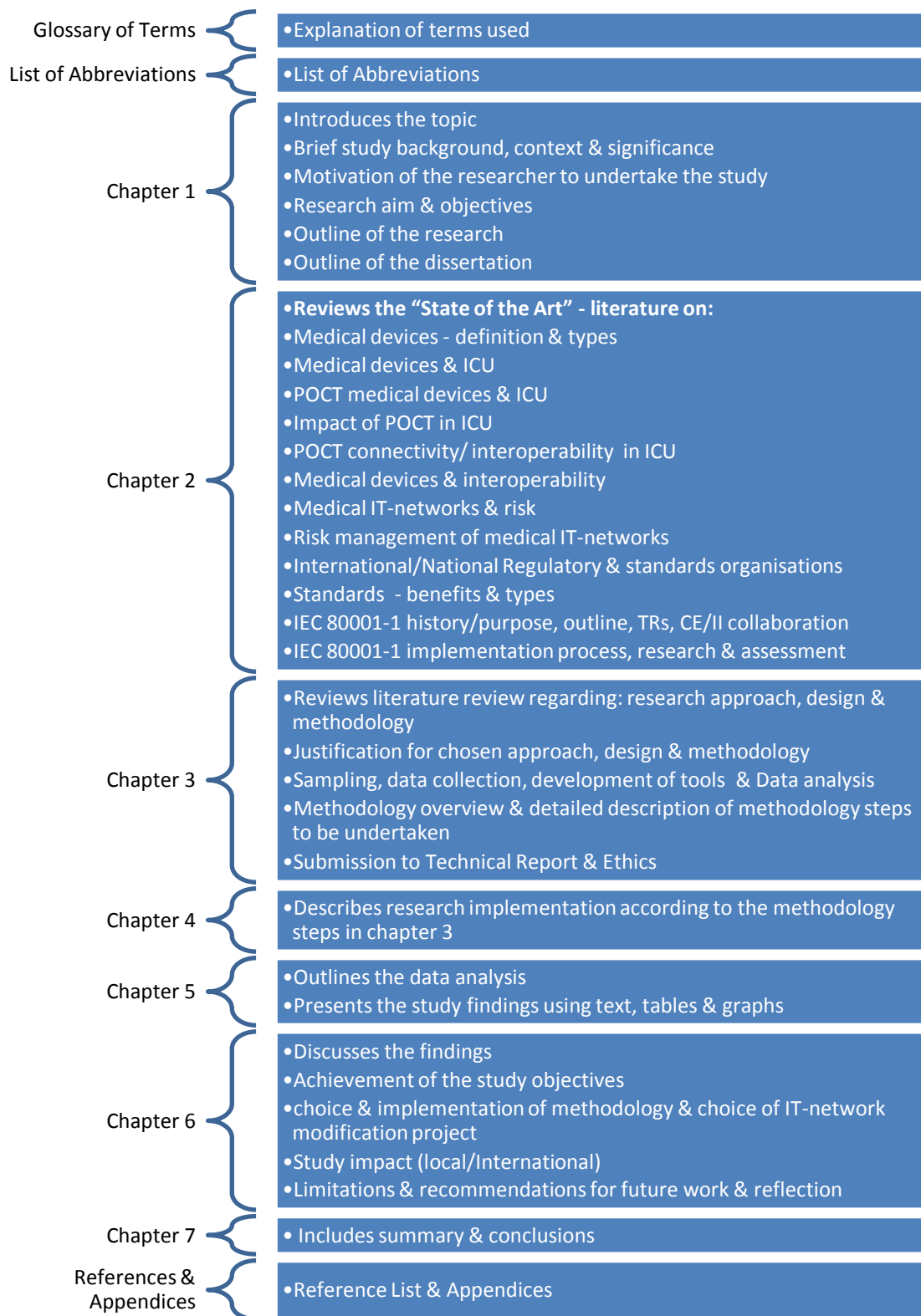


Figure 1 Outline of Dissertation

1.8 Summary

The increasing use of networked medical devices can introduce new risks to patient safety which can have adverse effects on patients, particularly in the ICU. The International Standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) aims to address these patient safety issues. Implementation of the standard has been slow and it is suggested that an assessment method would assist healthcare organisations in the implementation of the standard. Having provided the background and significance of the study in Chapter 1, Chapter 2 will now review the relevant literature in this area.

Chapter 2 Literature Review

2.1 Introduction

Increasing use of clinical information systems (CISs), electronic health records (EHRs) and medical devices, has resulted in an expansion of the IT-network to support this increased use and extended functionality. This has led to both a need and drive for interoperability to enable systems and devices to communicate within healthcare organisations and across organisation boundaries (Morrissey 2011). Complex network systems incorporating medical devices (known as medical IT-networks) are now common (Rakitin 2009), particularly in high technology areas such as intensive care units (ICUs). Point of care testing (POCT) is also common. The automation of healthcare processes including POCT, was driven by a need to reduce costs (Eagles 2008). However, benefits such as improved patient safety were also identified (Institute of Medicine 2000).

Interoperability also involves risks. The incorporation of medical devices into IT-networks leads to new behaviours and unforeseen consequences (Eagles 2008; ECRI Institute 2013) with challenges and increased risks to patient safety (from adverse events), confidentiality, effectiveness, data and system security (AAMI-FDA 2012). These risks are discussed in sections 2.3 and 2.4. Directives, standards and guidelines have been developed to reduce risks and improve medical device safety (Cahalane 2013). This literature review examines the following key areas:

- Medical Devices - Definition & Types
- Medical Devices & Intensive Care Unit (ICU)
- Point-of-Care Testing (POCT) Devices & ICU
- Medical Devices & Interoperability
- Medical IT-networks incorporating Medical Devices & Risk
- Risk Management of Medical IT-networks
- International/National Regulatory & Standards Organisations
- Standards Development Process & Contribution of this Study
- Standards
- IEC 80001-1 Standard (IEC 2010) & Technical Reports

This chapter ends with a summary (section 2.12).

2.2 Medical Devices – Definition & Types

Medical device directives (MDDs) regulating general medical devices, in-vitro diagnostic devices, and active implantable devices have been issued (The European Parliament & the Council of the European Union 1990; The European Parliament & the Council of the European Union 1998; The European Parliament & the Council of the European Union 1993). Directive 2007/47/EC revised the definition of a medical device. A medical device is:

“any instrument, apparatus, appliance, software, material or other article whether used alone or in combination [.....] for the purposes of:

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment or alleviation of or compensation for injury or handicap*
- *Investigation, replacement or modification of the anatomy or of a physiological process*
- *control of conception*

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means” (European Parliament & the Council of the European Union 2007).

Medical devices range from: radiology equipment, surgical instruments, POCT devices such as arterial blood gas (ABG) analysers, and software such as EHRs and CISs (Mc Cullough 2012).

The inclusion of software in the definition of a medical device in Directive 2007/47/EC (European Parliament & the Council of the European Union 2007) means that software is now subject to the same stringent regulation as other devices. Compliance with regulations and standards is challenging. It is not possible to produce software with no defects and identifying and quantifying the potential consequences of defective software is difficult, because increasing complexity also increases the number of defects (Rakitin 2006). To ensure software is safe and effective, medical device manufacturers (MDMs) require expertise in risk management practices, familiarity with software safety and adoption of a risk management mind-set (Rakitin 2006). The community's struggles to apply the MDD to software as a medical device (SaMD) are on-going. Indeed, a recent proposed document from the International Medical Device Regulator's Forum (IMDRF) suggests a framework to categorize types of SaMD based on their risk profiles, identify controls to address associated risk and assure safety and effectiveness (IMDRF SaMD Working Group N12 2014).

2.3 Medical Devices & ICU

Patient safety and survival rates in ICU can be adversely affected by high levels of patient acuity (Kiekkas *et al.* 2008). Patient acuity means the significance of time and urgency of diagnosis and treatment are essential to patient safety. Moreover, the need for rapid decision making, the safe use of technology and interoperable medical devices including POCT devices are essential in providing high quality safe care. Multiple medical devices and technology are used in ICU (Figure 2).

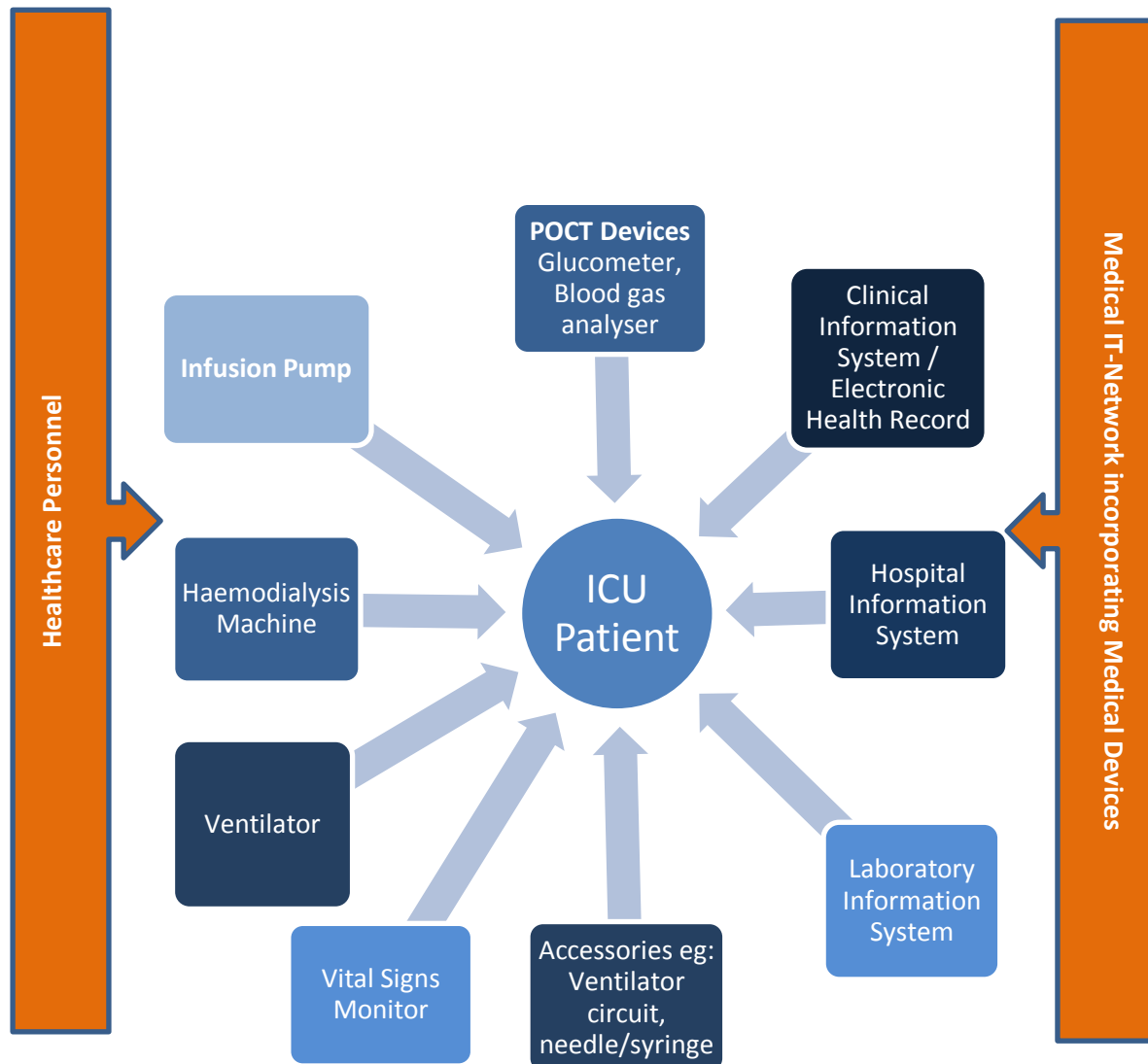


Figure 2 Medical Devices in ICU

ICU personnel interact with these devices, which are increasingly incorporated on the IT-network; this increased complexity increases risks to patient safety. In ICU, medical devices are usually managed by clinical engineering (CE) personnel, POCT devices are managed by POCT or laboratory personnel. Computers and the IT-network are managed by IT staff and the CIS or EHR is managed by

the clinical informatics unit or IT staff. This shared management of medical devices in ICU can lead to a lack of clarity regarding responsibility and accountability for patient safety.

2.4 Development of POCT Devices

POCT is the performance of a diagnostic laboratory test outside the central laboratory and near the site of patient care (Wagar *et al.* 2008). Previously specimens were sent to the laboratory for analysis, and expert laboratory staff managed the analysers (medical devices used for analysis). The slow result turnaround times (Lee-Lewandrowski *et al.* 2003) led to the development of POCT devices to analyse specimens at the point of care and produce results much quicker (Urwyler *et al.* 2009). The types of POCT tests being performed and devices in use is growing rapidly (Kost 2001). Technological advancements have led to device miniaturization, ease of use, increased test sophistication and accuracy and an expanded repertoire of POCT test availability (Kim & Lewandroski 2009; Mc Daniel 2010). In many instances this means management of POCT medical devices is delegated to clinical personnel whose main focus is the patient rather than the analyser (Wagar *et al.* 2008). This could lead to inadequate analyser management adversely affecting the quality of patient results (Lewandrowski 2009).

2.4.1 Impact of POCT in ICU

POCT arterial blood gas (ABG) analysis plays a critical role in defining and assessing clinical diagnoses and in therapeutic monitoring of critically ill patients (De Koninck *et al.* 2012). The direct impact of ABG analysis results on patient care means POCT is preferable to laboratory testing (De Koninck *et al.* 2012). The use of tight glycaemic control using POCT glucose in ICU has demonstrated reduced mortality and morbidity, a reduction in costs and reduced length of stay (Sadhu *et al.* 2008). One of the biggest advantages of POCT is speed (Scalise 2006). Indeed the rapid turnaround time leads to an improvement in patient outcomes (Lee-Lewandrowski & Lewandrowski 2009) by facilitating immediate diagnosis and treatment of critically ill patients (Adekola *et al.* 2012).

However, the rapid availability of results, and the results' immediate therapeutic implications is a risk factor in terms of patient safety and clinical outcomes if errors are made (Meier & Jones 2005). Some of the major risks related to POCT arise from: poor operator competency, lack of proper supervision, governance and accreditation of the POCT service, failure to use quality assurance schemes, inappropriate testing by inexperienced personnel and uncertainty on how to act on results (Academy of Medical Laboratory Science, Association of Clinical Biochemists in Ireland, Irish Medicines Board, Royal College of Physicians in Ireland Faculty of Pathology 2007). POCT connectivity can address some of these issues.

2.4.2 POCT Connectivity/ Interoperability in ICU

POCT connectivity or interoperability is key to managing POCT in terms of: quality control, identification of testing staff and transfer of results over the network to the EHR/CIS at multiple sites (Wagar *et al.* 2008). This leads to improved regulatory compliance, improved clinical outcomes and increased efficiency of hospital operations (Lewandrowski 2009). Electronic patient identification and download of results to the CIS from connected POCT devices (Wagar *et al.* 2008), minimises the error prone transcription of results into the patient record. Transcription errors (errors made in inputting the results or inputting results in the wrong patient chart) can negatively impact on patient care (MacMahon *et al.* 2012) resulting in incorrect or inadequate treatment. POCT device network connectivity enables efficient remote diagnostics and device management by laboratory staff (Grimes 2006).

POCT data management systems have become increasingly complex, allowing the interface of multiple POCT devices from different manufacturers to a central data manager that is bi-directionally interfaced to the laboratory information system (LIS) and hospital information system (HIS) (Kim & Lewandroski 2009; Wagar *et al.* 2008). Without connectivity to LIS or HIS, POCT results may only be available to the clinician performing the analysis, results may be unavailable to other care providers and may be excluded from the patient's EHR (Kim & Lewandroski 2009). This is because patient results held on POCT results printouts issued from the analyser at the time of testing may not be filed in the patient record. POCT connectivity can also introduce new risks which must be identified and managed if patient care is not to be adversely affected, more about this in Section 2.6.

2.5 Medical Devices & Interoperability

The widespread adoption of health information technology (HIT), to achieve the benefits of improved patient safety and quality of care, (AAMI-FDA 2012; West Health Institute 2013) is driving the requirements for interoperability. Interoperability is the essential factor in creating the infrastructure to produce, transmit, store and manage health related information (U.S. Department of Health & Human Services (DHHS) Office of the National Coordinator for Health Information Technology 2008). Interoperability ranges from sharing of information between systems, to control of medical devices by other devices (Rakitin 2009). The move from discrete medical devices to integrated devices and systems, means increased automation, and more medical data being collected, analysed, stored and transmitted (Grimes 2006).

Interoperability enables effective sharing of health information ensuring the delivery of safe, high quality care to patients and the timely and accurate monitoring and planning of services (Health

Information & Quality Authority (HIQA) 2011). The benefits of integrated devices and interoperability include: automatic charting of data such as physiological data to EHRs, storage, retrieval and remote viewing of data/images, closed loop systems enabling diagnostic devices (e.g. vital signs monitors) to control therapeutic devices (e.g. infusion pumps), and patient alarm management (Grimes 2006). This integration of course can be hazardous, if for example the vital signs monitor fails and results in inadequate or excessive treatment from the connected infusion device. The pitfalls of interoperability are discussed in section 2.6.

2.6 Medical IT-networks & Risk

Initially medical devices were linked on their own network, but the increasing number of devices and networks became unmanageable. This resulted in devices being incorporated into the organisation's general IT-network (MacMahon et al. 2013a). The incorporation of one or more medical devices into an IT-network creates a medical IT-network (International Electrotechnical Commission (IEC) 2010). The purpose of incorporating medical devices on the IT-network is to achieve the benefits of interoperability discussed above (Cooper & Eagles 2011). A medical IT-network communicates information or control to or from devices (e.g. CIS, ventilators, infusion pumps) used for patient diagnosis or treatment (Cooper *et al.* 2011). The increasing number of integrated medical devices and systems leads to an increased dependence on the clinical information maintained and transmitted therein. This can have implications for patient care and business operations should these systems fail (Grimes 2006).

Medical devices are designed and validated for their intended use, however when they are added to the IT-network (with other devices and IT-systems); a new system is created which is outside the parameters of the initial validation (Cooper *et al.* 2011). The safety requirements and constraints identified by MDMs for guaranteeing patient safety of the device, may not control hazards in this new system, and new hazards may emerge from network component interactions that were not considered or validated (Cooper *et al.* 2011). A multi-point connection a main feature of an IT-network is prone to interference and risks from each connection point. This can lead to data loss, corruption and data transfer errors, where data can end up in the wrong patient chart (Ellis 2011) leading to inadequate treatment/misdiagnosis. Indeed, the "*Top 10 Health Technology Hazards for 2014*" includes: data integrity failures in EHRs/health IT-systems and neglecting change management for networked devices/systems (ECRI Institute 2013). Data integrity can be compromised by: data/patient association error, data entry error, missing or delayed data entry and clock synchronisation errors (ECRI Institute 2013). This is particularly important in the case of POCT results sent to the CIS in ICU where the results are acted on immediately.

The introduction of medical devices onto the IT-network can compromise device safety and effectiveness of the device in achieving its intended purpose (MacMahon *et al.* 2012). Updates (e.g. software) or modifications made to one device/system can have inadvertent consequences on other connected devices/systems such as unintended operation of devices, mutual interference between devices/systems, and interactions between devices (ECRI Institute 2013; Eagles 2008; Ellis 2011). A resultant network failure can lead to adverse events regarding ventilators, infusion pumps, bar coding/scanning technology, and loss of patient data from the CIS (The Joint Commission 2008). Additional risks associated with networked devices include: security risks, threats and vulnerabilities (Finnegan *et al.* 2013) with threats (e.g. viruses) to both patient confidentiality and data security (AAMI-FDA 2012). Also unmanaged contention for network resources can cause applications to lose network communication, leading to delays in information flow between systems and devices. Issues with semantics and accuracy, timing and format of communicated data can cause problems for patient care (Eagles 2008; Ellis 2011).

The problems associated with the incorporation of medical devices into IT-networks are outlined in the very important International Standard IEC 80001-1 *“Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities”* (International Electrotechnical Commission (IEC) 2010). These include:

- Lack of consideration of IT-network risks during assessment of clinical risk.
- Lack of support from MDMs for incorporating devices on the IT-network in providing adequate information.
- Incorrect operation or degraded performance due to incompatibility of incorrect configuration.
- Incorrect operation due to combining medical device software and other software on the same IT-network.
- Lack of security controls on medical devices
- Conflicts between the requirement for strict change control of medical devices and the need for quick responses to cyber-attacks.

This standard and how it relates to this study are discussed in section 2.11. It is vital that risks from incorporating devices on the IT-network are managed to minimise patient harm.

2.7 Risk Management of Medical IT-networks

Healthcare organisations need to take responsibility for the functioning of the network that they install and for managing the risks related to connecting multiple devices from multiple manufacturers, to ensure those devices work safely and effectively (Rakitin 2009). Risk management involves: identifying the risks, analysing the risks, and implementing control measures to eliminate or reduce the risks. According to Boehm (1991) risk management also involves risk prioritisation and monitoring. Moreover, risk management means overcoming interoperability challenges (AAMI-FDA 2012) such as patient data mismatches and interoperability failures with medical devices, EHRs and other HIT systems (ECRI Institute 2012). Risk management must be applied to all elements of the medical IT-network including infrastructure and non-medical functions (Cooper *et al.* 2011). A risk management plan must incorporate identification of safety critical software components and data, which once identified may require additional assessment and testing (Rakitin 2006). Safety critical components include: software whose failure can directly compromise safety requirements, and software used to mitigate failures in sub-systems such as memory leak detection software (Rakitin 2006). Safety critical data includes: results, algorithm / calculation data, data ascertaining probability of occurrence of potential hazards and patient demographic data (Rakitin 2006).

Increased collaboration and sharing of information between stakeholders is required to effectively manage risk and address the problems associated with networked devices (Rakitin 2009). IT and CE staff must share information regarding the medical IT-network, device manufacturers must share specific technical information outlined in the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) and clinicians must share information regarding actual use of the device in the particular environment, situation and workflow (Rakitin 2009). Appropriate change management processes involving clinical users, CE and IT personnel are also essential to minimise the risks (ECRI Institute 2013). CE/IT and medical/nursing personnel must be aware of how their work affects other operations, patient care and work processes and must work together to prevent IT-related changes from negatively impacting networked medical devices/systems and the patients affected by these devices/systems (ECRI Institute 2013). Users must also be aware of the safety risks and preventable adverse events associated with networked devices and find ways of identifying and managing these risks before serious patient harm results (The Joint Commission 2008). Identifying problems and using proven techniques such as fault tree analysis (FTA) to analyse hazards will improve risk management of medical devices (Rakitin 2006) on the IT-network.

The risk of data integrity loss can be mitigated by assessing clinical workflow and use of data by clinical staff, testing the system and associated interfaces to verify functionality, providing user

training/support and including a feedback mechanism for reporting problems (ECRI Institute 2013; The Joint Commission 2008). Additionally, the Joint Commission (2008) suggest further actions to prevent harm from implementations of health information technology (HIT):

- involving clinical users in all project phases
- assessing technology requirements and site visits
- monitoring for problems
- developing/ communicating policies for roles / responsibilities,
- implementing alert systems
- protection of data entry staff from distractions
- use of error tracking
- evaluation and root cause analysis and
- re-evaluation of security protocols and Health Insurance and Portability Accountability Act (HIPAA) compliance.

To manage the security risks associated with medical IT-networks, the U.S. Food & Drug Administration (FDA) produced cyber-security guidance outlining software maintenance actions required to address cyber-security vulnerabilities for networked devices (US FDA 2005). However, this guidance did not address other risks to patient safety from networked devices. The standard that relates to risk management of medical IT-networks is IEC 80001-1 *“Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities”* (International Electrotechnical Commission (IEC) 2010). Before we discuss this standard (Section 2.11), we will examine medical device regulation and standards. Medical devices are highly regulated internationally and nationally. Who are these regulatory bodies and what are they responsible for?

2.8 International & National Regulatory & Standard Organisations

2.8.1 International Regulatory & Standard Organisations

International medical device regulatory bodies relevant to this dissertation include: International Electrotechnical Commission (IEC), International Organization for Standardization (ISO).

The **International Electrotechnical Commission (IEC)** prepares and publishes consensus based International standards and manages conformity assessment systems for electrical, electronic and

related technologies (IEC 2014). The IEC collaborates with other world standards development organisations such as ISO to ensure International standards fit together and complement each other (IEC 2014). Further information is available at: <http://www.iec.ch/> (International Electrotechnical Commission (IEC) 2014b).

Another International standards organisation is the **International Organization for Standardization (ISO)**, which consists of a network of national standards bodies. ISO standards are developed by international experts through technical committees (TCs) and working groups (WGs). Of particular interest to this project are TC 215 – Health Informatics, WG 4 (deals with confidentiality, integrity, availability, accountability, security management and information systems safety), and WG 7 which deals with medical devices. ISO also provides standards relevant to the healthcare domain (International Organization for Standardization (ISO) 2013). Further information is available at: <http://www.iso.org/iso/home.html> (International Organization for Standardization (ISO) 2013).

2.8.2 National Regulatory and Standards Organisations

The Irish National regulatory body is the **Irish Medicines Board (IMB)**, whose mission is:

“to protect and enhance public and animal health through the regulation of medicines, medical devices and healthcare products” (IMB 2014).

The objective of the IMB is to ensure the quality, safety and efficacy of medicines available in Ireland. The IMB is also the *“Competent Authority”* for the regulation of medical devices/cosmetic products (IMB 2014), ensuring all medical devices sold in Ireland comply with legislation. The IMB provides guidance for classifying medical devices covered by the medical device directives (IMB 2009). MDMs must notify the IMB of adverse events related to their devices. Further information is available at: <http://www.imb.ie/> (IMB 2014).

The **National Standards Authority of Ireland (NSAI)** is Ireland’s official standards body (National Standards Authority of Ireland (NSAI) 2014). The NSAI is the national certification authority for CE marking, providing a certification service to enable businesses demonstrate that Irish goods and services conform to applicable standards. The NSAI’s mission is to enable Ireland to implement best international standards and protect Irish consumers by setting regulatory standards and enforcing measurement accuracy. Further information is available at: <http://www.nsai.ie/> (National Standards Authority of Ireland (NSAI) 2014).

The **Health Information and Quality Authority (HIQA)** are an independent authority responsible for driving quality, safety and accountability in health and residential services in Ireland (Health

Information & Quality Authority (HIQA) 2013). Two of HIQA's main areas of responsibility are: 1) developing and setting standards for health and social services and 2) monitoring healthcare quality and safety, and investigating any concerns about healthcare services (Health Information & Quality Authority (HIQA) 2012b). Further information is available at: <http://www.hiqa.ie/> (Health Information & Quality Authority (HIQA) 2013).

The work of these regulatory and standards organisations yields standards for medical device manufacturers, IT, risk management, POCT and healthcare. Prior to discussing these standards it is necessary to briefly describe the standards development process and the benefits of standards.

2.9 Standards Development Process & Contribution of this Study

An International Standard is a standard adopted by an International standards organization and made available to the public (International Electrotechnical Commission (IEC) 2014b). The stages of standard development (International Electrotechnical Commission (IEC) 2014a) are outlined in Figure 3. These stages are described, as this study will contribute to a technical report (TR) which is being developed (section 3.8) which follows a similar development process. As depicted (Figure 3); a new work item proposal proceeds to a working draft, then a committee draft for comments, then to a committee draft for vote, and proceeds to final draft International Standard, which once approved is published (International Electrotechnical Commission (IEC) 2014a).

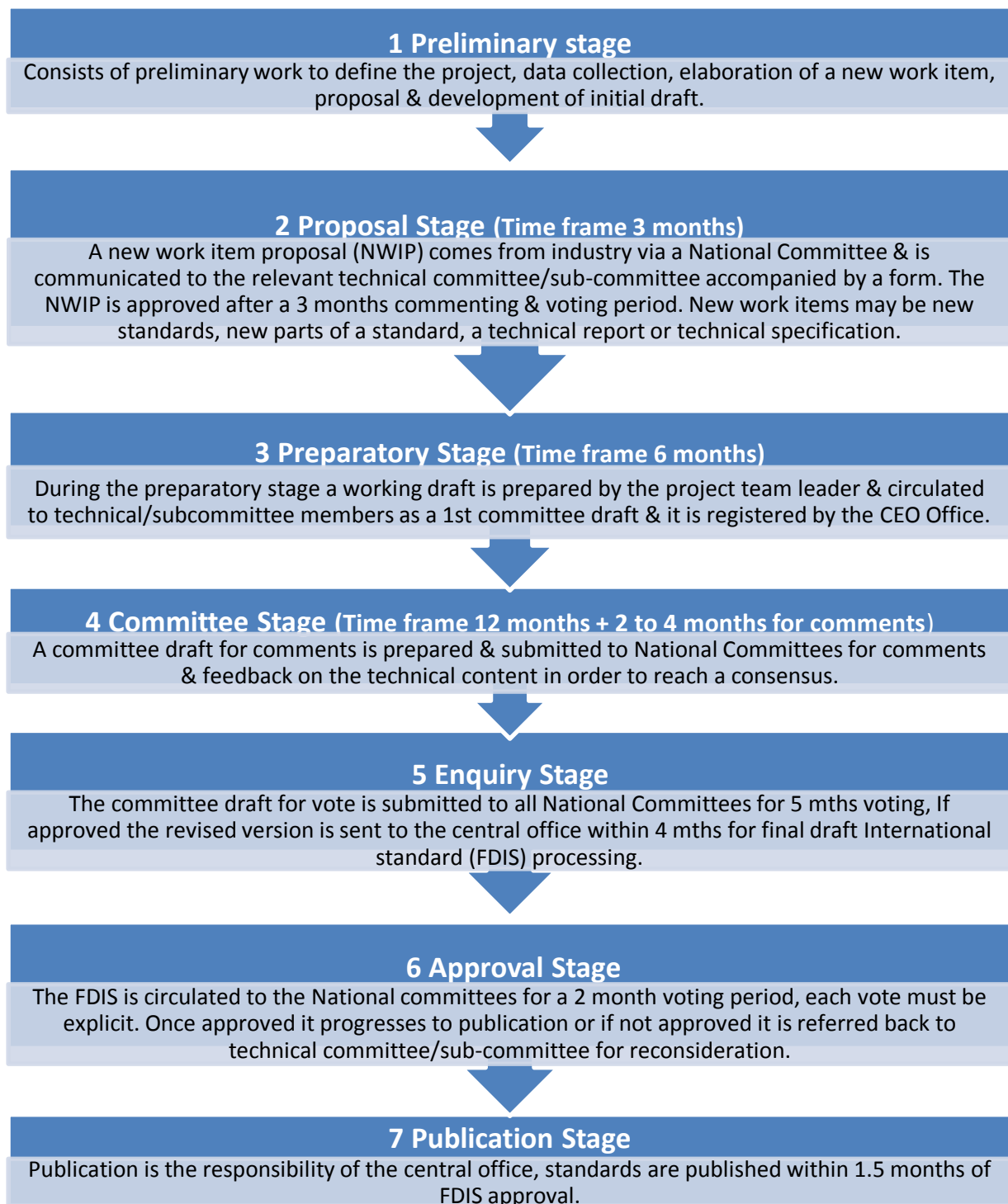


Figure 3 IEC Standard Development Stages (International Electrotechnical Commission (IEC) 2014a)

The ISO standards development process (Appendix A) is similar to that of the IEC. ISO also produce technical specifications (TSs) and technical reports (TRs). An ISO/TR Technical Report is:

“An informative document containing information of a different kind from that normally published in a normative document” (International Organization for Standardization (ISO) 2014a).

A technical report ISO/IEC TR 80001-2-7 *“Application of risk management for IT-networks incorporating medical devices – Part 2-7: Application Guidance – Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1”* is being developed. This technical report is proceeding through the development stages outlined (Figure 3) and it is anticipated that the findings from this study will contribute to this important international work (see section 3.8).

2.10 Standards

The sheer volume of standards relevant to medical devices, POCT devices, risk management of devices/network, device interoperability and patient safety is enormous. Magrabi *et al.* (2013) identified 27 standards across five countries addressing patient safety alone and highlighted the lack of health-IT standards (Magrabi *et al.* 2013). A full description of all these standards is beyond the scope of this dissertation, thus the most relevant standards are summarised below. But first, a summary of the benefits of standards is provided (section 2.10.1).

2.10.1 Benefits of Standards

International standards give state of the art specifications for products/services and good practice ensuring products/services are safe, reliable and fit for purpose (ISO 2013). Interoperability standards provide structured content and formatting to ensure the sending and receiving system accurately compiles and interprets a message, to meet information sharing needs across healthcare settings (Halley *et al.* 2009). Compliance with International standards/regulations for software development and risk management will ensure there is identification of potential hazards and implementation of effective mitigations in order to reduce patient safety risks from defective software (Rakitin 2006).

Healthcare standards aim to improve the quality of patient care, improve patient safety and reduce adverse events and errors (Health Information & Quality Authority (HIQA) 2012b). Quality and risk management standards outline requirements for service providers, ensuring health services are safe and of an acceptable quality (Department of Health & Children (DOHC) 2008). POCT standards ensure that quality management systems of POCT services are in place to manage the risks associated with POCT and outline the management/technology requirements of such systems (International Organization for Standardization (ISO) 2006). POCT connectivity standards identify

specific, essential requirements for safe POCT connectivity (The National Committee for Clinical Laboratory Standards (NCCLS) NCCLS 2001). Process assessment standards define concepts, and provide minimum requirements for performing an assessment, to ensure consistency and repeatability of capability ratings (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2004).

Medical device standards outline general requirements for safety and essential performance criteria for medical electrical equipment (International Electrotechnical Commission (IEC) 2012a). Risk management standards direct risk management activities for medical devices and medical IT-networks (International Organization for Standardization (ISO) 2007a; International Electrotechnical Commission (IEC) 2010).

2.10.2 Medical Device Manufacturer & IT Standards

Medical device manufacturers (MDMs) must ensure their technology/devices are safe and effective and quality process requirements such as enhanced quality systems, use of good manufacturing practices and reporting of any adverse events to the relevant regulatory body are adhered to (Cooper *et al.* 2011). Premarket aspects of medical device product safety, development and manufacture are outlined in the International Standard IEC 60601-1: *“General Requirements for Basic Safety and Essential Performance”* (International Electrotechnical Commission (IEC) 2005). MDMs must comply with this standard which also details the information that MDMs must provide for devices to be connected to the IT-network (International Electrotechnical Commission (IEC) 2005).

The standard; ISO 13485 *“Medical devices - Quality management systems - Requirements for Regulatory Purposes”* (International Organization for Standardization (ISO) 2003) outlines quality management, general aspects for medical devices, and specifies requirements of quality management systems. According to Cahalane (2013) compliance with ISO 13485 demonstrates compliance with medical device directives (section 2.2).

The ANSI/AAMI/IEC 62304: *“Medical Device Software - Software Life Cycle Processes”* standard defines the life cycle requirements (processes, activities, and tasks) for medical device software (American National Standards Institute (ANSI) *et al.* 2006). Additionally, the *“General Principles of Software Validation: Final Guidance for Industry and FDA Staff”* provides guidance on software validation and verification processes (U.S. DHHS FDA 2002).

The standard ISO 14971 *“Medical Devices – Application of Risk Management for Medical Devices”* (International Organization for Standardization (ISO) 2007a) outlines how risk management

principles should be applied to the design, manufacture, deployment and decommissioning of medical devices. Indeed, this standard has become the globally recognised standard used by manufacturers in implementing and operating a medical device risk management strategy (Sidebottom 2011). Compliance with ISO 14971 (International Organization for Standardization (ISO) 2007a) enables MDMs to prove their medical devices are safe for use, as the standard outlines the risk management process of a medical IT-network and its focus is patient safety (Cooper *et al.* 2011). Software risk management must focus on severity or risk of harm rather than probability (Rakitin 2006), and change the design to eliminate risks or incorporate protective measures in the device or manufacturing process (International Organization for Standardization (ISO) 2007a). The risk management process outlined in ISO 14971 (International Organization for Standardization (ISO) 2007a) involves: risk identification (hazard list with quantification of harm severity), analysis, evaluation and control, evaluation of residual risk acceptability, go-Live, and monitoring.

IT service management standards ISO/IEC 20000-1 "*Information Technology - Service Management - Part 1 Specification*" and ISO/IEC 20000-2 "*Information Technology - Service Management - Part 2 Code of Practice*" (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2005a; International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2005b), outline how the risk management process can be incorporated into the overall network management process. Cooper *et al.* (2011) suggest that many IT organisations use these two standards along with the methodology outlined in the IT Infrastructure Library (ITIL) (IT Infrastructure Library (ITIL) 2014) when planning and integrating life cycle technology.

ISO/IEC 15408-1 "*Information technology -- Security Techniques -- Evaluation Criteria for IT Security - Part 1: Introduction and General Model*" and ISO/IEC 15408-2 "*Information technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Functional Components*", are concerned with security as a key network characteristic which must be managed (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2009; International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2008). Implementing these standards for medical device manufacturers and IT will reduce the risks to patient safety from medical devices.

2.10.3 Healthcare Domain Standards

There are a plethora of standards related to patient safety, security, risk, medical devices and information sharing. The standard ISO 27799 "*Health Informatics Information Security Management in Health using ISO/IEC 27002*" (International Organization for Standardization (ISO) 2008) defines

guidelines to support the interpretation and implementation of ISO/IEC 27002 *“Information Technology Security Techniques: Code of Practice for Information Security Controls”* (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2013). ISO 27799 (International Organization for Standardization (ISO) 2008) specifies controls for managing health information security and provides best practice guidelines which, if implemented will enable healthcare organisations to maintain the confidentiality, integrity and availability of health information. A technical specification (TS) ISO/TS 25238 *“Health Informatics – Classification of Safety Risks from Health Software”* provides guidelines on the analysis and categorisation of hazards and risks to patients from health software (International Organization for Standardization (ISO) 2007b).

Technical standards for information systems outlining how patient information can be accurately and safely transmitted between organisations and advocating a standard exchange format for healthcare information transfer have also been published (Health Information & Quality Authority (HIQA) 2010; Health Information & Quality Authority (HIQA) 2012a). Use of standards or regulations related to the privacy and security of EHR data have been reported (Fernández-Alemán *et al.* 2013). Standards for interoperability will improve the safety, effectiveness, and efficiency of medical technology while ensuring security and confidentiality are maintained (AAMI-FDA 2012).

The *“National Standards for Safer Better Healthcare”* (Health Information & Quality Authority (HIQA) 2012b), address quality and safety in healthcare, mandating that healthcare providers undertake a self-assessment to identify and prioritise areas of risk to service users for immediate action (Health Information & Quality Authority (HIQA) 2012b).

2.10.4 POCT Standards

The increasing number and type of POCT medical devices in use, led to the development of the Clinical Laboratory Standards Institute (CLSI) guideline *“Selection, Criteria for Point of Care Testing Devices: Approved Guideline (POCT09-A)”* (CLSI 2010). The guideline provides guidance on evaluating, procuring, and implementing POCT, optimising devices to the setting/patient population, consideration of personnel needs, associated risks, ensuring patient safety, and regulatory and quality compliance (Mc Daniel 2010).

Other International standards pertaining to POCT include: ISO 22870 *“Point of Care testing (POCT) – Requirements for quality and competence”* (International Organization for Standardization (ISO) 2006), outlining management/technical requirements of POCT in healthcare (International Organization for Standardization (ISO) 2006) and the similar standard for laboratories ISO 15189: *“Medical Laboratories – Particular Requirements for Quality and Competence”* (International Organization for Standardization (ISO) 2012).

POCT1-A: *“Point-of-Care Connectivity; Approved Standard”* (NCCLS 2001) provides the basis for seamless connectivity/interoperability between POCT devices from different vendors, data managers and clinical results management systems. However, according to Wagar *et al.* (2008) the complexity of the document and the use of technical engineering language made it difficult for healthcare staff to understand and resulted in the development of a more user friendly guide POCT2A *“Implementation Guide Of POCT 01 For Health Care Providers”* (CLSI 2008). Integrating these connectivity standards for bidirectional information exchange in POCT along with implementation of user defined error prevention systems on POCT devices can reduce medical errors in POCT (Kost 2001) and lead to improvements in patient safety.

The standard *“Additional Standards for Point-of-Care Testing (POCT) facilities”* (Clinical Pathology Accreditation (CPA) UK Ltd 2010) is an accreditation standard for POCT. Irish guidelines provide guidance on regulatory requirements and implementation of POCT (Academy of Medical Laboratory Science, Association of Clinical Biochemists in Ireland, Irish Medicines Board, Royal College of Physicians in Ireland Faculty of Pathology 2007; Health Service Executive (HSE) *et al.* 2009). These standards and guidelines define how POCT should be implemented and managed, outline requirements (including documentation) of operator training, certification and maintenance of competence.

Despite all these standards and others, there are still real risks with medical IT-networks (Magrabi *et al.* 2013) in healthcare, which if not managed can result in serious patient harm.

2.11 IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) - History & Purpose

Until the publication of IEC 80001-1 *“Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities”* (International Electrotechnical Commission (IEC) 2010) no standard outlined how medical devices could be connected to the IT-network to achieve interoperability without compromising the organisation/healthcare delivery in relation to safety, effectiveness and data/ system security (International Electrotechnical Commission (IEC) 2010). The need for a standard arose in 2001, from MDM and healthcare facilities experiencing problems with their medical devices and hospital networks and identifying the network and/or interactions with other devices on the network as the cause of these problems (Cooper & Eagles 2011). Contributing to the problem was the divided technology support in hospitals with IT managing computer hardware and the network and clinical engineering managing medical devices (Cooper & Eagles 2011). Without a collaborative framework there was no means of identifying and mitigating against these problems (Cooper & Eagles 2011). The goal of IEC 80001-1 is the need to

consider the potential safety impacts in the design and implementation of IT-networks incorporating medical devices prior to putting them into use and to improve patient safety in a networked environment (Cooper & Eagles 2010).

2.11.1 Outline of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010)

IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) recognises that medical devices are incorporated into IT-networks to achieve interoperability. It defines the roles, responsibilities and activities which are required for risk management of medical IT-networks to address the key properties of a medical IT-network (Table 4) identified in the standard (International Electrotechnical Commission (IEC) 2010).

Key properties of a medical IT-network (International Electrotechnical Commission (IEC) 2010)	
Term	Definition
Safety	<i>“freedom from unacceptable risk of physical injury or damage to the health of people, or damage to property or the environment”</i>
Effectiveness	<i>“ability to produce the intended result for the patient and the responsible organisation”</i>
Data and system security	<i>“operational state of a medical IT-network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity and availability”</i>

Table 4 Key properties of a medical IT-network (International Electrotechnical Commission (IEC) 2010)

The standard defines harm as:

“physical injury or damage to the health of people, or damage to property, or the environment or reduction in effectiveness or breach of data and system security” (International Electrotechnical Commission (IEC) 2010).

Maintaining the key properties is achieved by identifying and controlling conditions that could adversely impact them (Cooper *et al.* 2011). Safeguarding the key properties is the responsibility of the responsible organisation or healthcare organisation (International Electrotechnical Commission (IEC) 2010).

IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) takes a life cycle approach to risk management of the medical IT-network and therefore is applicable on inception of the medical IT-network, addition of medical device(s) on an IT-network, when medical devices already on a medical IT-network are changed/modified or undergo maintenance and when medical devices are removed

from an IT-network (International Electrotechnical Commission (IEC) 2010). Therefore, following any IT-network modifications, on-going monitoring of the new patient environment is required to ensure the key properties are not adversely affected (Cooper *et al.* 2011). The introduction of IEC 80001-1 (2010) gives healthcare organisations a comprehensive framework for managing clinical and security related risks throughout the IT-network life cycle, thus improving their ability to provide safe and effective healthcare (Ellis 2011). In addition, by defining the roles and responsibilities of:

- the responsible organisation,
- top management,
- the IT-network risk manager,
- medical device manufacturers (MDMs) of medical devices connected to the network, and
- network suppliers

the standard aims to assist healthcare organisations to improve risk management of the IT-network to improve patient safety (Eagles 2008).

IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) also advocates greater levels of communication between healthcare organisations, MDMs and providers of IT-networks to undertake risk management of medical IT-networks (Cooper *et al.* 2011). The standard outlines the information that MDMs are expected to provide to healthcare organisations, if this information is insufficient to manage potential hazards, the standard mandates that the information be provided by MDMs under the auspices of a responsibility agreement (International Electrotechnical Commission (IEC) 2010). IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) provides a framework that defines consistent expectations between MDMs and healthcare organisations. If implemented the standard helps MDMs understand expectations and assists them in preparing and providing the required information, leading to greater customer satisfaction and improved patient safety (Sidebottom 2011). The risk management process described in IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) is based on the process used by MDMs outlined in ISO 14971 (International Organization for Standardization (ISO) 2007a) discussed previously. When implementing the risk management process the healthcare organisation must consider the impact of network problems on the key properties in order to identify any ensuing hazards (Cooper *et al.* 2011).

2.11.2 IEC 80001-1 Technical Reports (TRs)

Various technical reports have been published to assist hospitals and CE/IT departments to implement the standard IEC 80001-1 (IEC 2010). These include:

- IEC TR 80001-2-1 - provides a ten step process governing risk analysis, risk evaluation and risk control elements of life cycle risk management processes and gives practical applications and examples of medical IT-network risk management (International Electrotechnical Commission (IEC) 2012b).
- IEC TR 80001-2-2 - offering guidance for disclosure/communication of medical device security needs, risks and controls (International Electrotechnical Commission (IEC) 2012c).
- IEC TR 80001-2-3 - delivering guidance related to wireless networks (International Electrotechnical Commission (IEC) 2012d).
- IEC TR 80001-2-4 - issuing general implementation guidance (International Electrotechnical Commission (IEC) 2012e).
- ISO TR 80001-2-6 - guidance for responsibility agreements (under development) (International Organization for Standardization (ISO) 2014b).
- ISO TR 80001-2-7 - guidance for healthcare organisations on assessment of conformance with IEC 80001-1 (under development) (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014).

2.11.3 CE-IT Collaboration & IEC 80001-1 Implementation

Implementing IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) into existing activities requires greater collaboration between IT and CE personnel to identify how the new requirements can be fulfilled (Cooper *et al.* 2011). Indeed CE and IT knowledge and skills are similar and include: project management, disaster recovery, HIPAA compliance, device risk assessment, adverse event investigation, understanding/complying with regulations, interoperability of standards and accreditation plans, user/service provider training, change management and service support (Cooper *et al.* 2011). Grimes (2006) agrees suggesting that these combined CE-IT competencies are essential for the delivery of safe, efficient quality patient care in the current networked environment.

Increasingly CE/IT programs are uniting and supporting increased collaboration to sustain a safe patient care environment with the deployment of integrated, interoperable clinical processes (Cooper *et al.* 2011). CE-IT collaboration can be challenging as CE programs focus on individual medical devices and risk management of life critical assets, while IT programs focus on network infrastructure and mission critical applications (Cooper *et al.* 2011). Nonetheless, the convergence calls for a change in business processes and innovation of service provisions to provide a common service (Cooper *et al.* 2011). This service includes: freedom from unacceptable risk, effective patient care/organisation operation and secure transmission/storage of data (Cooper *et al.* 2011). This can

lead to better co-ordination of clinical systems integration and infrastructure support (Grimes 2006), fostered by collaborative functions and practice (Association for the Advancement of Medical Instrumentation (AAMI) *et al.* 2014). The inclusion of medical devices, network and EHRs in the same domain requires revised CE-IT operations including: analysing overall system vulnerability, single point of failure assessment, combined technical documentation, management of vendors' relationships and first call responsibility (Cooper *et al.* 2011).

Although IEC 80001-1 (IEC 2010) advocates greater collaboration between stakeholders and adds responsibilities to personnel (IT) managing networks and those managing medical devices (Clinical engineering personnel), the expectation is that these responsibilities will be incorporated into existing activities (Cooper *et al.* 2011). As CE increasingly integrates with computers, closer relationships among personnel will come from CE personnel's understanding of medical devices and patient dynamics, and IT personnel's understanding of computer hardware/software and information processing (Grimes 2006).

2.11.4 IEC 80001-1 (IEC 2010) Implementation Process

Cooper *et al.* (2011) provide advice on getting started with IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) implementation and suggest the first step is defining roles and responsibilities, followed by establishment of a project charter divided into phases:

- 1) assess the current state,
- 2) create and adapt risk management policy and process tools, and
- 3) transition the pilot to operational mode.

Ahlbrandt & Röhrig (2013b) suggest starting with a risk assessment of a small medical IT-network project. Other possible starting points for implementation suggested include:

- 1) Firstly to convene a multidisciplinary team and draft an organisational risk management policy and then use this policy in an IT-network modification project
- 2) Start with a list of hazards or faults and mitigate for those, or alternatively
- 3) start with redesigning the IT security planning process for medical devices to guard against virus attacks (Cooper & Eagles 2011).

The voluntary nature of IEC 80001-1 (IEC 2010) may negatively impact implementation (Cooper & Eagles 2011). Implementing IEC 80001-1 (IEC 2010) does not mean the network is safe and effective as the standard is designed to be a tool not a set of criteria for success (Cooper *et al.* 2011). Even by implementing IEC 80001-1 (IEC 2010) it is possible to create an unsafe network, if insufficient information is available, poor decisions are made and careful consideration of every

network/network issue is overlooked (Cooper *et al.* 2011). The standard does however provide a prescriptive set of tasks for the entire medical IT-network risk management process (Cooper & Eagles 2011).

2.11.5 IEC 80001-1 (IEC 2010) Implementation Research

Evidence of IEC 80001-1 (IEC 2010) implementation is scarce. Ahlbrandt & Röhrig (2013b) applied IEC 80001-1 (IEC 2010) to a small IT-network project involving a chain of medical devices connected to a hospital IT-network in Germany. The risk assessment was carried out on a bedside setup of a nitric oxide dispenser connected to a respirator and workstation with data transfer across the network and the findings were compiled in a risk management file (Ahlbrandt & Röhrig 2013b). In applying IEC 80001-1 (IEC 2010), they identified 11 potential risks that could result in patient harm and defined counter measures for each (Ahlbrandt & Röhrig 2013b). While acknowledging the extra effort that risk management as per IEC 80001-1 requires, Ahlbrandt & Röhrig (2013b) report that the benefits of identifying the risks and controls in terms of reducing potential patient harm and financial liabilities, outweighed the cost of delaying device implementation. Also the process improved communication and transparency among the staff involved (Ahlbrandt & Röhrig 2013b); such improved collaboration is exactly what the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) advocates.

Hegarty *et al.* (2014) assessed a hospital's medical IT-network risk management practice relating to the management of a CIS with IEC 80001-1 (IEC 2010) using an assessment framework consisting of a PRM, PAM and assessment method under development by (MacMahon *et al.* 2013b). The assessment identified inadequate documentation of risk management policy, a need for different groups to jointly address risk related issues specific to IT-network technology management and weaknesses in how medical IT-network risk management is managed (Hegarty *et al.* 2014). Implementation of a single policy; outlining CE/IT roles in jointly managing the system (bedside devices, computers/network) is suggested to improve the management process (Hegarty *et al.* 2014). Improvements reported include: mapping of the IT-network configuration, review and improvements of the CIS change control process, review of responsibility agreements with the CIS supplier, and upgrade of power management of network components with a policy for on-going maintenance (Hegarty *et al.* 2014).

2.11.6 The Need for an Assessment Method for IEC 80001-1 (IEC 2010)

This lack of evidence of implementation of IEC 80001-1 (2010) is due to a lack of a process assessment method (MacMahon *et al.* 2012) to assess risk management processes against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). Healthcare provision is based on clinical processes which are interactions between patients, healthcare providers and technologies (Marx & Slonim 2003). These processes can be analysed to identify potential risks to patient safety and care. Various process analysis methods exist (Marx & Slonim 2003; Goddard 2000). Indeed, prospective process analyses are a requirement of organisational patient safety plans (The Joint Commission on Accreditation of Healthcare Organisations 2000).

Process analysis or assessment is particularly important in the case of medical IT-network modifications to avoid patient safety critical adverse events. The International standard for performing process assessment is ISO/IEC 15504-2 "*Software Engineering - Process Assessment - Part 2: Performing an Assessment*" (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). The standard ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003) describes two aspects of process assessment; namely process (consisting of purpose and outcomes) and capability levels (1 - 6), defines the requirements for assessment performance and describes the necessary development of a Process Reference Model (PRM), Process Assessment Model (PAM) and assessment method to be used. MacMahon *et al.* (2013b) highlighted the lack of a process assessment method for the risk management roles, responsibilities and activities of healthcare organisations outlined in IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) to manage risks of medical IT-networks.

To address the need to assess how effectively these processes were being carried out, a PRM and PAM were developed (MacMahon *et al.* 2013b; MacMahon *et al.* 2013c) in line with ISO/IEC 15504 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). The PRM contains a description of the 14 processes (Table 5) and includes the purpose and outcomes of each process (MacMahon *et al.* 2013b; MacMahon *et al.* 2013c).

IEC 80001-1 Processes (International Electrotechnical Commission (IEC) 2010)	
Risk Management Policy Processes	
1.	Risk Management Policy
Medical IT-network Risk Management Planning Processes	
2.	Medical IT-network Risk Management Planning
3.	Medical IT-network Documentation
4.	Responsibility Agreements
5.	Organisational Risk Management
Medical IT-network Risk Management Processes	
6.	Medical IT-network Risk Management
7.	Risk Analysis & Evaluation
8.	Risk Control
9.	Residual Risk
Change Release Management & Configuration Management	
10.	Change Release Management & Configuration Management
11.	Decision on how to apply Risk Management
12.	Go-Live
Live Network Risk Management Processes	
13.	Monitoring
14.	Event Management

Table 5 IEC 80001-1 PAM Processes (Mac Mahon *et al.* 2013)

The IEC 80001-1 PAM extends the IEC 80001-1 PRM with the addition of a measurement framework incorporating base practices (activities performed to achieve the process purpose) and work products which are used or produced during the performance of the process (MacMahon et al. 2013b). An IEC 80001-1 PAM sample process “Go-Live” is shown in Appendix B Table 13. Once

validated and approved the IEC 80001-1 PRM and PAM will be incorporated into the IEC 80001-1 (2010) family of standards (MacMahon et al. 2013a; MacMahon et al. 2013b).

The validated IEC 80001-1 PAM will be used to inform the development of an assessment method to which this research will contribute. The assessment method guarantees a standard approach to assessment procedures by defining; roles and responsibilities in the assessment, the scope of the assessment and the questions to be utilised to establish the capability levels related to undertaking each process (MacMahon et al. 2013a). The assessment method will use a set of scripted questions to assess performance of the processes (MacMahon et al. 2013a).

2.12 Summary

The increasing use of interoperable medical devices (including POCT devices) incorporated into the medical IT-network presents challenges to healthcare organisations in terms of managing the potential risks to patient safety, effectiveness and data and system security. In addition, maintaining awareness of, implementation of and compliance with national/international regulations and standards surrounding medical devices, interoperability and risk management is a challenge for healthcare organisations (AAMI-FDA 2012). Implementation of IEC 80001-1 (IEC 2010) by healthcare organisations will improve risk management of networked medical devices and lead to improved patient safety. The next chapter (chapter 3) will outline the research methodology (step-by-step) to be used in this study to develop and validate an assessment method for IEC 80001-1 (IEC 2010). This will be used to assess a healthcare organisation's risk management processes related to a medical IT-network modification project involving networked POCT devices. Chapter 4 will describe the implementation of this methodology using the same step-by-step process.

Chapter 3 Research Design & Methodology

3.1 Introduction

The standard “IEC 80001-1: *Application of Risk Management for IT-Networks incorporating Medical Devices-Part 1: Roles, Responsibilities and Activities*” (International Electrotechnical Commission (IEC) 2010) suggests that compliance be checked by assessment. However to date limited assessment of compliance with IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) has been reported, partly due to the lack of an available assessment method. Risk management of medical IT-networks involves numerous processes (MacMahon et al. 2013b) therefore any assessment developed must follow process assessment standards. This research study will contribute to the development and validation of the assessment method for IEC 80001-1 (IEC 2010) using the IEC 80001-1 PRM and PAM (MacMahon et al. 2013a) and compliant with ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). The study will follow the methodology described in section 3.6.

The process assessment method developed for IEC 80001-1, will include a selection of questions (which must be validated) to determine compliance with the standard IEC 80001 (International Electrotechnical Commission (IEC) 2010). One approach to assessment method validation is to use the consensus approach. The consensus approach in this context involves the circulation and re-circulation of committee drafts of the assessment method to technical committees of international standards organisations until consensus and agreement is reached on the content and the final document is approved. MacMahon et al are pursuing this approach (MacMahon et al. 2013a).

Another approach to validation of the assessment method; which this research will adopt, is to undertake research utilising the developed assessment method to assess a medical IT-network modification project. The resulting knowledge gained could be used to refine the assessment method and the question set. The IT-network modification project on which the assessment will be based and the methodology to be used is described in sections 3.6.3 and 4.2.3.

The main literature review is outlined in chapter 2, however, a short literature review regarding research methodology, outlining the key elements of research: research approach, research design, and methodology is included. Then, application of these elements to the study and justification for choices is provided. Sampling type and strategy to be used is outlined. Data collection methods chosen and reasons for same are explained along with a description of data collection instrument development. An overview of the methodology steps to be undertaken is shown in section 3.6. An outline of each step with links to research elements and other steps is provided. A detailed

description of these steps is provided in Appendix C. In chapter 4, we will return to these steps to discuss the methodology implementation, experiences therein and challenges encountered. Finally, ethical considerations will be discussed at the end of this chapter (Chapter 3).

3.2 Research Approach, Design & Methodology

3.2.1 Research Approach

The main research paradigms are *Positivism*, which underpins quantitative research (Bowling and Ebrahim, 2005), *Interpretivism*, which is the basis of qualitative research (Bowling 2009) and *Pragmatism* which underpins mixed methods research (DePoy & Gitlin 2011). These paradigms are based on philosophical assumptions of the nature of reality (ontology), the boundaries between researcher and participant, and epistemology which is the nature of knowledge or truth and how it is generated (Liamputtong 2013). Knowledge of these paradigms directs researcher decisions regarding the conduct of research.

Positivism advocates the theory of a single reality, which is context neutral, objective, and measurable, boundaries between researcher and participant are controlled, and truth is based on measurable evidence (Edwards 2001). Proponents of the ontological position of objective reality adopt a position of objective detachment, believing this enables the reality to be accurately captured by undertaking quantitative research (Liamputtong 2013).

In contrast, *Interpretivism* believes in multiple realities, which are subjective, and context specific, and boundaries between researcher and participant are indistinct, providing knowledge from a shared understanding of patterns (Burns & Grove 2005). Researchers in this paradigm, reject this notion of objective detachment, believing that it is impossible and undesirable to conduct research in a detached manner and that to understand the realities and experiences of others, researchers must acknowledge their own subjectivities. Neither *Positivism* nor *Interpretivism* is appropriate to this study as explained in section 3.2.3

The third paradigm called *Pragmatism* argues that reality does not exist only as natural and physical reality but incorporates psychological and social realities which include subjective experience and thought, and language and culture (Liamputtong 2013). This reality is in fact reality in context. Pragmatists according to Liamputtong (2013) believe knowledge is based on the reality of the world and the way one experiences it. Pragmatists suggest knowledge can be obtained from multiple sources and theories and through multiple research methods (mixed methods) combining the advantages of *Interpretivism* and *Positivism* (Liamputtong 2013). This methodological diversity

promotes objectives driven research (Liamputtong 2013). The rationale for basing this study in the *Pragmatism* paradigm is explained in section 3.2.3.

3.2.2 Research Design

The research design is a clearly defined structure for undertaking research and is closely associated with the framework which guides the study (Burns & Grove 2005). The design selected must be appropriate to the study purpose, feasible given limitations and effective in decreasing threats to validity and reliability (Burns & Grove 2005). The three main types of design methodologies are *Quantitative*, *Qualitative* and a combination of both called *Mixed Methodology* (DePoy & Gitlin 2011).

Quantitative research is a formal, objective, systematic process for generating theory that is then tested empirically (Parahoo 2001). The purpose of *Quantitative* research according to Burns & Grove (2005) is to develop and refine knowledge, to explore new ideas and describe situations, to examine relationships, and to determine effectiveness of interventions. Contrastingly, *Qualitative* research is subjective, concerned with the meanings of phenomena and involves developing and testing theory inductively (Holloway & Wheeler 1996). The purpose of qualitative research is to describe and interpret the lived experience, to study culture, and to formulate and test theory of social processes (Polit *et al.* 2001).

The third type of research design is known as *Mixed Methodology*. This involves purposively selecting and combining designs and methods from both qualitative and quantitative standpoints, so that one complements the other and contributes to an understanding of the whole (DePoy & Gitlin 2011). Hammersley (1996) advocate three different approaches to combining methods: 1) triangulation - whereby the use of one method is used to confirm the findings of another, 2) facilitation - one method is used to facilitate the use of another and 3) complementarity – two approaches are used to examine different aspects of an issue. This study will use a semi-structured group interview, a quantitative survey, and qualitative individual interviews. This *Mixed Methodology* research design fits well with the aims and objectives of this study (section 3.2.3).

The research design must fit the purpose of the study, which in this instance is development and validation of an assessment method for IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). This puts the study in the *Design Science* paradigm also referred to as *Design Research*. The aim of *Design Research* is the discovery of useful real world solutions to unsolved problems (Tuffley 2012). In the case of this study; the problem of how to assess the risk management processes of medical IT-networks against the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). *Design Research* aims to expand the boundaries of human and organisational

capabilities by creating new and innovative artefacts (Hevner *et al.* 2004). In *Design Research*, knowledge and understanding of a problem area and its solution are achieved by constructing and applying the designed artefact (Hevner *et al.* 2004). The resulting artefacts are evaluated and improved until they adequately meet the identified business need (Hevner *et al.* 2004).

The assessment method artefact for IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) which addresses the risks involved in incorporating medical devices on an IT-network is the focus of this study. As *Design Research* is a problem solving process with its principle goal of utility (Hevner *et al.* 2004), this fits with the purpose of this study; to develop a useful assessment method; to enable healthcare organisations to solve the problem of determining compliance against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). The use of the assessment method in the context of a healthcare organisation will provide knowledge in context. Hevner *et al.* (2004) propose guidelines for *Design Research* which will be followed in this study:

- creation of an innovative artefact (in this study an assessment method)
- to address a specific unsolved problem (compliance with IEC 80001-1 (IEC 2010))
- evaluated to prove usefulness (via focus group and questionnaire)
- defined and consistent (based on IEC 80001-1 PRM & PAM and compliant with ISO/IEC 15504)
- problem area is described and solution is implemented
- results to be disseminated to technical/managerial personnel.

3.2.3 Research Paradigm, Design & Methodology of this Study & Justification for choice

In light of the discussion of the various research paradigms/approaches outlined in section 3.2.1, this study will be based on the *Pragmatism* approach, as the study will be conducted in the context of a healthcare organisation in which the culture, language and subjective experience of the participants is vital to achieve the research objectives. In addition, the involvement of the researcher in the project under study precludes an objective detached stance required by positivism, and the need to use a mixed methods design to achieve the study aims and objectives outlined earlier, indicate the suitability of this approach.

Neither a *quantitative* or *qualitative* research design alone, would sufficiently address the study purpose and objectives. Therefore a mixed methodology design will be used. Three different data collection methods will be used, each for specific purposes (outlined in section 3.4.1); to facilitate and complement each other and inform the development and validation of the assessment method

for IEC 80001-1 (IEC 2010). Each method will generate different kinds of knowledge and perspectives regarding the issue under investigation as described by Burns & Grove (2005). To use *Mixed Methods* research however, the researcher must understand both the strengths and weaknesses of both qualitative and quantitative traditions, in the pursuit of a comprehensive understanding of the issue (DePoy & Gitlin 2011). It is anticipated that the combination of methods to be used in this study, will result in a more comprehensive understanding of the issues surrounding development and validation of an assessment method for IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

In addition to the *Mixed Methods* approach this study will take a *Design Research* approach. *Design research* involves the creation of artefacts which are then tested, with the findings being fed back into the next iteration to improve the artefact (Keyson & Bruns Alonso 2009). *Design research* develops knowledge in the service of action to address real world challenges and problems (Pascal *et al.* 2013). The aims and objectives of this study include these key features of: design, feedback loops to improve iteration, and knowledge development in addressing the development and validation of an assessment method for IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

Hevner *et al.* (2004) describe the steps involved in design research (design, review, and improvement cycles) before the final fit for purpose artefact is realised. This approach is perfectly suited to PRM / PAM and assessment method development which by their very nature require numerous iterations and reviews before being finalised for use. We will look at how well this worked in practice in the discussion in chapter 6. This approach will guide the iterative design process of the assessment method, whereby the evaluation phases will provide vital feedback to the construction phase regarding the quality of the design process and product (the assessment method). Feedback gained from the assessment used in context and a questionnaire will be used to refine the question subset (see sections 4.8.2 & 5.6).

Tuffley & Rout (2009) successfully used design research to develop a leadership process reference model (PRM) which is compliant with ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003) and ISO/IEC TR 24774 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2007). The leadership PRM went through a series of 5 review cycles with improvements made with each cycle (Tuffley & Rout 2009). The assessment method for IEC 80001-1 (IEC 2010) under development is based on an ISO/IEC 15504 compliant PRM and PAM developed using design research by MacMahon *et al.* (2013a). A design artefact is complete and effective when it satisfies the requirements and constraints of the problem it is addressing (Hevner *et al.* 2004), this will be

achieved by undertaking the various validation steps outlined in the methodology section 3.6. Validation of the assessment method will require a sample of the target population (risk management stakeholders involved in IT-network creation and modification in healthcare organisations) for whom the assessment method is designed.

3.3 Sampling

Purposive sampling involves selection of participants that will provide information about the research topic in question (Griffiths 2009). Therefore, purposive sampling will be used as the most effective means of including risk management stakeholders involved in a medical IT-network modification project in a healthcare organisation to which the standard IEC 80001-1 (IEC 2010) is applicable (see section 4.2.3). It is acknowledged that this form of sampling can increase the risk of selection bias and reduce the generalisability of the findings to a wider population (Parahoo 2001), however generalisation of findings to all IT-network modification projects is not an intention of this study.

The sampling strategy will involve the researcher identifying the suitable IT-network modification project and inviting personnel involved to participate. The hospital risk manager will also be invited to participate. An information pack (Appendix D) including:

- participant information sheet
- consent form
- focus group assessment interview schedule
- post assessment questionnaire (described below) and the
- assessment questions document (outlined below)

will be issued to participants. Once the sample is identified a suitable means of data collection must be devised.

3.4 Data Collection Methods

A combination of data collection methods (focus group interview, questionnaire and individual interviews) will be used. The development of data collection instruments and intended use is outlined in section 3.4.1. The purpose of assessing the appropriateness and usefulness of new instruments (developed for this study) also fits with one of the reasons for mixing methods identified by Collins *et al.* (2006). The results of each data collection method are presented in chapter 5, and chapter 6 will discuss those results.

3.4.1 Development of Data Collection Instruments, Purpose & Use

3.4.1.1 Assessment Focus Group Interview

A focus group is a discussion between a group of people and a facilitator, with the facilitator introducing the topic and facilitating participant's contributions and the discussion providing a rich source of insight and interpretation from participants (Polgar & Thomas 2008). The assessment will take the format of a focus group interview. The assessment is examining the requirements of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). As there are numerous risk management stakeholders involved, the focus group structure will enable the views of all stakeholders to be taken into account and also generate group discussion on the risk management processes. Additionally, it is anticipated that the results of the assessment will be utilised by the project team to make improvements to these processes and fulfil research objective 7 (section 1.5). The focus group interview was also selected as conducive to increasing collaboration of the multi-disciplinary risk management stakeholders as advocated by the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

The assessment method development will involve drafting the assessment question set and guidance document based on the base practices for all processes in the IEC 80001-1 PAM (MacMahon et al. 2012; MacMahon et al. 2013b). The base practices are the risk management activities undertaken to achieve the purpose and outcomes of risk management processes. These will be jointly examined (by this researcher and the developer of the PAM) and converted into question format. Guidance from the standard will also be included to clarify the requirements of the standard and promote discussion during an assessment. Once all questions have been developed these will be reviewed, focusing on usability in context, and guidance in the standard IEC 80001-1 and other related technical reports.

The purpose of the assessment is the validation of an assessment method (question set), developed to assess the risk management processes related to medical IT-network modification projects referred to in the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). This validation will achieve research objective 2 (section 1.5). This assessment method validation takes into account the context of use in an actual medical IT-network modification project in a healthcare organisation; a feature of design research (Hevner *et al.* 2004). It is anticipated that the assessment will identify the risk management processes employed and assess them against the requirements of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). Data collected will be qualitative (researcher notes and audio recording). The focus group assessment interview schedule

and the assessment question set are included in Appendix D.3 and D.5. Feedback on the assessment will be collected via a questionnaire.

3.4.1.2 Questionnaire

A questionnaire is composed of a structured set of questions with standardised responses which can be easily analysed (Liamputtong 2013). One of the advantages of using a questionnaire is increased confidentiality and anonymity (Parahoo, 2001). In addition, the absence of the interviewer effect, where participants may respond as they think the researcher wants (Dockrell and Joffe, 1992) is eliminated in self-administered questionnaires resulting in more meaningful data. This is particularly important in the current study where the researcher is involved in the medical IT-network modification project under study. The main disadvantage of questionnaires is questions may be misinterpreted (Cormack, 2000), this will be minimised by using an expert panel review.

The purpose of this questionnaire is to:

- Gain information relating to the experience of participants with the use of standards, and discover their level of awareness of the standard IEC 80001-1 (IEC 2010),
- Enable participants to provide feedback on the pre-assessment presentation
- Enable participants to provide feedback on the assessment method developed and the use of the assessment method in context. This feedback will be used to achieve research objective 5 (section 1.5).

Guidelines for questionnaire development will be followed (Dillman 2000). A Likert scale, which is a 5 point response scale used in questionnaires (strongly agree, agree, neither agree or disagree, disagree, strongly disagree (Bowling 2009) along with numerical scales (scale of 0 – 5 where 0 = not aware and 5 indicates very aware) and open ended free text questions will be included. The researcher will code the data in the Likert scales to enable analysis. A numerical value will be assigned to each response ranging from 1 – 5 which implies a hierarchy of order with the lowest value 1 = strongly disagree and the highest value (5 = strongly agree) for the most positive response. The data collected will be mainly quantitative data with free text questions (n=4) generating qualitative data. Once developed, the questionnaire will be reviewed by an expert panel (consisting of 4 staff from IT, clinical, management, and engineering in different healthcare organisations) to determine ease of completion and usability. Feedback received will be used to improve the questionnaire prior to use in the study proper. The questionnaire will be distributed to participants prior to the assessment for completion post the assessment (see sections 3.6.9 & 4.2.9).

3.4.1.3 Individual Interview Schedule

Individual semi-structured interviews will be undertaken with assessment participants 2-4 weeks following the assessment. The individual interview schedule will be devised by the researcher using the assessment findings report (section 3.6.11 & 4.2.11) and a copy is included in Appendix E. The purpose of the individual interview is to:

- discuss the assessment findings report
- validate the recommendations (research objective 4)
- determine if recommendations can be implemented
- identify any additional recommendations
- Allocate / agree tasks to / with relevant personnel to determine which recommendations (if any) the participant will assume responsibility for.

Data collected will be mainly qualitative data (researcher notes/audio recordings which will be transcribed (copy in Appendix F).

3.5 Data Analysis Methods

Data analysis is conducted to reduce, organise and give meaning to the data (Burns & Grove 2005). Making sense of the data in quantitative research involves counting responses, whereas in qualitative research it involves looking for patterns of ideas or themes (Cormack 2000). Quantitative data will therefore be analysed by descriptive statistic techniques and qualitative data will be analysed by thematic analysis. The data analysis to be undertaken and undertaken is explained in sections 3.6.10, 3.6.12, 4.2.10 and 4.2.12.

3.6 Methodology Overview

An overview of the methodology steps to be undertaken is shown in Figure 4, followed by a brief description of each step and how the steps fit together. A detailed description of each step is included in Appendix C and chapter 4 section 4.2.

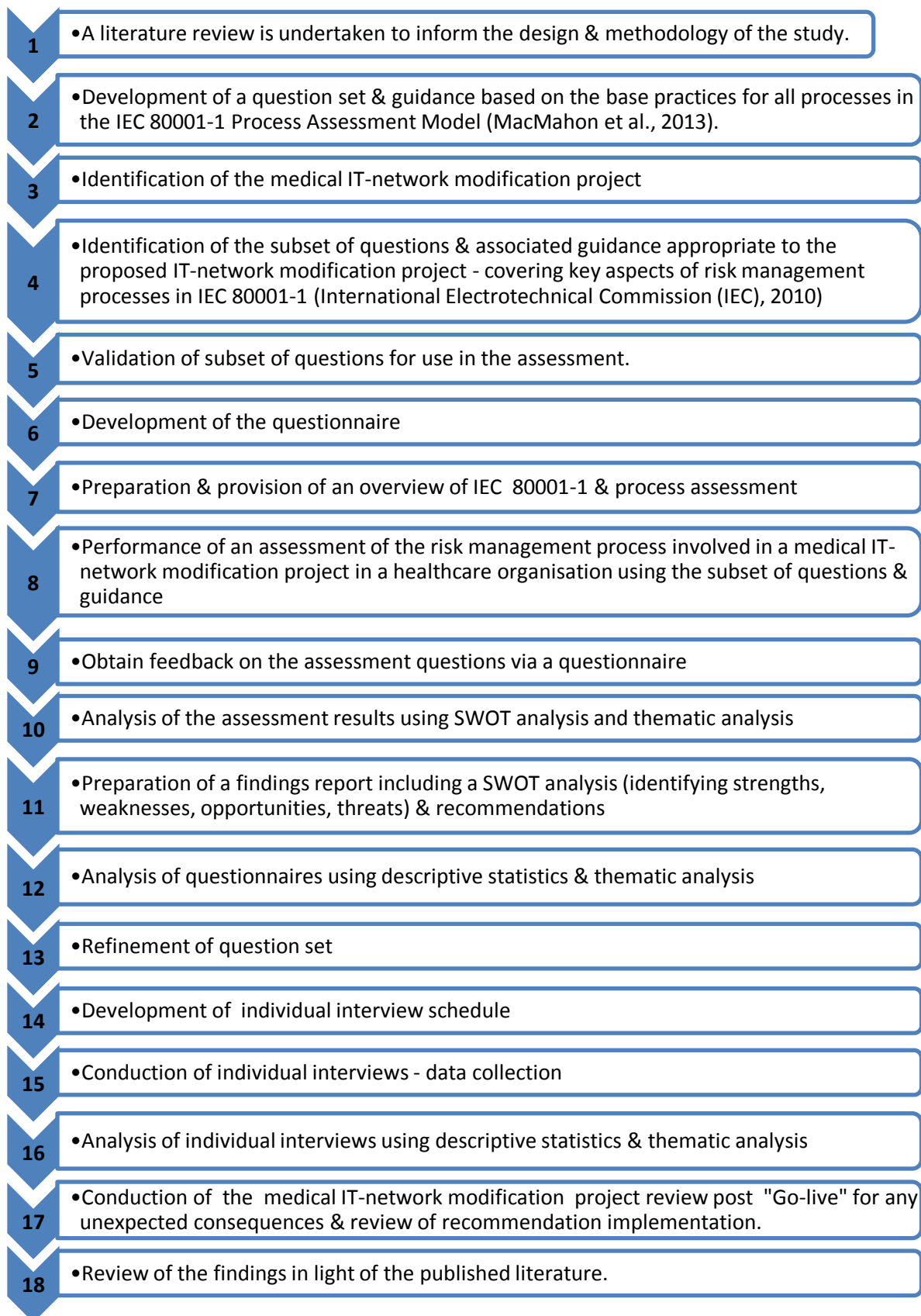


Figure 4 Methodology Overview

3.6.1 Step 1: Perform Literature Review

The literature review performed is outlined in chapter 2 and the start of chapter 3 section 3.2. The following concepts introduced:

- Medical IT-networks and risk
- Risk management of medical IT-networks
- IEC 80001-1 (IEC 2010) implementation
- CE-IT collaboration and IEC 80001-1 (IEC 2010) implementation
- Compliance with process assessment standard ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003)
- Design research
- Research Paradigm – *Pragmatism*
- Research Design – Mixed methodology
- Purposive Sampling
- Data collection / analysis methods & tools

are linked to the relevant methodology steps below.

3.6.2 Step 2: Develop question set & guidance

The second step in this study methodology will be the development of the assessment method (comprising of a question set and guidance document) based on the base practices for all risk management processes in the validated IEC 80001-1 PAM and PRM (MacMahon et al. 2012; MacMahon et al. 2013b). This step is linked to design research with the creation of an innovative artefact (see section 3.2.2). This step will follow the standard for development of an assessment method ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). This step is described in section 3.4.1.1, Appendix C step 2 and chapter 4 section 4.2.2. The output from this step will achieve research objective 1 and will be used in step 4 below.

3.6.3 Step 3: Identify the Medical IT-network Modification Project to be the focus of the assessment

A medical IT-network modification project in a healthcare organisation for which the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) is applicable (see section 2.11.2) will be identified. A medical IT-network modification project can introduce risks to patient safety as outlined in section 2.6. The identified medical IT-network modification project will be the focus of the assessment so that the project team can validate use of the assessment method in context; a

requirement of design research. This is also linked to the research approach of *Pragmatism* in that the culture, language and context of the healthcare organisation is an important aspect of this study. Appendix C step 3 provides further details on this step and chapter 4 section 4.2.3 describes step 3 implementation.

3.6.4 Step 4: Identify the subset of questions & associated guidance appropriate to the identified IT-network modification project

The next step is to prepare the assessment document to be used in the assessment of the medical IT-network modification project in a healthcare organisation. The assessment method contains 84 base practice questions but a subset will be used. The subset of questions will be derived by examining each process and selecting questions based on key base practices within each process, ensuring a minimum of one question from each process is included. The researcher copy of the assessment document will also include guidance for each question. Additional information regarding this step is provided in Appendix C step 4 and chapter 4 section 4.2.4 explains step 4 implementation.

3.6.5 Step 5: Validate subset of questions & ensure all processes are represented

The subset of questions will be reviewed to ensure each risk management process is represented in the assessment document.

3.6.6 Step 6: Develop the Questionnaire

The questionnaire (a component of the study's mixed methodology) will be developed as outlined in Section 3.4.1.2.

3.6.7 Step 7: Provide an overview of the Standard IEC 80001-1 (IEC 2010) Process Assessment

Information regarding the standard will be provided to participants as described in Appendix C step 7 and chapter 4 section 4.2.7. Performance of step 7 will achieve research objective 6 (section 1.5).

3.6.8 Step 8: Perform the assessment using the subset of questions

Step 8 will be performance of the assessment to achieve research objective 2 in the form of a focus group with a purposive sample of risk management stakeholders. The assessment will identify strengths, weaknesses, opportunities and threats related to the risk management of the medical IT-network modification project. This focus group will foster collaboration among risk management

stakeholders as described in section 2.11.4. Further information on this step can be found in Appendix C step 8 and chapter 4 section 4.2.8.

3.6.9 Step 9: Post Assessment Questionnaire Distribution/Completion

Participants will provide feedback on the assessment by completing the questionnaire as described in section 4.2.9. This feedback will be used in step 13 below to achieve research objective 5: refinement of the criteria question set.

3.6.10 Step 10: Assessment Analysis

The assessment data recordings will be transcribed, coded and categorised into themes. A SWOT analysis identifying strengths, weaknesses, opportunities and threats will be undertaken (see Appendix C step 10 and chapter 4 section 4.2.10).

3.6.11 Step 11: Prepare a Findings Report

The results of the SWOT analysis (outlined in chapter 5) along with the recommendations identified will be compiled in a findings report as described in section 4.7.11 fulfilling research objective 3.

3.6.12 Step 12: Questionnaire Analysis

Questionnaires will be analysed using mixed methods; descriptive statistics using MS Excel for quantitative data and thematic analysis for qualitative data.

3.6.13 Step 13: Refinement of the assessment question set

The question set will be revised (research objective 5) based on the results of the assessment and questionnaire analysis using the iteration feedback loop of design research as described in chapter 4 section 4.2.13.

3.6.14 Step 14: Individual Interview Schedule Development

An interview schedule for the individual interviews will be developed as outlined in section 3.4.1.3.

3.6.15 Step 15: Individual Interview Data Collection

Individual interviews will be undertaken with assessment participants as described in Appendix C step 15 and chapter 4 section 4.2.15. Performance of this step will achieve research objective 4: to validate recommendations arising from the assessment.

3.6.16 Step 16: Individual Interview Analysis

Individual interview recordings will be transcribed and analysed using mixed methods (see Appendix C step 16).

3.6.17 Step 17: Project Review Post Go-Live

A project review post Go-Live (of the IT-network modification) will identify any unforeseen consequences and review the status of recommendation implementation. Implementation of recommendations will achieve research objective 7: Improvement of risk management processes in line with IEC 80001-1 (IEC 2010).

3.6.18 Step 18: Review the findings in light of the published literature

The findings will be reviewed and discussed in light of published literature in chapter 6.

3.8 Submission of revised question set to Technical Committee 62A - ISO/IEC TR 80001-2-7 (Committee draft) (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014)

The final iteration of the question set will be submitted to working group 7 for incorporation into the Technical Report ISO/IEC TR 80001-2-7 which is due to be published in 2014.

3.9 Ethical Considerations

The ethical principles of autonomy (right to self-determination), beneficence / non-maleficence (doing good and avoidance of harm) and justice (Beauchamp & Childress 2009) and the Data Protection Act 2003 (Government of Ireland 2003) were adhered to throughout the study. Ethical approval to conduct the study was provided by the Research Ethics Committee of the School of Computer Science and Statistics (SCSS) University of Dublin (Appendix G) and access to participants was provided by the healthcare organisation (Appendix H). A hospital information sheet and consent form requested by the SCSS Ethics committee were drafted, provided and approved for use in the study (Appendix I)

3.10 Summary

This chapter detailed the approach to the development and validation of an assessment method for the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). This study is based in the *Pragmatism* paradigm using design research and mixed methodology. Design research has been used in the development of PRMs/PAMs and assessment methods compliant with IEC 15504 (MacMahon et al. 2013a; Tuffley 2012). Sampling, data collection methods and instruments to be used, and reliability/ validity were examined. The methodology overview and steps to be taken were described. Finally, ethical considerations were outlined. Chapter 4 will describe the implementation of the methodology step by step along with the challenges experienced. The study findings will be reported in Chapter 5, followed by a discussion of results in Chapter 6.

Chapter 4 Research Implementation

4.1 Introduction

Chapter 3 described the research methodology of this study, presented a methodology overview (Figure 4) and described the methodology steps (1-18) to be used. As mentioned earlier, Chapter 4 will describe the implementation of these same methodology steps shown again in Figure 5 below.

4.2 Research Implementation: Step by Step

The research implementation steps (1 - 18) in Figure 5 are described in sections 4.2.1 – 4.2.18.



Figure 5 Research Implementation Steps

4.2.1 Step 1: A literature review was undertaken

The literature review performed to inform the design and methodology of the study is outlined in chapter 2 and chapter 3 (section 3.2 – 3.4).

4.2.2 Step 2: Development of a question set & guidance based on the base practices for all processes in the IEC 80001-1 PAM (MacMahon *et al.*, 2013).

The PRM and PAM for IEC 80001-1 developed by MacMahon *et al.* (2013b) and described in section 2.11.6 were examined by the researcher and the developer of the PRM and PAM (MacMahon). The base practices/risk management activities in the IEC 80001-1 PAM were meticulously expressed as questions for inclusion in the assessment method. A total of 84 questions and associated guidance were devised. These 84 questions will be included in the ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) which will be published shortly. Due to copyright issues these questions cannot be included here. The output from this step will achieve research objective 1 (section 1.5).

4.2.3 Step 3: Identification of the Medical IT-network Modification Project for the Assessment

The standard IEC 80001-1 is applicable throughout the life cycle of a medical IT-network (International Electrotechnical Commission (IEC) 2010). The medical IT-network at the study site (large healthcare organisation) incorporates numerous medical devices which undergo regular maintenance and new devices are added and old devices are removed frequently. Planned medical IT-network modification projects at the study site included: software upgrade to networked dialysis machines, replacement of anaesthetic machines, procurement of new networked ventilators, replacement of POCT ABG analysers, upgrade of the ICU CIS, and upgrade of the laboratory information system.

The medical IT-network modification project selected for the study was the project to replace the POCT ABG analysers. This IT-network modification project involved replacing 2 types of POCT ABG analysers with one type from one manufacturer and interfacing the new analysers on the medical IT-network with the:

- 1) Clinical Information System (CIS) in ICUs,
- 2) Laboratory Information System (Laboratory Information System)
- 3) Patient Administration System (PAS)

4) Electronic Patient Record (EPR) / Order Communications Application

This IT-network modification project (“the project”) was selected for the following reasons:

- The standard IEC 80001-1 (IEC 2010) governing risk management of medical IT-networks is applicable to this project because the project involves modification of a medical IT-network in a healthcare organisation.
- The project involves collaboration between Information Technology (IT) and Clinical engineering (CE) personnel which is identified in the literature as a vital factor in terms of minimising risks to patients from incorporating medical devices into a medical IT-network.
- The project will have a direct impact in ICU where critically ill patients are particularly vulnerable to any unforeseen adverse effects of the project with potentially serious consequences.
- The researcher is employed in ICU and involved in the project and is keen to utilise the study findings to improve risk management processes.
- The expected time frame of the project provided a unique opportunity for involvement in the IEC 80001 -1 assessment method validation.

Once the project was identified project personnel were informed of the study and provided with the study participation information pack as outlined in section 3.6.3 step 3.

4.2.4 Step 4: Identification of the subset of questions & associated guidance appropriate to the proposed IT-network modification project

As mentioned previously, as this IT-network modification project is the first IT-network modification project to be assessed against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) it would be unreasonable to expect the IT-network modification project selected for assessment to be compliant with all 84 base practice questions. Therefore the 84 base practices and questions were reviewed and a selection was chosen for inclusion in the subset to be used for the assessment. This resulted in a subset of 37 questions and associated guidance (with a minimum of one and a maximum of five questions from each of the 14 processes) and an additional question seeking general comments to be used in the assessment (Appendix J).

4.2.5 Step 5: Validation of subset of questions for use in the assessment.

The subset of questions was reviewed to ensure all fourteen risk management processes outlined in the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) were included. Due to copyright issues it is not possible to publish the full set of questions ahead of publication of the Technical Report ISO/IEC TR 80001-2-7.

4.2.6 Step 6: Development of the Questionnaire

The questionnaire developed by the researcher (Appendix D.4) as described in section 3.4.1.2 includes 18 questions under the following sections:

1. **Standards** – seeking information regarding use of standards, awareness of the standard IEC 80001-1.
2. **Pre-assessment presentation** – evaluation of the pre-assessment presentation.
3. **Assessment** – clarity and ease of understanding of questions, adequacy of questions in addressing the risk management processes, appropriateness of the assessment method, knowledge gained/usefulness of knowledge gained.
4. **Comments** – general comments.

The questionnaire (Appendix D.4) was reviewed by an expert panel in terms of format and usability. The only changes made following this review were to revise the layout, increasing the space around questions. The questionnaire findings and analysis are outlined in chapter 5 section 5.5 and chapter 6 Section 6.2.

4.2.7 Step 7: Provision of an overview of IEC 80001-1 (2010) & Process Assessment

A brief summary of the standard IEC 80001-1 (IEC 2010) was included in the participant information sheet (Appendix D.1) provided to participants prior to the study. A PowerPoint presentation outlining the key elements of the standard IEC 80001-1 (IEC 2010) and an explanation of process assessment was prepared and provided before the assessment (Appendix K). Completion of this step along with step 8 is required to achieve research objective 6 (section 1.5).

4.2.8 Step 8: Performance of an assessment of the risk management processes involved in a medical IT-network modification project

To achieve research objective 2 (section 1.5) an assessment which took the format of a focus group interview was conducted. The focus group interview was selected as conducive to increasing

collaboration of the multi-disciplinary risk management stakeholders as advocated by the standard IEC 80001-1 (International Electrotechnical Commission (IEC), 2010). The literature suggests that 6 – 10 participants per focus group is adequate (Morgan, 1996), however all members of the IT-network modification project team (n=10) and the risk manager were invited to participate. The assessment participants (n=11) are listed in Table 6 along with a brief description of their role.

Discipline	Role Description
Point of Care Testing (POCT) Personnel (n=2)	Project lead, project planning & implementation, POCT device selection/ procurement and configuration, results validation, installation, & staff training.
IT Personnel (n=2)	Network configuration, interface testing (CIS/LIS/PAS/EPR)
Clinical Informatics Personnel (n=2)	Procurement/ device specification requirements, site visits, configuration related to CIS, Validation of results in CIS.
Clinical Information System Supplier (n=1)	Mapping of POCT device parameters to the patient record in the CIS & interface of POCT device to the CIS.
Clinical Engineering (CE) (n=1)	Validation of results to CIS.
POCT analyser supplier (n=1)	Validation of POCT results, installation, testing, interface works to the LIS & PAS, staff training.
Clinical User (n=1)	Input into POCT device specification requirements, procurement, site visits, user testing, workflow / practice review.
Healthcare Organisation Risk Manager (n=1)	Provision of advice regarding risk management activities.

Table 6 IT-Network Modification Project Personnel & Role Description

Participants were given advance notice (2 weeks) of the date, time and venue (ICU) of the assessment. The focus group assessment interview schedule is in Appendix D.3. All participants were reminded of the need for confidentiality within the group and encouraged to actively engage with the process. The researcher asked each question in turn making a note of responses and providing clarification where required from the guidance section of the assessment document (Appendix J). The assessment (inclusive of the presentation) took two hours and was audio-recorded with permission.

4.2.9 Step 9: collection of feedback on the assessment questions via a questionnaire

On completion of the assessment, participants completed the post assessment questionnaire. Questionnaires were returned immediately (hard copies) or returned later (electronically).

4.2.10 Step 10: Assessment Analysis using SWOT analysis & thematic analysis

Having consulted the literature on undertaking a SWOT analysis, a SWOT analysis of the assessment data identifying strengths, weaknesses, opportunities and threats as outlined by Berry (2013) involving the following was undertaken:

- Transcription (verbatim) and review of assessment recordings.
- Typing and review of researcher's and research assistant's notes from assessment.
- Review of transcript and notes and IEC 80001-1 (2010) requirements to identify strengths, weaknesses, opportunities and threats.
 - Positive aspects of the project along with areas of compliance with the standard IEC 80001-1 (IEC 2010) were identified as strengths.
 - Weaknesses were items identified where requirements were not met and improvements could be made.
 - Opportunities were issues arising from the project which were capitalised on.
 - Threats were issues that threatened the completion of the project in the expected timeframes and contributed to project delays.

The findings are reported in section 5.3.1. The transcript and researcher notes were also examined for themes and categories (section 5.3.2).

4.2.11 Step 11: Preparation of assessment findings report

The assessment findings report was drafted by the researcher to provide feedback on the assessment to participants. The report included the results of the SWOT analysis and recommendations (Appendix L). Recommendations were compiled mainly from the weaknesses, opportunities and threats to address areas of non-compliance with IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) requirements and to improve the processes involved in the application of risk management for medical IT-networks outlined previously in section 2.11.6 Table 5. Successful completion of this step will achieve research objective 3.

4.2.12 Step 12: Questionnaire Analysis

Questionnaires were analysed as outlined in section 3.6.12 using descriptive statistics and thematic analysis. The results of this analysis are in section 5.4.

4.2.13 Step 13: Refinement of question set

The question set was revised based on the results of the assessment and questionnaire analysis (Appendix M). The main changes were some rewording of questions and guidance to clarify the questions (section 5.6). This step contributes to research objective 5 (section 1.5).

4.2.14 Step 14 Development of the individual interview schedule

The interview schedule (Appendix E) was provided to participants before the interview.

4.2.15 Step 15: Conduction of individual interviews - data collection

Individual interviews (n=6) were undertaken lasting 30-60 minutes. Data collected included: interview notes and audio recordings yielding both quantitative and qualitative data. Interview participants included representatives from all disciplines involved in the medical IT-network modification project (Table 7). Participants reviewed the recommendations, identified the recommendations which they would take responsibility for implementing and agreed to proceed with implementation of same. This step is to achieve research objective 4 (section 1.5).

Number	Discipline	Number of participants (n)
1	Point of Care Testing (POCT) personnel	1
2	IT personnel	1
3	Clinical Informatics Personnel	1
4	Clinical Engineering (CE)	1
5	ABG Analyser Supplier	1
6	Clinical User (n=1)	1

Table 7 Individual Interview Participants

4.2.16 Step 16: Individual interview Analysis

Individual interview analysis as outlined in Appendix C step 16 was undertaken. The transcription was challenging due to the time required. The findings are provided in chapter 5 section 5.8.

4.2.17 Step 17: Conduction of a project review post go-live for any unexpected consequences

Following the “Go-Live” process a review was undertaken and issues arising from “Go-Live” were reviewed and actioned. No further changes were made to the question set. The status of recommendation implementation was also reviewed (Appendix N Table 14).

4.2.18 Step 18: Review of the findings in light of the published literature.

The findings of the study were reviewed in light of the published literature and are discussed in Chapter 6.

4.3 Submission of question set to Technical Committee 62A for ISO/IEC TR 80001-2-7

The initial complete question set developed jointly by the researcher and the developer of the IEC 80001-1 PRM & PAM for use in the assessment was incorporated into the Technical Report ISO/IEC 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”* by MacMahon which is at committee draft stage. The committee draft ISO/IEC TR 80001-2-7 was circulated to National Committees for comment (standards development process stage 4) as outlined in section 2.9. The researcher’s experience with using IEC 80001-1 informed the researcher review of this Technical Report which was submitted to ISO through the NSAI. A copy of the response received is included in Appendix O. Additionally; the assessment question set along with the revised question set was submitted for possible inclusion in the Technical Report.

4.4 Summary

Now that the study’s mixed methodology has been implemented, chapter 5 will present the study findings and chapter 6 will discuss these findings in light of published literature and the research objectives.

Chapter 5 Data Analysis & Findings

5.1 Introduction

Chapter 3 outlined the study methodology, while chapter 4 described the implementation of that methodology. As outlined in chapters 3 and 4, data collected included: assessment interview (n=1) notes/audio recordings, questionnaires (n=11) and individual interview (n=6) notes/audio recordings. Quantitative and qualitative data analysis is described in chapter 4 sections 4.2.10, 4.2.12 and 4.2.16). This chapter (chapter 5) outlines the findings generated.

5.2 Assessment Analysis

As described in sections 3.6.8 and 4.2.8 an assessment against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) of a real medical IT-network modification project relating to POCT ABG analysis was undertaken. Use of POCT analysers was discussed during the assessment; therefore the procedure for performing POCT ABG analysis is included in Appendix P.

5.3 Assessment Findings

5.3.1 SWOT Analysis Findings

The SWOT analysis performed is outlined in section 4.2.10, the findings are summarised below (sections 5.3.1.1 to 5.3.1.4). Direct quotes from participants are used and text inserted by the researcher in square brackets [] is provided for explanatory or anonymisation purposes.

5.3.1.1 SWOT Analysis - Strengths

The strengths identified are listed in Table 15 (Appendix Q.1) and summarised below. Participants identified that risk management resources are in place and involvement of all relevant stakeholders many of whom had worked together previously facilitated better engagement in the project. Participant stakeholders contributed extensive expertise, knowledge and experience which were used to identify potential problems and safety hazards relating to the devices/ devices on the network, these potential problems and hazards are outlined in Appendix R.

“I suppose you could say [researcher name] that we know from experience what the hazards are [emphasis] associated with the devices [POCT ABG analysers] themselves” (Participant 3)

Participants reported that change release processes were followed and negative events are captured and documented.

“Are negative events captured and documented?” (Researcher)

Response “yes” (Participant 1)

Risk assessments were undertaken:

“I do a biological and chemical assessment, risk assessment on any chemicals that might be hazardous within the device, which are recorded” (Participant 3)

Participants identified that IT standards for security are in place which must be complied with before items are added to the medical IT-network:

“there are certain standards that are applied and requested in relation to the devices from the company when they were looking for it to be added to the network until those are done the device wouldn’t be left on, so it has to fall in with the security standards that we would have set down” (Participant 9)

Participants identified risks such as: data download failure, user picks incorrect medical record number (MRN), users fails to mark sample as venous, manual data entry errors or transcription errors due to failed download caused by power issues and unavailability of results outside of ICU.

“you have 2 risks, you are aware the report [analyser results printout] won’t make it to the system, if the data doesn’t come through [to the Clinical Information System (ICIP)], the other risk is the user picks the wrong patient, wrong medical record number (MRN)” (Participant 7)

“The other one is the user doesn’t mark a sample as venous and it’s a venous sample” (Participant 7)

“risk of transcribing results when the power is down, even though they have a printout [analyser results] the risk of transcribing incorrectly is always there” (Participant 3)

“it [result] is only available in ICU” (Participant 7)

Participants also identified risk control measures such as:

1) analyser printout – the analyser produces a printout of the POCT ABG analysis results which is used to guide patient treatment and is filed in the patient’s medical record (hard copy). In areas which do not have a CIS this is the only record of the POCT, while in areas which have a CIS, this printout serves as a validation tool, as the printout can be cross checked with the result electronically sent to the patient’s CIS chart to confirm that the details are correct. Incorrect details can be corrected, the reasons can be identified and actions taken to prevent a recurrence.

2) transcription of results - manually entering results into the CIS using the analyser results printout, if a result does not download automatically to the CIS (if the result is not sent by the analyser or received by the CIS - possibly due to a failure of the IT-network interface).

3) audit of MRN mismatches and feedback of results – an audit of MRNs entered onto the analyser can identify incorrect MRNs entered and the user responsible, the audit results are provided to relevant departments and additional training of users is undertaken where required.

4) training to reduce errors – training is provided one to one/group sessions

5) possibility of a double check to reduce transcription errors – user to double check manually entered data in the CIS

6) use of a bar-code scanner to input staff/patient identity - scanning the barcodes to reduce manual data entry errors – the bar code scanner is integrated into the analyser, however problems have been encountered with some staff Identity badges not scanning due to wear and tear.

7) use of bar-coded syringes is being considered – pre barcoded syringes facilitate scanning of the syringe and the patient identity band at the bedside, thereby identifying the sample immediately and reducing the risk of sample identification errors.

8) provision of results outside of ICU – Configuration of the analyser to interface with the Laboratory system and the EPR so that POCT ABG analysis results can be viewed across the hospital is being considered.

*“the report won’t make it to the system if the data doesn’t come through this is mitigated by having the printed copy [analyser results printout]”
(Participant 7)*

“risk control measures – transcribe the result (Researcher)

“the MRN mismatches whatever, where you find them coming up again and again, that’s where you’d re-audit” (Participant 8)

Response “we do that every month we run it at an acceptable level, we have set it as 4% compliance” (Participant 3)

“maybe get the person who is transcribing to double check themselves between the printout and download” (Participant 3)

“we have talked about that [control measures] a lot, bar code syringes, removing the ability of manually entering the data, forcing them [users] to scan ID” (Participant 1)

“they [staff] are more likely to use the patient ID [refers to patient identification details on a barcode addressograph label] if they are scanning their own ID [refers to staff Identification badge]” (Participant 1)

“a lot of those risks are going to be training issues” (Participant 11)

Participants indicated that the nature of the change was a project and that an event management process was in use.

“it’s a project” (Participant 3)

“we do discuss our events and your events at the meetings” (Participant 3)

Participants reported that an installation plan for connection of the POCT analysers to the network was provided by the supplier.

“An installation plan, we forwarded that at the start of the project” (Participant [number])

The project leader/manager was identified during the assessment.

“It can be me if someone wants to put my name to it” (Participant 3)

“It is you, you are the head of [department name]” (Researcher)

Participants stated that the need for a responsibility agreement had been determined.

“it [responsibility agreement] is signed at the end of the project, it won’t be released off until everything is validated” (Participant 2)

In addition the risk management process includes a corporate risk register which is provided to the hospital board.

“we have a corporate risk register”, “there is a process for formulating and escalating to top management” and “the risk register is fed to the board quarterly” (Participant 8)

The project leader reports that risk management activities are well documented:

“I am absolutely confident that everything is well documented, the whole process, we have to show that for accreditation (Participant [number])

5.3.1.2 SWOT Analysis – Weaknesses

The weaknesses identified using the SWOT analyses are listed in Table 16 (Appendix Q.2) and summarised below. Participants suggested that it would have been beneficial to have the assessment at the start of the project:

“should we have gone through this process before the project?” (Participant 7)

“I actually think you need to do this process before you go out to tender” (Participant 7)

Participants identified that disciplines had separate project plans:

“We got a lovely project plan from [the supplier] at the very beginning, [...] had to make changes as we went along” (Participant 3)

“do you have a separate project plan in IT [name] (Researcher)?

Yes (Participant 2)

“everyone has their own plan we realise we could have been more integrated and maybe avoided issues” (Participant 1)

One participant suggested that as the work is part of the day job a project plan isn't necessary:

***“a lot of people involved in this process, it gets ridiculous to document every bit , there’s bits that don’t need documenting - it is just the day to day job”
(Participant 7)***

While another participant suggested project plans are time consuming:

“It takes time to do those plans” (Participant 5)

Prior to the assessment there was a lack of clarity as to who was the project manager and the roles/responsibilities of the project manager as the following exchange shows:

“the question that struck me who is the owner of the project, we have different groups with their own processes” (Participant 9)

“Who has the responsibility for the risk, who is going to ensure the standards are applied” (Participant 9)

“it is the project manager who is responsible” (Participant 8)

“Who is the project manager? (Participant 1 / Participant 9)

“It was never identified” (Participant 3)

“There needs to be one identified person who is the lead for this whole project” (Participant 8)

“you can’t have a project and not have a project manager” (Participant 9)

“It can be me if someone wants to put my name to it” (Participant 3)

“It is you, you are the head of [laboratory department name]” (Researcher)

“it is essentially, I look on it as my baby” (Participant 3)

Participants identified that there is no Medical IT-network Risk Management File as required by the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010):

“No Not for IT” “Not as regards risk” (Participant 3)

“No Not yet” (Participant 2)

Risk management resources are informally assigned, these are not referred to as such:

***“You have assigned people because you have all the relevant people involved”
(Participant 7)***

“you just don’t use the terms isn’t that it”? (Participant 4)

Participants were asked if risk management activities are performed as per risk management plan & process (requirements of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010):

“Not by design but they might have been by default maybe, not knowing the process you wouldn’t know we can’t answer that” (Participant 7)

“I suppose from my point of view to my knowledge there isn’t really a defined plan & process” (Researcher)

Participants reported that risk management processes were not addressed formally:

“yesterday we got to a stage where we planned the connection from the instrument to ICIP [Clinical Information System] via the various processes the next phases, we defined various risks within that conversation highlighting stuff there”(Participant 2)

When asked if risk management activities are documented the response was:

“We have minutes of all the meetings it’s documented” (Participant 3)

Although it was identified that risk management templates are available from the risk manager, some participants were unaware of them and did not use them.

“There is a formal risk assessment matrix that should be used, I don’t know if you have been using it” (Participant 8)

“I don’t think we have” (Researcher)

“I think if you populated that document [risk assessment sheet] from your previous meetings you’ll capture it and you’d see what mitigating actions you have to take, so at least you’d have a documented process” (Participant 8)

***“we have filled that out in the laboratory”, “I wouldn’t have done IT”
(Participant 3)***

It was also identified that the risk manager was not involved in the project.

***“You [risk manager] probably are not even aware of this project?”
(Participant 1)***

***“I don’t even know what’s happening (Risk Manager) so I certainly won’t put
my hand up for that one” (Participant [number])***

5.3.1.3 SWOT Analysis – Opportunities

The SWOT analysis also identified opportunities arising from the project outlined in Table 17 (Appendix Q.3). The project enabled a review/revision of workflow in relation to ABG analysis to improve practice.

***“we have talked about that (control measures) a lot, bar code syringes,
removing the ability of manually entering the data, forcing them [users] to
scan ID [staff ID badge]” (Participant 1)***

Additionally, standardisation of analysers in use and implementation of the multi-device data manager (described in section 2.4.2), provides associated benefits identified in the literature such as: ease of use, simplified training, improved traceability and monitoring of end users, and interfaces to the LIS and CIS with automatic downloads of results to the ICU CIS.

***“you can see all devices [POCT devices including analysers] together on one
system, it’s easier for managing operators, training, certification, and results
etc” (Participant 3)***

***“allowing us to put all POCT devices in one area and broadcast the results to
EPR via the laboratory system” (Participant 2)***

The project involved training staff to use the new analysers and ensuring all staff are up to date with current best practice.

***“when those things [errors] do happen we would have always gone back to
training individuals, the individuals are followed up” (Participant 1)***

“we cover them [risks] in training” (Participant 3)

The project assessment also afforded participants an opportunity to review practices and procedures related to: medical IT-network modification, CIS configuration changes, interface works, validation, and risk management aspects of individual roles and record of same (recommendations 4 - 8 in the findings report). This is evident in section 5.7.2.

5.3.1.4 SWOT Analysis – Threats

The main threats to the completion of the project in the expected timeframe identified by the SWOT analysis are outlined in Table 18 (Appendix Q.4). Availability of the various personnel to undertake their respective works (particularly the interface works) led to project delays experienced.

“the biggest delay has been [Company Y]” (Participant 3)

“the thing holding you up is the IT stuff to connect it” (Participant 2)

Additionally, the co-ordination of the large number of people involved in the project to ensure works were completed to enable contingent works to be undertaken was also a threat.

“it’s huge, it’s a really big project” (Participant 3)

“I think the team / group that [name] put together from the laboratory, clinical, IT, MPBE [Medical Physics & Bioengineering]” (Participant 1)

There was also a lack of an overall project plan encompassing all disciplines / tasks:

“is there an IT project plan after the implementation of the analysers?” “how are there 2 project plans?” (Participant 10)

“the major project plan probably has 3 or 4 parts, each one with its own project plan feeding into the overall” (Participant 3)

5.3.2 Thematic analysis Findings

In addition to the strengths, weaknesses, opportunities and threats the following themes were identified from the assessment transcript and interviewer notes:

- Terminology
- Documentation - formal & informal
- Resources (personnel & information)
- Formal versus informal processes
- Tendering process
- Role of Meetings
- Roles / Responsibilities
- Collaboration / Integration of separate/shared processes
- Operational / Performance Feedback
- Project Planning / Project Plan(s)
- Timing of the assessment
- Learning among project members
- Adherence to standards

A copy of this transcript is included in Appendix S. These themes will be discussed in section 6.2.

5.4 Questionnaire Analysis

The results of questionnaire (n=11) analysis are presented in tables and graphs below.

5.5 Questionnaire Findings

5.5.1 Demographics

The response rate was 100% (n=11), 27% (n=3) of respondents were male and 73% (n=8) were female. Respondents were from various disciplines (Table 8).

Roles of Questionnaire Respondents (n=11)

Role of Participant	Number of participants
Clinical user	1
Laboratory IT	1
IT applications	1
Clinical Information System (CIS) Configurator	2
Medical device supplier	2
Medical Physics & Bioengineering (MPBE)	1
Risk Manager	1
Laboratory Point of Care Testing (POCT)*	2

*The project manager was one of the Laboratory POCT personnel

Table 8 Roles of Questionnaire Respondents.

5.5.2 Standards

The majority of respondents (82%, n=9) either strongly agreed (46%, n=5) or agreed (36%, n=4) that they used standards in a professional capacity, while two respondents (18%) had not used standards (Figure 6). This is important as will be seen later in chapter 6. 64% of respondents (n=7) specified the standards (e.g. ISO, accreditation (n=3) and clinical practice (n=2)) used (Table 9).

Question 1 I have used standards in a professional capacity previously? (n=11)

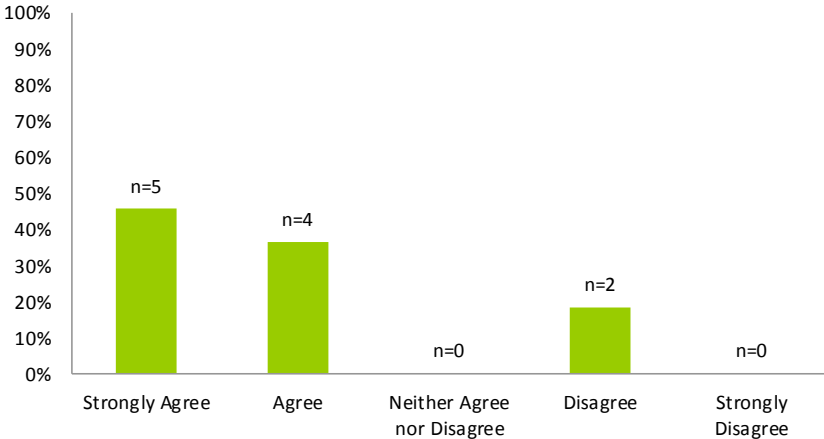


Figure 6 Number/percentage of respondents that had used standards previously.

Question 1 (b) If you have used standards, please indicate the standards used?	
Types of standards used*	Number of participants
BS EN ISO 9000 “Quality management systems - Fundamentals & vocabulary” (British Standards Institution (BSI) 2000) (identical to European standard ISO 9000)	1
ISO 22870 <i>Point-of-care testing (POCT) - Requirements for Quality and Competence</i> (International Organization for Standardization (ISO) 2006)	2
ISO 15189 “ <i>Medical laboratories - Requirements for quality and competence</i> ” (International Organization for Standardization (ISO) 2012)	2
Clinical practice standards	2
Accreditation & regulatory processes (including Irish National Accreditation Board (INAB))	2
HIQA	1
CPA standard for medical laboratories (Clinical Pathology Accreditation (CPA) UK Ltd 2010)	2
Standards used but unspecified	2
# Some standards were used by more than one respondent	

Table 9 Types of standards used by respondents

Participants were asked to rate their level of awareness of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) between 0 - 5 where 0 = indicates not aware and 5 indicates very aware. There was a general lack of awareness of the standard. Interestingly, prior to participating in the assessment, the respondent’s level of awareness of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) was low (Figure 7) with 73% of respondents (n=8) indicating a level of awareness of 0 (55%, n=6) or 1 (18%, n=2). The level of awareness of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) after participating in the assessment was high with 100% of respondents (n=11) indicating a level of awareness of 3-5 (Figure 7). This demonstrates that the study achieved research objective 6 to raise awareness of the standard among healthcare personnel.

Question 2 (a) Level of awareness pre assessment
Question 2 (b) Level of awareness post assessment
(n=11)

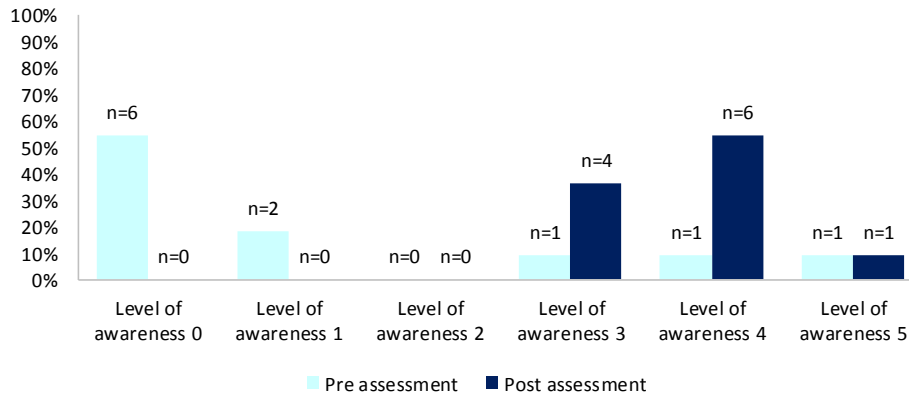


Figure 7 Level of Awareness of IEC 80001-1.

5.5.3 Pre-assessment Presentation

As discussed in section 4.2.7 a pre-assessment presentation (Appendix K) provided participants with information on the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) and process assessment. Respondents (100%) agreed that this presentation was clear (Figure 8).

Question 3 The pre assessment presentation was clear? (n=11)

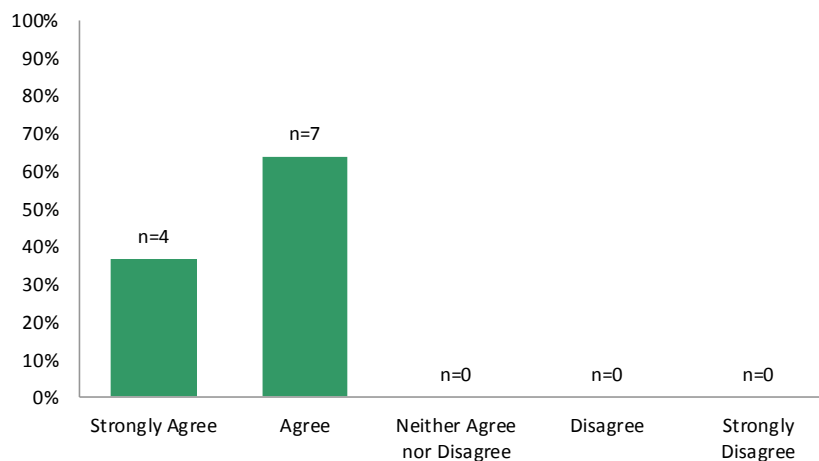


Figure 8 Clarity of the Pre-Assessment Presentation

The majority of respondents (91%, n=10), agreed that the pre-assessment presentation provided enough information on IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) (Figure 9).

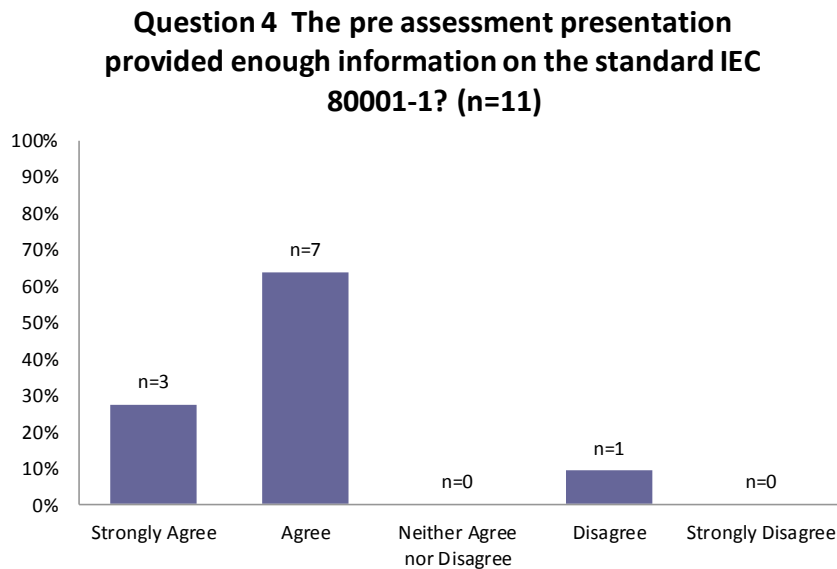


Figure 9 The pre-assessment provided enough information on IEC 80001-1 (IEC 2010)

Most of the respondents (82%, n=9), either agreed or strongly agreed that the pre-assessment presentation provided enough information on process assessment (Figure 10).

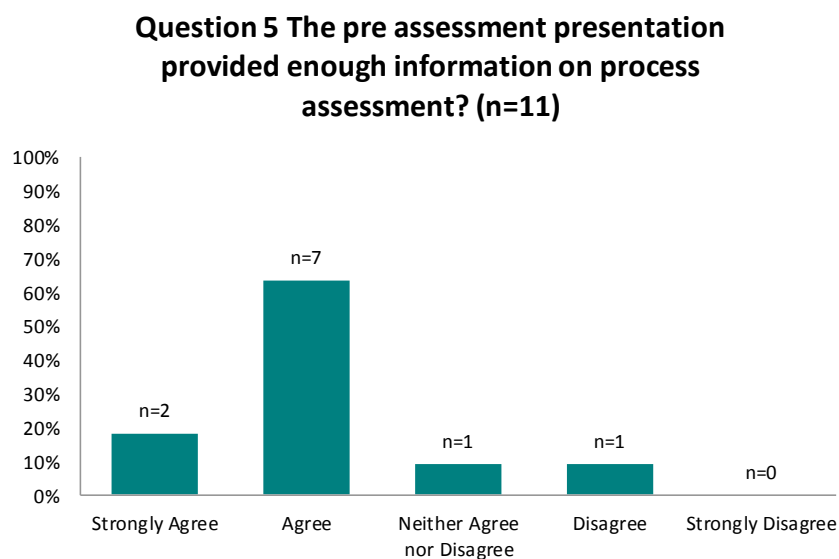


Figure 10 The pre-assessment presentation provided enough information on process assessment.

27% of respondents (n=3) either agreed (18%, n=2) or strongly agreed (9%, n=1) that the pre-assessment presentation could have provided additional information, while 36% (n=4) disagreed (Figure 11).

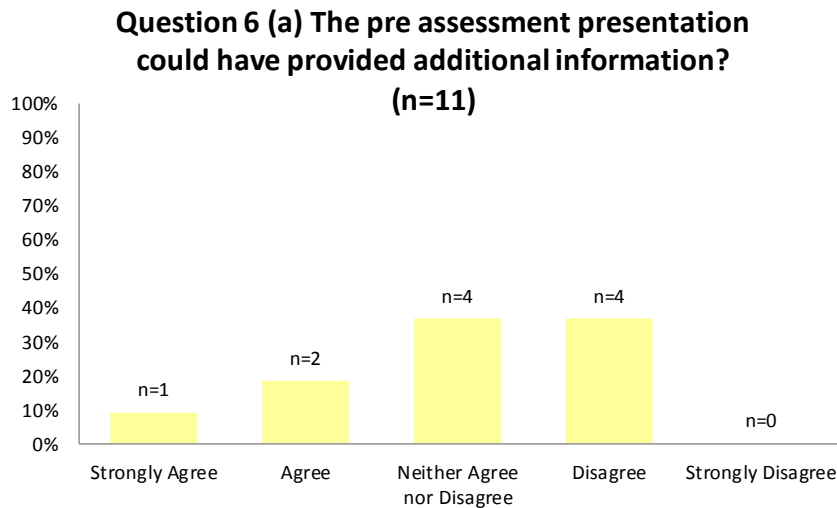


Figure 11 The pre-assessment presentation could have provided additional information.

In relation to what additional information respondents felt was missing from the pre-assessment presentation, one respondent (9%) did not specify the additional information that could have been provided, while 2 respondents (18%) provided comments (Table 10).

Q6 (b) What additional information did you feel was missing (from the pre-assessment presentation)?

- Comment 1 The scope of works is clearly defined in the project.

- Comment 2 The additional information is more to do with the requirement to absorb and comprehend the different elements covered in the assessment & the distinction between each. Covering such an extensive topic for an initial phase will always be challenging from the level of data being introduced & given the amount of time available to impart this information.

Table 10 Additional Information missing from the pre- assessment presentation.

5.5.4 Assessment - Standard 80001-1 (International Electrotechnical Commission (IEC) 2010)

Successfully performing the assessment using the developed assessment method validated the question set as suitable for use in the context of a medical IT-network modification project (research objective 2). Generally, assessment participants agreed (63%, n=7) that the assessment questions were clear/easy to understand (Figure 12).

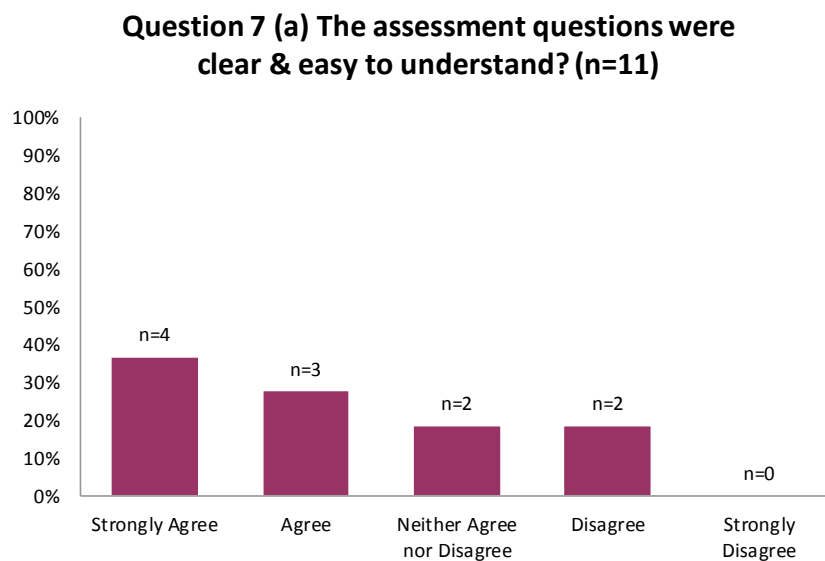


Figure 12 The assessment questions were clear & easy to understand.

Only 18% of respondents (n=2) disagreed that the assessment questions were clear/easy to understand, and 18% (n=2) also neither agreed nor disagreed. The reasons given for the assessment questions not being clear/easy to understand included:

“difficult to interpret what the questions meant” (Respondent 8)

“a lot of the questions were it seemed repeated” (Respondent 10)

“More to do with understanding where questions related to differing stages of the standard being applied / assessed” (Respondent 11)

However, questions that seemed to be repeated were not identified by respondents, but some repetition in the questions was noted during the assessment (see section 4.2.13). Respondents (n=11) indicated that the assessment questions adequately addressed the risk management processes (Figure 13).

Question 8 (a) The assessment questions adequately addressed the risk management processes? (n=11)

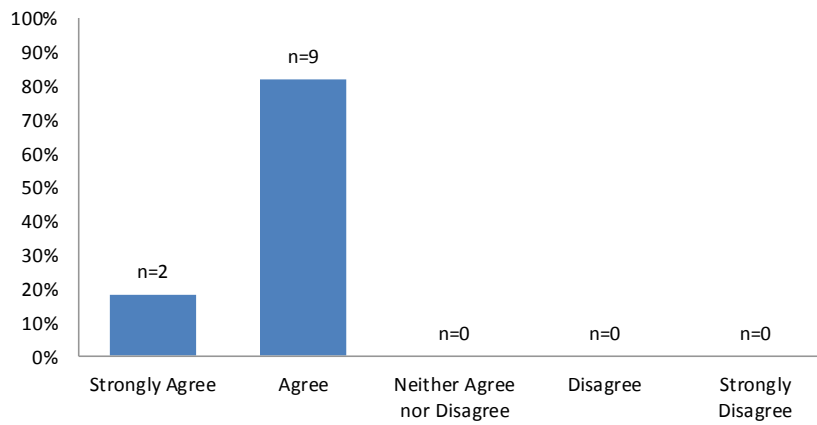


Figure 13 The Assessment questions adequately addressed risk management processes.

All respondents either strongly agreed (55%, n=6) or agreed (46%, n=5) that participating in the assessment increased their knowledge and understanding of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) (Figure 14).

Question 9 (a) Participating in the assessment increased my knowledge & understanding of IEC 80001-1? (n=11)

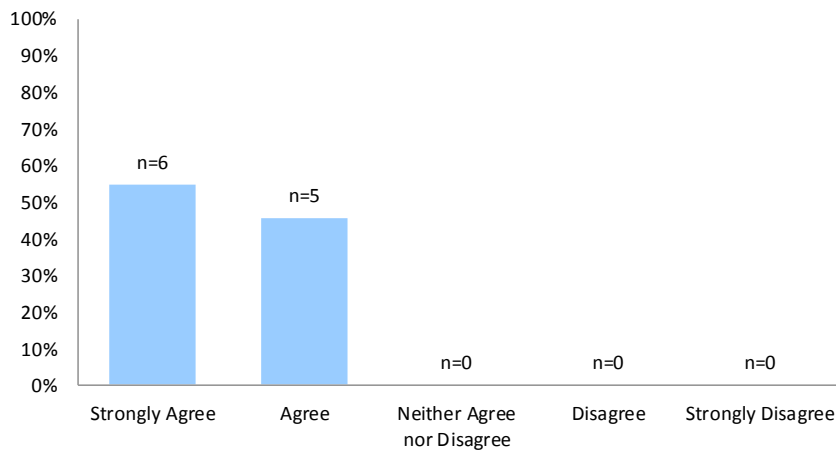


Figure 14 Participating in the assessment increased my knowledge & understanding of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

The majority of respondents (91%, n=10) agreed that they could use their increased knowledge and understanding of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) in their work (Figure 15).

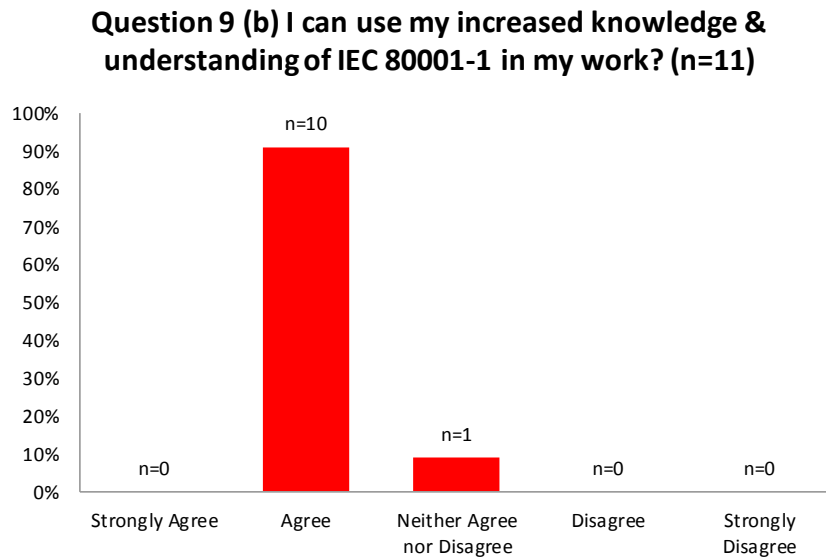


Figure 15 I can use my increased knowledge & understanding of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) in my work.

Similarly, the majority of respondents (82%, n=9) agreed or strongly agreed (18%, n=2) that participating in the assessment has informed them of the risk management activity requirements of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) (Figure 16).

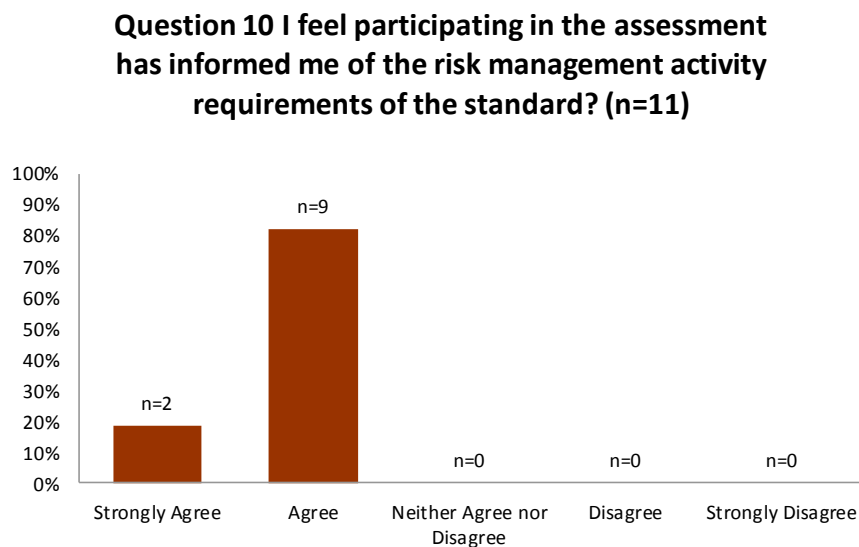


Figure 16 I feel participating in the assessment has informed me of the risk management activity requirements of the standard.

Regarding the assessment method, 64% of respondents (n=7) agreed and 18% strongly agreed (n=2) that the assessment method seemed appropriate; while 18% indicated they neither agreed nor disagreed (Figure 17).

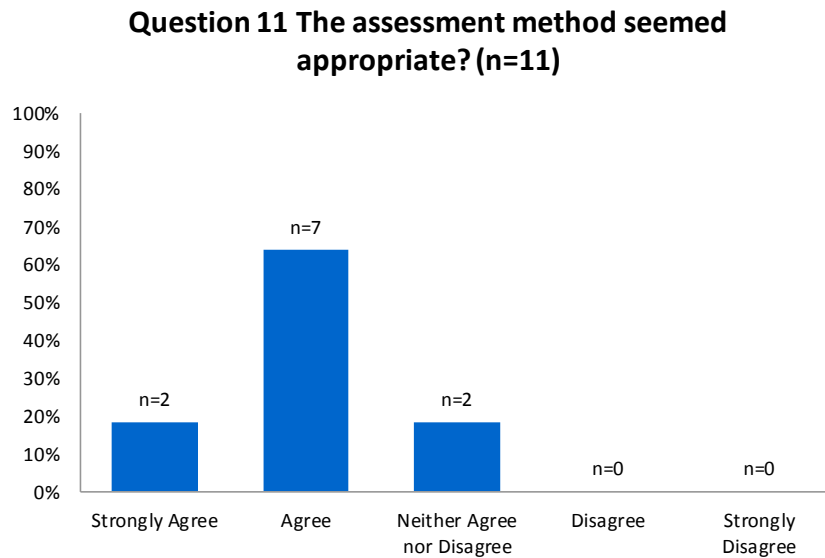


Figure 17 The assessment method seemed appropriate.

Over half the respondents 55% (n=6) provided additional comments regarding the assessment (Appendix T Table 20). Comments were mainly positive such as:

“got a very good understanding of the standard and will be more aware and confident to use the standard in the next project of a similar nature” (Participant 4).

“very interesting and informative process” (Participant 6) and

One participant commented that questions overlapped:

“There was overlap in many of the questions” (Participant 3)

5.6 Validation of assessment questions

The transcripts and interview notes of the assessment and the completed questionnaires were reviewed to identify changes required to the assessment questions. Participants felt there was overlap in some of the questions.

“I think a lot of them [questions] are repetitive as in you feel you have addressed this already (Participant 8)

Question 8 seemed to be asking the same thing as question 7 in terms of response:

Q7: How do you analyse the system as a whole to identify likely safety hazards?

Q8: How do you consider the impact of the device on the environment, effectiveness, data security and system security?

“that’s risk assessment we have covered that” (Participant 3)

Likewise Question 28 and Question 29:

Q28 Has an event management process been established?

Q29 Are negative events captured and documented?

“yes I suppose as above for Q28” (Researcher)

The following changes to the questions were made: Guidance section for question 7 amended to highlight it’s the analysis of the system as a whole and question 8 to focus on the impact of the individual device. Similarly, question 28 guidance amended, question 29 (Are negative events captured/documentated as per event management process) amended and question 29 guidance amended to distinguish between the event management process (question 28) and its application (ie capture/documentation of events) question 29. The revised questions are shown in Appendix M with changes highlighted.

5.7 Individual Interviews Analysis

The purpose of the individual interviews is outlined in section 3.4.1.3 and the interviews were transcribed and analysed as described in section 3.6.16 and section 4.2.16. Individual interviews (n=6) were undertaken with assessment participants representing various disciplines (Table 11).

Roles of Interviewees (n=6)	
Role of Participant	Number of participants
Clinical user	1
Laboratory IT	1
Clinical Information System (CIS) Configurator	1
Medical Device Supplier	1
Medical Physics & Bioengineering (MPBE)	1
Laboratory Point of Care Testing (POCT)*	1

*also the project manager

Table 11 Roles of Interviewees

5.8 Individual Interview Findings

Research objectives 3 and 4 were to develop and validate recommendations arising from the assessment. As discussed previously, these recommendations were included in the findings report (achieving research objective 3) and the focus of the individual interviews for validation purposes.

5.8.1 Feedback on Findings Report

The interviewees agreed that the recommendations were valid (100%, n=6) and indicated that recommendations could be implemented (83%, n=5) (Table 12). One interviewee didn't specifically answer question 3.

Feedback on the Findings Report from Interviewees					
Question	Yes %	Yes Number	No %	No Number	Comments
Q1 Have you had time to read the findings report?	83%	5	17%	1	"Yes I had a read through them at the time" (Participant 1)
Q2 Do you agree with the recommendations outlined?	100%	6	0%	0	"I agree with all of them" (Participant 4)
Q3 Can the recommendations be implemented?	83%	5	0%	0	"Yes, I don't see why not" (Participant 3)

Table 12 Feedback on the Findings Report from Interviewees

5.8.2 Review & Allocation of Recommendations

The recommendations in the assessment findings report are listed in Appendix U Table 19. These recommendations were reviewed and discussed by interviewees and the researcher. The recommendations applicable to each interviewee were identified (Appendix V Table 22). Many recommendations were applicable to several interviewees; all were accepted /allocated among the interviewees except one (Number 13) which was allocated to another team member.

5.8.3 Thematic Analysis of Interviews

The following themes emerged from the review of recommendations and additional comments from interviewees:

- Assessment
- Lack of awareness / Knowledge, Learning
- Practice review & improvements
- Areas of responsibility & role
- Project team – makeup, relationships, culture
- Training
- Delays
- Formal & informal processes & consequences of same
- Formal & informal documentation

These themes are discussed in chapter 6 section 6.2.

5.9 Summary

The findings from the IEC 80001 assessment, questionnaires and interviews have been presented using tables, graphs and explanatory text including direct quotes from participants which have been anonymised to preserve confidentiality. These findings will now be discussed in chapter 6 in light of the published literature and the research objectives.

Chapter 6 Discussion of Findings

6.1 Introduction

Chapter 5 presented the findings of this research using graphs, tables and text. This chapter will discuss those findings in light of the published literature and the achievement of the research objectives. The choice and implementation of methodology and choice of IT-network modification project will also be examined. A synopsis of the impact of the study is presented. Study limitations are outlined. Finally, suggestions for future research are included.

6.2 Discussion of Findings

6.2.1 Use of standards

The findings show that the use of standards among risk management stakeholders involved in the medical IT-network modification project was high (82% of participants (n=9) indicated they use standards in their work). Participants used accreditation and clinical practice standards. It is also clear that international standards are used. Participants named specific ISO standards used such as the laboratory standard ISO 15189 (International Organization for Standardization (ISO) 2012), POCT standard ISO 22870 (International Organization for Standardization (ISO) 2006) and ISO 9000 (International Standardisation Organisation (ISO) 2005) described in the literature review. However, it is interesting to note that none of the participants reported having used IEC 80001-1, even though this standard is specifically addressed to healthcare organisation's risk management of medical IT-networks; which this project involved. Indeed, participants (73%) reported a low level of awareness of the standard prior to the study which could explain this reported non-use. The literature reports a lack of an assessment method as a barrier to implementation MacMahon *et al.* (2012), which indeed it is, but lack of awareness of the standard is certainly worth considering as a contributory factor.

Participation in the assessment increased the participant's knowledge and awareness of the standard, with 100% of participants indicating a level of awareness of 3-5 (scale 0-5) following the assessment. More importantly, from a patient safety perspective, the majority of participants indicated that they can use their increased knowledge and understanding in their work; which will enhance patient safety in relation to medical IT-networks (see section 6.6.1). Participants reported that there are standards (eg security standards) that MDMs and suppliers must comply with, and compliance is checked before the device is incorporated onto the network in the test environment and extensively tested before Go-Live as described in ISO 20000-2 Part 1 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2005b). Participants also

reported being better informed regarding the risk management activity requirements of the standard as a result of participation.

6.2.2 Risk Management Resources

The standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) advocates the appointment of a medical IT-network risk manager whose responsibility includes management and performance of the risk management process, and managing communication between participants in risk management. There is no medical IT-network risk manager at the study site. In the absence of this role, components of the role were undertaken by different members of the project team (project manager, clinical informatics and IT personnel). This led to a lack of clarity as to who had overall responsibility of managing the risks associated with incorporating the analysers on the network and interfacing them to the CIS. In the absence of this role, it would seem to fall to the project manager to fulfil this function. Indeed, this was expressed by one of the participants:

“who has the responsibility for the risk” (Participant 9)

Response: “the project manager” (Participant 8)

Cooper *et al.* (2011) recommend that in smaller organisations the role of project manager and medical IT-network risk manager may be undertaken by the same person, but in larger organisations the roles need to be independent. It was suggested at the assessment that the project manager should assume this role, given their global view as project manager. But, when the project manager is from a department other than IT, as was the case in the project under study, they may be unaware or not focused on the IT risks. Indeed, this is reflected in the following comment:

“we may not have identified all risks in relation to putting them on the network that wouldn’t have been our main focus” (Participant [number])

Moreover, the person managing the project (project manager) was only formally identified during the assessment. The risk manager was not involved in the project until the assessment, and their advice offered proved useful, suggesting that earlier involvement would have been beneficial. Hegarty *et al.* (2014) reported that the role of the medical IT-network risk manager in relation to risk management of a CIS was informally assumed by the project manager, who had a clinical engineering background. In our study the clinical engineer was mainly involved in the later stages of the project for validation works and therefore would not have been in a position to undertake the role of medical IT-network risk manager. In a similar medical IT-network modification project

involving a CIS, perhaps the role could be assumed by a clinical informatics person, given that they have oversight of the CIS architecture configuration and interfaced devices. But, the informatics person (if there is one) may not be aware of other IT-network components or projects and some medical IT-network modification projects may not involve a CIS. The author therefore suggests that in the absence of a medical IT-network risk manager; this role should be undertaken by the member of the IT department involved in the project. In terms of risk management resources, there were relevant personnel involved, although not formally assigned as advocated in the standard. Participants reported that risk management was an additional burden (in terms of time required to undertake risk management processes and documentation) on their normal role.

“to do a lot of the stuff it’s very time consuming, now a lot of it can be worth it” (Participant 5)

Indeed, it is acknowledged that risk management increases the effort required to deploy a medical device on the IT-network, however the benefits in terms of a secure network and increased patient safety outweigh any costs incurred (Ahlbrandt & Röhrig 2013b).

6.2.3 Documentation of Risk Management Activities

The standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) recommends that the responsible organisation (e.g. hospital), establish and maintain a medical IT-network risk management file with specified contents. The assessment revealed an absence of this file. This meant risk management activities were mainly informally documented in the minutes of project meetings and clinical information system multi-disciplinary meetings. The problem with meeting minutes as a source of risk management information is that risk may not receive the attention focus it deserves, and it may be difficult to assess the quality of the documentation. The lack of specific risk management documentation meant that documentation of risk management activities was inadequate; there was no documented list of risks with corresponding risk control measures, no description of risk relevant assets and no system architecture diagram showing data flow. A deficit in formal documentation of risk management processes as advocated by IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) was also highlighted by Hegarty *et al.* (2014). Formal documentation of the validation processes for the analysers and the network interfaces was evident, a finding also reported by Hegarty *et al.* (2014).

6.2.4 Risk management processes

The assessment identified which risk management processes were in place and which ones were lacking. Change release processes were followed, negative events were captured and documented as per event management process, the nature of the change was identified and the need for a responsibility agreement had been determined. However, although there was a corporate risk management policy and process with involvement of top management, there was no formal risk management plan or established process in use at project level. Many of the risk management processes were reported as being undertaken informally.

Risks had been discussed informally, risk assessments had been carried out in relation to the analysers themselves by laboratory staff, but risks related to the medical IT-network appeared to have been given less attention. Although the focus of IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) is the risks related to the IT-network, it was highlighted that when performing an assessment, risks relating to the devices themselves and those related to the network need to be examined simultaneously. This is because at times the risks related to the analysers themselves can lead to or cause risks due to the incorporation on the IT-network and vice versa. For example if an operator enters the wrong patient name or medical record number (MRN) the results will not be sent to the patients chart but they may be sent to another patient's chart via the network.

The assessment identified risks to patient safety from networked POCT analysers: data download failure, download to wrong chart due to incorrect MRN or data entry error on the analyser during POCT ABG analysis, user fails to mark sample type as venous, transcription errors, power outage, results only available in ICU. Many of these risks are also reported in the literature (Malloch 2007; Lewandrowski *et al.* 2011; Ward *et al.* 2012). Following the assessment formal documented risk assessment with identification of errors in the pre-analytic, analytic and post analytic phases as classified by Kost (2001) was undertaken. Indeed, a proper assessment can reduce potential harm and financial liabilities (Ahlbrandt & Röhrig 2013b). These risks were either eliminated or minimised via identified risk control measures post assessment as advocated by the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

During the assessment the lack of a process for monitoring and inclusion of monitoring requirements in the project plan were identified. A monitoring plan was established with continuation of the patient identification audit and monitoring of result reporting to detect errors in POCT as advocated by Meier & Jones (2005) was initiated. This led to identification of data entry errors (0.04%), the causes were determined and addressed.

6.2.5 Communication / Collaboration

Ahlbrandt & Röhrig (2013b) reported improved communication and transparency among participants involved in an IEC 80001-1 (2010) implementation project. This study supports this finding as the assessment of a medical IT-network modification project against IEC 80001-1 (2010) resulted in improved communication and transparency among the risk management stakeholders. Roles and responsibilities were also clarified by the designation of individuals to address specific recommendations. Prior to the assessment, project meetings were held with sub groups of the project team and therefore some participants were unaware of the numbers of stakeholders involved as this comment demonstrates:

“to see how many people are actually involved in the project, when you have everybody in one room, you know I didn’t realise there were that many people within [Hospital name] involved in the project and the impact of that”(Participant 5)

Additionally, it was identified that the different disciplines had individual project plans and there was a lack of an overall plan. This reduced total project transparency in terms of tasks/deliverables and may have contributed to project delays. Participant 1 expressed this:

“everyone has their own project plan, we realise we could have been more integrated” (Participant 1)

Following the assessment, project meetings became more inclusive of the entire team, and communication and collaboration among participants was improved with an increased awareness and appreciation for the different roles involved. The overall project plan was also reviewed and updated to include all major tasks / activities from the various disciplines (Recommendation 2).

6.2.6 IEC 80001 Assessment Method - Validation

The primary purpose of the assessment was to validate the developed assessment method (assessment criteria questions) for IEC 80001-1 (2010). This was achieved by using it in the context of a real medical IT-network modification project in a healthcare organisation to identify the risk management processes employed. This use in context is a key feature of design research (Hevner *et al.* 2004) employed in this study. The assessment did identify the risk management processes employed, highlighted shortcomings and areas for improvement discussed in sections 6.2.1 – 6.2.3. This is in accordance with one of the key objectives of process assessment outlined in the standard for process assessment (International Organization for Standardization (ISO) & International

Electrotechnical Commission (IEC) 2003). The assessment questions generated discussion around risk/risk management. At times the terminology of the questions was unfamiliar to participants as expressed by participant 4:

“We just don’t use the terms” (Participant 4)

Therefore, the supporting guidance from the assessment tool was used to clarify and aid understanding. Hegarty *et al.* (2014) also noted a lack of familiarity of healthcare personnel with the industry terms for process improvement expressed in the standard IEC 80001-1 (2010).

As 63% of participants indicated the assessment questions were clear and easy to understand only minor changes were made to assessment questions (section 5.6.) Participants also indicated that the questions adequately addressed the risk management processes outlined in the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). Participants indicated that they would use the assessment tool with accompanying guidance in future medical IT-network modification projects. This suggests that the assessment questions are indeed useful and fit for their intended purpose of assessment against IEC 80001-1 (IEC 2010). The assessment method developed also underwent validation through international experts. The final assessment method which contains a planned approach to performing an assessment and the assessment questions is outlined in ISO/IEC TR 80001-2-7 and is due for publication later in 2014.

6.2.7 Assessment against IEC 80001-1- Timing

The assessment was conducted 5 months into the medical IT-network modification project (duration 9 months) with the entire project team. It was suggested by participants that the assessment would be of greater benefit if it was conducted prior to the start of the project to identify requirements of the standard that need to be complied with. However, how do you assess something that isn’t yet done! Perhaps medical device (MD) suppliers looking for an “edge” could offer healthcare organisations assistance in applying IEC 80001 (2010), capitalising and sharing their experiences in medical device implementations across multiple sites. Indeed the analyser supplier involved in this study indicated that they would use the experience in their next implementation:

***“I suppose from the standard here and the risks that we are talking about, maybe it’s something that I will definitely think about in future projects”
(Participant [number])***

According to Ahlbrandt & Röhrig (2013a), however some manufacturers have to be convinced to participate in risk management.

Another possibility is to undertake a multi stage assessment. The first assessment could be undertaken prior to the project commencement or even before going out to tender as suggested by Participant 7:

“I actually think you need to do this process before you go out to tender, there are a lot of questions that really you need to ask manufacturers” (Participant 7)

The second stage assessment could be undertaken mid project and a final assessment performed post Go-Live on project completion. This multi stage assessment along with document review at each stage is perhaps the best way to ensure the requirements of IEC 80001-1 (2010) are met and that all the necessary inputs and outputs are in place. Section 6.3 will review the research objectives.

6.3 Achievement of Objectives

6.3.1 Research Objective 1: To contribute to the development of the assessment criteria questions in ISO/IEC TR 80001-2-7 (ISO & IEC 2014)

The researcher and the developer of the Technical report ISO/IEC TR 80001-2-7 due for publication in 2014 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014), jointly participated in an assessment criteria development workshop. This resulted in the development of the assessment criteria questions component of the assessment framework for the risk management processes outlined in IEC 80001 (International Electrotechnical Commission (IEC) 2010).

6.3.2 Research Objective 2: To validate the developed question set

An assessment of a real medical IT-network modification project (to replace the POCT ABG analysers in use and add them to the medical IT-network) in a healthcare organisation was performed using a subset of the questions developed.

6.3.3 Research Objective 3: To develop a set of recommendations to address any weaknesses identified during the assessment

Following the assessment against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010), a SWOT analysis (Berry 2013) was performed. The results of the SWOT analysis along with recommendations to address weaknesses and areas for improvement were included in a findings report (Appendix U).

6.3.4 Research Objective 4: To validate recommendations arising from the assessment of the IT-network modification project

Interviews conducted with assessment participants validated the recommendations arising from the assessment. All participants agreed with the recommendations and agreed to implement them.

6.3.5 Research Objective 5: To utilise the assessment feedback to refine the criteria question set that is part of the output of this work

Questionnaires were used to collect feedback on the assessment method and questions from participants. The findings from the questionnaire and the assessment itself were used to identify changes to the assessment tool for use in future assessments.

6.3.6 Research Objective 6: To raise awareness of the standard among healthcare stakeholders

The level of awareness of the standard among risk management stakeholders involved in the assessment was low. Following the assessment the level of awareness of the standard had increased. The increased awareness can be attributed to the provision of information regarding the standard in the study participant information sheet, provision of a presentation overview of the standard, and participation in the assessment against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). Publication of the results of this study would add to the limited body of knowledge regarding implementation of IEC 80001-1 (IEC 2010).

6.3.7 Research Objective 7: To improve risk management processes related to a medical IT-network modification project

The assessment highlighted gaps in the risk management processes related to the medical IT-network modification project. These gaps were incorporated into the recommendations that arose from the assessment. Implementation of the recommendations resulted in improvements to the risk management processes of the project and improved documentation of these processes. A review of the recommendation implementation status post Go-Live revealed that 89% (n=16) of the recommendations were implemented with implementation of the remaining two in progress (Appendix N Table 14).

6.4 Choice & Implementation of Methodology

This study's methodology is outlined in chapter 3 and 4. The study adopted the *Pragmatism* paradigm, design research and a mixed methodology for data collection and analysis. Design research as described by Hevner *et al.* (2004), provided the ideal framework for the design and

validation of an assessment method for IEC 80001-1 (International Electrotechnical Commission (IEC) 2010); whereby the developed artefact was used in context. The feedback gained was used to refine the assessment method questions. Indeed, Tuffley (2012) also used design research to develop and validate a process reference model for organisational behaviour (RMOB) and used a focus group to improve the usability and usefulness of the model.

The ability of the focus group to provide in-depth information as reported by Morgan (1996) led to a clear understanding of risk management of the medical IT-network modification project. This highlighted both strengths and weaknesses. The focus group also provided a means of capturing the individual perspectives among the project team and the diversity within the team in terms of risk management behaviour. For example some participants answered no to a question while others were able to answer yes. This ability of focus groups to observe the extent and nature of participants agreement / disagreement is a unique strength of focus groups (Morgan 1996).

The recording of the 1.5 hour assessment worked well, although the transcribing of the assessment was labour intensive and at times challenging when several participants spoke simultaneously. The questionnaires used were an excellent anonymous means of capturing the feedback of participants. The individual interviews, aimed at reviewing the findings/recommendations also yielded additional information regarding the assessment.

6.5 Choice of Medical IT-network Modification Project

Cooper *et al.* (2011) suggest that starting to apply the standard IEC 80001-1 to the whole network is unrealistic, and recommend choosing a new project or a portion of the network as a starting point. The medical IT-network modification project: to replace the POCT ABG analysers and add them to the network was the chosen project for the reasons outlined in section 4.2.3. One of the principal reasons for choosing this specific project was the patient safety issues inherent in POCT ABG analysis in ICU as highlighted (section 2.4.1). The choice of this project proved to be useful as the project involved a large number of risk management stakeholders. Indeed, the number of stakeholders involved only became evident to some stakeholders at the assessment.

A decision was taken to use a bi-directional interface between the POCT analysers and the laboratory system using a non-proprietary database manager/integration engine. This will cater for all POCT devices from multiple MDMs which has been shown to greatly improve the quality of POCT and the ability of hospital staff to effectively manage POCT (Lewandrowski *et al.* 2011). This decision added two more suppliers of IT applications (i.e. laboratory and data manager systems), increasing the complexity of the interface works. This complexity added to the project delays experienced. However, the benefits of the revised network configuration led to improved management of POCT

devices regarding: training and certification of users, remote diagnostics and availability of POCT results across the hospital which were worth the extra effort involved. Implementation of the POCT analysers complied with the POCT standards and guidelines outlined earlier in section 2.10.4 in order to maximise patient benefit and minimise testing errors (Farrance 2012).

6.6 Study Impact

This study had a positive local impact and contributed to an international standard.

6.6.1 Local Impact

This study was conducted in the ICUs of an academic teaching hospital. There are frequent modifications to both the CIS in use and the medical devices connected to it via the hospital IT-network. This has implications for patient safety, if formal risk management processes are not adhered to, risks are not identified and effective control measures implemented (The Joint Commission 2008). This study had a positive effect on the risk management of a medical IT-network modification project at the study site. The assessment highlighted gaps in risk management processes for this particular project which were addressed following the assessment. A findings report was compiled which identified strengths, weaknesses, opportunities and threats and outlined recommendations to improve risk management processes and fulfil requirements of the standard. These recommendations were implemented. This led to improved project risk management processes, improved formal documentation of those processes and a reduction in patient safety risks. In addition, the practices and procedures of individual roles were reviewed and improved as a direct result of study participation.

Many of the study participants were unaware of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) and none had used it in their practice. Many of the participants expressed an appreciation for being made aware of the standard and indicated that they would use this new awareness in their work, thereby perpetuating the positive benefits of the study for future projects. In addition, participants indicated that the assessment tool would be a useful checklist for future projects and that they would use this in their work, thereby applying risk management processes as advocated by IEC 80001-1 in future projects. Some of the participants were external to the study site and therefore the likelihood of their changes in practice and increased knowledge positively affecting numerous sites is increased.

6.6.2 International Impact - Standards Development Contribution

This study contributed to the development & validation of an assessment method for IEC 80001-1 (2010). The assessment method was developed in conjunction with the developer of the IEC 80001-1 PAM and is included in the Technical Report ISO/IEC TR 80001-2-7: *“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”* (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) due for publication shortly. The author reviewed & submitted comments to the NSAI on the committee draft of ISO/TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) based on experiences gained with using the developed assessment method in context for validation purposes. The author participated in the comments resolution process to address the application of suggested changes to the document. Following the assessment the author provided a copy of the sample assessment tool used and revised questions for possible inclusion in ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014).

6.7 Limitations of this Study

This study is based in one healthcare institution and around an assessment of one medical IT-network modification project, so therefore findings cannot be generalised across all medical IT-network modification projects. However, the study did provide valuable insights into projects of this nature and the issues that arose are I suspect not specific to this particular project.

6.8 Future Work

6.8.1 Capability / compliance level measurement

A determination of capability/ compliance level to IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) using the measurement framework defined in ISO/IEC 15504-2: *“Software Engineering - Process Assessment Part 2: Performing an Assessment”* (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003) could be established. The measure of capability would be based on a set of process attributes (base practices), and the extent of process attribute achievement could be measured on a defined rating scale as described in ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). It was not possible to measure the capability level in this study, as only a selection of base practices for each process were assessed, therefore future studies should examine a number of processes in their entirety and then measure the process capability

levels as per ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003).

6.8.2 Survey of hospitals to determine use of standards and in particular level of awareness and use of IEC 80001-1 (2010)

It would be interesting to conduct a survey of Irish acute hospitals to determine use of standards and level of awareness/use of IEC 80001-1 (2010) among risk management stakeholders (particularly healthcare informatics personnel). It would also be important to examine utilisation of the developed assessment method contained in ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) for medical IT-network modification projects across multiple healthcare sites. This would determine compliance with IEC 80001-1 (2010) and potentially improve risk management of medical IT-network modification projects to enhance patient safety.

6.8.3 Standards Development Potential

This work represents a pattern which could be used to invigorate the standards development community. The possibility for other Masters Research studies to be focused on standards development work and contribute real live scenarios to the standards and technical reports developed, is a potentially as yet untapped resource. Indeed, conduct of this study enabled the author to provide comments through the NSAI on a committee draft of the technical report (ISO/IEC TR 80001-2-7) for IEC 80001-1 as described in section 6.6.2. This valuable contribution is acknowledged in Appendix O. The benefits for the standards development community are enormous in terms of furthering the valuable standards work. However, even more importantly bringing standards and standard development to the coalface of healthcare informatics/healthcare delivery, and receiving feedback from end users; would I think be an invaluable asset to healthcare informatics and standards development communities. This will ultimately benefit the patient in terms of patient safety. Healthcare personnel involvement in standards development would serve to inform and raise awareness of standards but more importantly, to positively affect their implementation at a healthcare delivery level. HIQA do use public consultation for standards being developed and encourage healthcare providers to contribute (Health Information & Quality Authority (HIQA) 2012c).

6.9 Reflection

The sheer volume of standards related to patient safety, risk, medical devices and IT was overwhelming. Many of these standards and terminology were unfamiliar to the clinical author and were difficult to understand. Performance of the assessment provided the project team an opportunity to meet and examine the project in light of the requirements of the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010). Providing the pre-assessment presentation on the standard to work colleagues and medical device suppliers; while daunting for the author was well received by participants and contributed to their increased awareness of the standard. Undertaking the assessment and following up on recommendations required time and effort, but a raised awareness of the risks involved in medical IT-network modifications for patient safety provided encouragement. The involvement in standards development work, comments resolution process of the ISO/IEC TR 80001-2-7 afforded by this work were challenging and rewarding; knowing that this contribution is appreciated and useful is highly satisfying. The author looks forward to continuing involvement in standards development work in the future.

6.10 Summary

The findings of this research have been discussed in light of the literature. Limitations of the study have been outlined and possibilities for future work have been proposed. Reflection on the study is also included. Chapter 7 will provide the study conclusions and a summary of the research.

Chapter 7 Summary & Conclusion

7.1 Summary

The literature review highlighted the increasing use of medical devices incorporated into IT-networks and the need to manage the risks to patient safety to prevent unintended consequences and patient harm. The standard IEC 80001-1 *“Application of risk management for IT networks incorporating medical devices - Part 1: Roles, responsibilities and activities”* (International Electrotechnical Commission (IEC) 2010) was developed to address these patient safety risks from medical IT-networks. Evidence of implementation of the standard is scarce, but studies have shown: identification of risks involved in incorporation of medical devices onto the medical IT-network, improved collaboration among stakeholders and improved risk management of medical IT-networks. The lack of evidence of standard implementation has been attributed to the lack of an assessment method to assess compliance with the standard (MacMahon et al. 2013a). This research sought to address this gap.

The aim of this study was therefore to contribute to the development and validation of an assessment method for the International Standard IEC 80001-1 *“Application of risk management for IT-networks incorporating medical devices”* (International Electrotechnical Commission (IEC) 2010).

The **research question** asked: How can a healthcare organisation assess their compliance with the requirements of the standard IEC 80001-1?

The achievement of the **research objectives** is outlined in section 6.3

The development of the assessment method was undertaken by the researcher in collaboration with the developer of the IEC 80001-1 PRM and PAM. The development followed the standard for process assessment IEC 15504 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). The assessment method developed included a set of criteria questions (and guidance) to assess against IEC 80001-1 (2010). To validate the question set an assessment was undertaken of a healthcare medical IT-network modification project to assess it's

suitability for use in context and to examine the risk management processes employed in terms of the compliance with the standard.

The assessment demonstrated that the assessment method was indeed appropriate and fit for purpose. The assessment highlighted strengths weaknesses opportunities and threats relating to the medical IT-network modification project. Lack of a medical IT-network risk manager and IT network risk management file were also reported. This meant that components of the role were assumed by different disciplines and documentation of risk activities was mainly informal.

The assessment findings and feedback from a questionnaire, was used to refine the criteria question set. This resulted in minor modifications to the questions and associated guidance (assessment tool) as outlined in section 5.6. Participants indicated they would use the assessment tool in future projects. The developed assessment method has been incorporated into the technical report ISO/IEC 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) due for publication shortly. The researcher's experience with using IEC 80001-1 (IEC 2010) informed the researcher review of this Technical Report (Committee Draft) which was submitted to ISO through the NSAI.

Recommendations to address weaknesses identified by the assessment were drawn up, and validated with assessment participants (section 5.8.2). Implementation of the recommendations to improve compliance with IEC 80001-1 (Appendix N Table 14) resulted in improvements in both the risk management processes and the documentation of same. The risk control measures identified were also implemented and monitoring indicated their effectiveness.

There was a low level of awareness of the standard IEC 80001-1 among participants and although the use of standards generally among participants was high, none reported having used IEC 80001-1 (IEC 2010). Provision of information regarding the standard IEC 80001-1 (IEC 2010) and participation in the assessment led to a raised awareness of the standard among risk management stakeholders. Participants indicated that they would use their increased awareness, knowledge and understanding in their future work. Participation in the assessment also led to improved transparency among risk management stakeholders with improved communication and collaboration which was also reported by (Ahlbrandt & Röhrig 2013b).

7.2 Conclusions

In conclusion, in order to perform an assessment against IEC 80001-1 an assessment method is required. Limited implementation of IEC 80001-1 (IEC 2010) has been attributed to the lack of an assessment method to assess compliance with the standard requirements. This study has addressed this gap by contributing to the development and validation of an assessment method for IEC 80001-1 (IEC 2010). The assessment method developed and validated is indeed fit for purpose and is incorporated into the pending technical report ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) which will be published shortly. Healthcare organisations can assess their conformance with the requirements of IEC 80001-1 (IEC 2010) using the guidance and assessment method contained in ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014). An assessment will identify areas for improvement in relation to the risk management of medical IT-networks (outlined in IEC 80001-1) which if actioned will ensure effective risk management of the medical IT-network.

Participation in the review of the draft Technical Report by the researcher provided an insight into standards development work and contributed experiences of frontline application of IEC 80001-1 (IEC 2010) to the process. The possibility of future Masters research studies participating in standards development work is perhaps something the standards development community could capitalise on.

Use of the assessment method in the context of a medical IT-network modification project in a healthcare organisation highlighted areas for improvement in relation to roles, responsibilities and activities regarding the application of risk management for medical IT-networks. Addressing these areas for improvement reduced the risks to the key properties of the network: safety, effectiveness and data and system security. The assessment method resulted in improved collaboration and transparency among risk management stakeholders. Implementation of the standard IEC 80001-1 (IEC 2010) facilitated by ISO/IEC TR 80001-2-7 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2014) will ensure the key properties of the network are not adversely affected by the incorporation of medical devices and lead to reduced risks to patient safety from networked devices.

References

- AAMI-FDA, 2012. Medical Device Interoperability - A Safer Path Forward. Priority Issues from the 2012 AAMI-FDA Interoperability Summit.
- Academy of Medical Laboratory Science, Association of Clinical Biochemists in Ireland, Irish Medicines Board, Royal College of Physicians in Ireland Faculty of Pathology, 2007. Guidelines for Safe and Effective Management of Point of Care Testing.
- Adekola, O.. et al., 2012. The incidence of electrolyte and acid-base abnormalities in critically ill patients using point of care testing (i-STAT portable analyser). *Nigerian Quality Journal of Hospital Medicine*, 22(2), pp.103–108.
- Ahlbrandt, J. & Röhrig, R., 2013a. Safety first! Managing risks for a daisy chain of medical devices connected to the IT-network – first experiences applying IEC 80001-1. In *14th World Congress on Medical and Health Informatics*. Medinfo 2013. Copenhagen, Denmark: IOS Press, pp. 982 – 982. Available at: <http://ebooks.iospress.nl/volumearticle/34198> [Accessed May 3, 2014].
- Ahlbrandt, J. & Röhrig, R., 2013b. Safety first! Managing risks for a daisy chain of medical devices connected to the IT-network - First experiences applying IEC 80001-1. *Studies in Health Technology and Informatics*, 192, p.982.
- American National Standards Institute (ANSI), Association for the Advancement of Medical Instrumentation (AAMI) & International Electrotechnical Commission (IEC), 2006. ANSI/AAMI / IEC 62304 Medical Device software - software life cycle processes. Available at: <http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FAAMI%2FIEC+62304%3A2006> [Accessed February 6, 2014].
- Association for the Advancement of Medical Instrumentation (AAMI), American College of Clinical Engineering (ACCE) & Healthcare Information and Management Systems Society (HIMSS), 2014. CE - IT Community: A Clinical Engineering/IT Collaboration. *CE - IT Community: A Clinical Engineering/IT Collaboration*. Available at: <http://www.ceitcollaboration.org/>.
- Beauchamp, T.L. & Childress, J.F., 2009. *Principles of Biomedical Ethics* 6th ed., New York.: Oxford University Press.
- Berry, T., 2013. How to Perform a SWOT Analysis? Available at: <http://articles.bplans.com/business/how-to-perform-swot-analysis/116> [Accessed December 24, 2013].
- Boehm, B.W., 1991. Software risk management - Principles and practices. *IEEE Software*, 8(1), pp.32 – 41.
- Bowling, A., 2009. *Research Methods in Health: Investigating Health and Health Services*. 3rd ed., Berkshire, England: Open University Press.
- British Standards Institution (BSI), 2000. BS EN ISO 9000 Quality Management Systems - Fundamentals & Vocabulary. BSI.

- Burns, N. & Grove, S.K., 2005. *The Practice of Nursing Research: Conduct, Critique and Utilization*. 5th ed., Missouri USA: Elsevier Saunders.
- Cahalane, D., 2013. Software as a Medical Device. In European Union, United States of America Bilateral Conference. RCSI Dublin Ireland.
- Clinical Pathology Accreditation (CPA) UK Ltd, 2010. Standards for Point-of-Care Testing (POCT) Facilities. PD-LAB-POCT Additional Standards v1.00. CPA.
- CLSI, 2008. *CLSI POCT2 A Implementation Guide Of Poct01 For Health Care Providers*. 1st ed., Clinical Laboratory Standards Institute (CLSI). Available at: <http://infostore.saiglobal.com/EMEA/Details.aspx?ProductID=1072948>.
- CLSI, 2010. Selection Criteria for Point of Care Devices; Approved Guideline (POCT09-A). Available at: https://s3.amazonaws.com/2013catalog/2013_Interactive_Catalog_Final_WebVersion.pdf [Accessed February 2, 2014].
- Collins, A., Joseph, D. & Bielaczyc, K., 2004. Design research: Theoretical and methodological issues. *The Journal of the Learning Sciences*, 13(1), pp.15–42.
- Collins, K.M.T., Onwuegbuzie, A.J. & Sutton, I.L., 2006. A model incorporating the rationale and purpose for conducting mixed methods research in special education and beyond. *Learning Disabilities; A Contemporary Journal*, 4, pp.67 – 100.
- Cook, T.M. et al., 2011. Major complications of airway management in the UK: results of the Fourth National Audit Project of the Royal College of Anaesthetists and the Difficult Airway Society. Part 2: intensive care and emergency departments. *British Journal of Anaesthesia*, 106(5), pp.632–642.
- Cooper, T. & Eagles, S., 2011. 80001: New era dawns for medical devices. *Biomedical Instrumentation & Technology*, 45(1), pp.16 – 25.
- Cooper, T. & Eagles, S., 2010. Update on IEC 80001-1 - Aiming for patient safety in the networked healthcare environment. *Information Technology Horizons*, pp.18–20.
- Cooper, T., Yadin, D. & Eagles, S., 2011. Getting started with IEC 80001. Essential Information for Healthcare Providers Managing Medical IT Networks. Association for the Advancement of Medical Instrumentation (AAMI).
- Cormack, D.F.S. ed., 2000. *The Research Process in Nursing*. 4th ed., Oxford: Blackwell Science.
- Department of Health & Children (DOHc), 2008. *Building a Culture of Patient Safety. Report of the Commission on Patient Safety & Quality Assurance.*, Dublin Stationery Office: Department of Health & Children (DOHc).
- DePoy, E. & Gitlin, L.N., 2011. *Introduction to Research: Understanding and Applying Multiple Strategies*. 4th ed., St Louis Missouri USA: Elsevier Mosby.
- Dillman, D., 2000. *Mail and Internet Surveys*. 2nd ed., USA: John Wiley & Sons.
- Eagles, S., 2008. An Introduction to IEC/CD2 80001: Aiming for patient safety in the networked healthcare environment. *Information Technology Horizons*, pp.15 – 19.

- ECRI Institute, 2013. ECRI Health Devices: Top 10 Health Technology Hazards for 2014 Executive Brief. ECRI Institute. Available at: www.ecri.org/2014hazards [Accessed April 5, 2014].
- ECRI Institute, 2012. ECRI Health Devices: Top 10 Health Technology Hazards for 2013. ECRI Institute. Available at: www.ecri.org/2013hazards [Accessed November 10, 2012].
- Edwards, S.D., 2001. *Philosophy of nursing.*, Hampshire: Palgrave.
- Ellis, M., 2011. IT Technology Industry Perspective. In *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT Networks*. Virginia: Association for the Advancement of Medical Instrumentation, p. 5.
- European Parliament & the Council of the European Union, 1993. 93/42/EEC : Medical Device Directive. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF>.
- European Parliament & the Council of the European Union, 2007. Directive 2007/47/EC of the European Parliament and of the Council. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:en:PDF> [Accessed November 9, 2013].
- Farrance, I., 2012. Review, Policies, Procedures, Guidelines for Point of Care Testing. RCPA Quality Assurance Program.
- Fernández-Alemán, J.L. et al., 2013. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S1532046412001864> [Accessed April 19, 2013].
- Finnegan, A., Mc Caffery, F. & Coleman, G., 2013. Framework to Assist Healthcare Delivery Organisations and Medical Device Manufacturers Establish Security Assurance for Networked Medical Devices. In *Systems, Software and Services Process Improvement: 20th European Conference, EuroSPI 2013, Dundalk, Ireland*. Communication in Computer and Information Science. Dundalk, Ireland: Springer Berlin Heidelberg, pp. 313 – 322.
- Goddard, P.L., 2000. Software FMEA Techniques. In *Annual Reliability and Maintainability Symposium*. Annual Reliability and Maintainability Symposium. Los Angeles, CA, pp. 118 – 123.
- Government of Ireland, 2003. *Data Protection Act 1988 & 2003*, Available at: <http://www.dataprotection.ie/viewdoc.asp?DocID=796> [Accessed October 22, 2012].
- Griffiths, F., 2009. *Research Methods for Healthcare Practice.*, Los Angeles, London, New Delhi, Singapore, Washington DC.: SAGE Publications Ltd.
- Grimes, S.L., 2006. CHIME Convergence of Clinical Engineering and Information Technology. Available at: <http://www.accenet.org/downloads/chime.pdf> [Accessed January 20, 2014].
- Halley, E.C., Sensmeier, J. & Brokel, J.M., 2009. Nurses exchanging information: understanding electronic health record standards and interoperability. *Urologic Nursing*, 29(5), p.305.

- Hammersley, M., 1996. The Relationship between Qualitative and Quantitative Research: Paradigm loyalty versus methodological eclecticism. In J. T. E. Richardson, ed. *Handbook of Research Methods for Psychology and Social Sciences*. Leicester: BPS Books, pp. 159 – 74.
- Hayrinen, K., Saranto, K. & Nykanen, P., 2008. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 77(5), pp.291–304.
- Health Information & Quality Authority (HIQA), 2011. Developing national eHealth interoperability standards for Ireland: a consultation document. HIQA. Available at: <http://hiqa.ie/system/files/eHealth-Interoperability-Consultation.pdf> [Accessed April 24, 2013].
- Health Information & Quality Authority (HIQA), 2010. General Practice Messaging Standard. HIQA.
- Health Information & Quality Authority (HIQA), 2012a. Guidance on Messaging Standards for Ireland. HIQA. Available at: <http://www.hiqa.ie/system/files/Guidance-on-Messaging-Standards.pdf> [Accessed February 5, 2014].
- Health Information & Quality Authority (HIQA), 2013. Health Information and Quality Authority (HIQA). Available at: <http://www.hiqa.ie/about-us/what-we-do-and-why> [Accessed November 19, 2013].
- Health Information & Quality Authority (HIQA), 2012b. National Standards for Safer Better Healthcare. HIQA. Available at: <http://www.hiqa.ie/standards/healthcare> [Accessed February 5, 2014].
- Health Information & Quality Authority (HIQA), 2012c. Safer-Better-Healthcare-Standards HIQA.pdf. Available at: <http://www.hiqa.ie/standards/healthcare> [Accessed February 5, 2014].
- Health Service Executive (HSE) et al., 2009. Guidelines for Safe and Effective Management and Use of Point of Care Testing in Primary & Community Care. HSE, PSI, AMLS, ACBI, IMB, RCPI.
- Hegarty, F.J. et al., 2014. Assessing a hospital's IT network risk management practice with IEC 80001-1. *Biomedical Instrumentation & Technology*, 48(1), pp.64–71.
- Hevner, A.R. et al., 2004. Design science in information systems research. *MIS quarterly*, 28(1), pp.75–105.
- Holloway, I. & Wheeler, S., 1996. *Qualitative Research for Nurses.*, Oxford: Blackwell Science.
- IEC, 2014. International Electrotechnical Commission (IEC). International Standards and Conformity Assessment for all electrical, electronic and related technologies. *International Electrotechnical Commission (IEC)*. Available at: <http://www.iec.ch/> [Accessed January 19, 2014].
- IMB, 2009. Guide to the Classification of a Medical Device v2 IMB. Available at: <http://www.imb.ie/EN/Publications/Publications.aspx?q=Guide%20to%20the%20classification%20of%20a%20medical%20device> [Accessed November 9, 2013].
- IMB, 2014. Irish Medicines Board (IMB). Available at: <http://www.imb.ie/>.

- IMDRF SaMD Working Group N12, 2014. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Controls (Proposed Document). IMDRF SaMD Working Group N12.
- Institute of Medicine, 2000. *To Err is human. Building a Safer Health System.*, Washington D.C.: National Academies Press. Available at: http://www.nap.edu/openbook.php?record_id=9728 [Accessed February 27, 2014].
- International Electrotechnical Commission (IEC), 2012a. IEC 60601-1 Medical Electrical Equipment - Part 1: General requirements for basic safety and essential performance. Edition 3.1.
- International Electrotechnical Commission (IEC), 2005. IEC 60601-1 Medical Electrical Equipment Part 1 General Requirements for Basic Safety and Effective Performance. IEC.
- International Electrotechnical Commission (IEC), 2010. IEC 80001-1 Application of Risk Management for It-Networks incorporating Medical Devices- Part 1: Roles, Responsibilities and Activities. IEC.
- International Electrotechnical Commission (IEC), 2012b. IEC TR 80001-2-1 Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples.
- International Electrotechnical Commission (IEC), 2012c. IEC/TR 80001-2-2: "Application of risk management for IT Networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls" IEC.
- International Electrotechnical Commission (IEC), 2012d. IEC/TR 80001-2-3:"Application of risk management for IT networks incorporating medical devices – Part 2-3: Guidance for wireless networks" IEC.
- International Electrotechnical Commission (IEC), 2012e. IEC/TR 80001-2-4: Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations. IEC. Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62323&ics1=35&ics2=240&ics3=80 [Accessed February 7, 2014].
- International Electrotechnical Commission (IEC), 2014a. International ElectroTechnical Commission (IEC) International Standards. *International Electrotechnical Commission (IEC) International Standards*. Available at: <http://www.iec.ch/standardsdev/publications/is.htm> [Accessed February 5, 2014].
- International Electrotechnical Commission (IEC), 2014b. International Electrotechnical Commission (IEC). Available at: <http://www.iec.ch/standardsdev/publications/is.htm> [Accessed February 5, 2014].
- International Organisation for Standardisation (ISO), 2003. ISO 13485 Medical Devices - Quality Management Systems - Requirements for Regulatory purposes.
- International Organization for Standardization (ISO), 2014a. International Organization for Standardisation (ISO). Available at: <http://www.iso.org/iso/home.html> [Accessed February 4, 2014].

- International Organization for Standardization (ISO), 2013. International Organization for Standardization (ISO). Available at: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=54960.
- International Organization for Standardization (ISO), 2003. ISO 13485 Medical devices — Quality management systems — Requirements for regulatory purposes. ISO.
- International Organization for Standardization (ISO), 2007a. ISO 14971 Medical Devices - Application of Risk Management to Medical Devices. ISO.
- International Organization for Standardization (ISO), 2012. ISO 15189: Medical laboratories -- Requirements for quality and competence. ISO. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=56115 [Accessed February 7, 2014].
- International Organization for Standardization (ISO), 2006. ISO 22870 Point-of-care testing (POCT) - Requirements for Quality and Competence. ISO. Available at: <http://www.iso.org/iso/home.html> [Accessed February 2, 2014].
- International Organization for Standardization (ISO), 2008. ISO 27799 Health Informatics Information Security Management in Health using ISO/IEC 27002. ISO.
- International Organization for Standardization (ISO), 2007b. ISO TS 25238 Health Informatics – Classification of Safety Risks from Health Software. ISO.
- International Organization for Standardization (ISO), 2014b. ISO/PRF TR 80001-2-6 Application of risk management for IT-networks incorporating medical devices - Part 2-6: Application guidance - Guidance for responsibility agreements. (under development). ISO. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63108.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2008. ISO/IEC 15408 - 2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2009. ISO/IEC 15408 -1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2004. ISO/IEC 15504-1 Information technology - Process assessment - Part 1: Concepts and vocabulary. Available at: <http://eu.i2.saiglobal.com/management/click2view/index/1/10/9423/681769/117120/0/-/ae08f43e2e9a056d23d06f7c07a3e1f3> [Accessed June 18, 2014].
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2003. ISO/IEC 15504-2: Software Engineering - Process Assessment Part 2; Performing an Assessment. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2005a. ISO/IEC 20000 -1 Information Technology - Service Management - Part 1 Specification. ISO/IEC.

- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2005b. ISO/IEC 20000 -2 Information Technology - Service Management - Part 1 Code of Practice. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2013. ISO/IEC 27002 Information technology Security techniques Code of practice for information security controls. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2007. ISO/IEC TR 24774 "Software and systems engineering – Life cycle management – Guidelines for process description. ISO/IEC.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), 2014. ISO/IEC TR 80001-2-7: 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 (Committee Draft) ISO/IEC.
- International Standardisation Organisation (ISO), 2005. ISO 9000 Quality Management Systems - Fundamentals and Vocabulary. Available at: http://www.iso.org/iso/iso_9000.
- IT Infrastructure Library (ITIL), 2014. IT Infrastructure Library (ITIL). Available at: <http://www.itil-officialsite.com/Publications/Publications.aspx> [Accessed January 20, 2014].
- Kaukonen, K.-M. et al., 2014. Mortality related to severe sepsis and septic shock among critically ill patients in Australia and New Zealand, 2000-2012. *The Journal of the American Medical Association (JAMA)*, 311(13), p.1308.
- Keyson, D.V.V. & Bruns Alonso, M., 2009. Empirical research through design. In *Proceedings of the 3rd IASDR Conference on Design Research*. International Congress of International Association of Societies of Design Research (IASDR) : Design / Rigor & Relevance. Seoul, Korea, pp. 4548–4557. Available at: <http://gsct3237.kaist.ac.kr/e-lib/Conferences/IASDR/2009/Papers/Special%20Session/Assessing%20knowledge%20generated%20by%20research%20through%20design/Empirical%20Research%20Through%20Design.pdf> [Accessed March 9, 2014].
- Kiekkas, P. et al., 2008. Association between nursing workload and mortality of intensive care unit patients. *Journal of Nursing Scholarship*, 40(4), pp.385–390.
- Kim, J.Y. & Lewandroski, K., 2009. Point-of-Care Testing Informatics. *Clinics in Laboratory Medicine*, 29(3), pp.449–461.
- De Koninck, A.-S. et al., 2012. Analytical performance evaluation of four cartridge-type blood gas analyzers. *Clinical Chemistry and Laboratory Medicine*, 50(6). Available at: <http://www.degruyter.com/view/j/cclm.2012.50.issue-6/cclm-2011-0685/cclm-2011-0685.xml> [Accessed March 4, 2013].
- Kost, G.J., 2001. Preventing medical errors in point-of-care testing: security, validation, performance, safeguards, and connectivity. *Archives of Pathology & Laboratory Medicine*, 125(10), pp.1307–1315.

- Leino, A. & Kurvinen, K., 2011. Interchangeability of blood gas, electrolyte and metabolite results measured with point-of-care, blood gas and core laboratory analyzers. *Clinical Chemistry and Laboratory Medicine*, 49(7). Available at: <http://www.degruyter.com/view/j/cclm.2011.49.issue-7/cclm.2011.185/cclm.2011.185.xml> [Accessed March 4, 2013].
- Lee-Lewandrowski, E. et al., 2003. Implementation of a point-of-care satellite laboratory in the emergency department of an academic medical center: impact on test turnaround time and patient emergency department length of stay. *Archives of Pathology & Laboratory Medicine*, 127(4), pp.456–460.
- Lee-Lewandrowski, E. & Lewandrowski, K., 2009. Perspectives on cost and outcomes for point-of-care testing. *Clinical Laboratory Medicine*, 29(3), pp.479–489.
- Lewandrowski, K., 2009. Point-of-Care testing: An Overview and a Look to the Future (Circa 2009 United States). *Clinics in Laboratory Medicine*, 29(3), pp.421–432.
- Lewandrowski, K., Gregory, K. & Macmillan, D., 2011. Assuring quality in point-of-care testing: evolution of technologies, informatics, and program management. *Archives of Pathology & Laboratory Medicine*, 135(11), pp.1405–1414.
- Liamputtong, P., 2013. *Research Methods in Health: Foundations for evidence-based practice*. 2nd ed., Australia & New Zealand: Oxford University Press.
- Mac Mahon, S.T., Mc Caffery, F. & Keenan, F., 2013. Towards a Process Assessment Model for IEC 80001-1. In *6th International Conference on Health Informatics (HealthInfo) 2013*. Health Informatics 2013. Barcelona Spain.
- MacMahon, S. et al., 2012. Development of a Process Assessment Model for Assessing Medical IT Networks against IEC 80001-1. In *Software Process Improvement and Capability Determination*. Springer, pp. 148–160. Available at: http://link.springer.com/chapter/10.1007/978-3-642-30439-2_14 [Accessed November 9, 2013].
- MacMahon, S., Mc Caffery, F. & Keenan, F., 2013a. Risk management of medical IT networks: an ISO/IEC 15504 compliant approach to assessment against IEC 80001-1. In *Proceedings of the 2013 International Conference on Software and System Process*. International Conference on Software and System Process (ICSSP). San Francisco, US: Association for Computing Machinery (ACM), pp. 156–160. Available at: <http://dl.acm.org/citation.cfm?id=2486074> [Accessed October 30, 2013].
- MacMahon, S., Mc Caffery, F. & Keenan, F., 2013b. The Approach to the Development of an Assessment Method for IEC 80001-1. In *Software Process Improvement and Capability Determination*. Springer, pp. 37–48. Available at: http://link.springer.com/chapter/10.1007/978-3-642-38833-0_4 [Accessed November 9, 2013].
- MacMahon, S., Mc Caffery, F. & Keenan, F., 2013c. Transforming Requirements of IEC 80001-1 into an ISO/ IEC 15504-2 Compliant Process Reference Model and Process Assessment Model. In EuroSPI. Dundalk, Co. Louth, Ireland.: EuroSPICE.

- Magrabi, F. et al., 2013. A comparative review of patient safety initiatives for national health information technology. *International Journal of Medical Informatics*, 82(5), pp.e139–e148.
- Malloch, K., 2007. The electronic health record: An essential tool for advancing patient safety. *Nursing Outlook*, 55(3), pp.159 – 161.
- Marx, D.A. & Slonim, A.D., 2003. Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. *Quality and Safety in Health Care*, 12(suppl 2), pp.ii33–ii38.
- Mc Cullough, C., 2012. MedSun Reporting by Biomedical and Clinical Engineers - Safety Stories and Successes. MedSun Webinar.
- Mc Daniel, G., 2010. Point-of-care testing guideline published by CLSI. *Laboratory Medicine*, 41(8), pp.499–500.
- Meier, F.A. & Jones, B.A., 2005. Point-of-care testing error: sources and amplifiers, taxonomy, prevention strategies, and detection monitors. *Archives of Pathology and Laboratory Medicine*, 129(10), pp.1262–1267.
- Morgan, D.L., 1996. Focus groups. *Annual review of sociology*, pp.129–152.
- Morrissey, J., 2011. Health Information Exchange (HIE). *Hospitals & Health Networks Magazine*, (February 2011), pp.22 – 27.
- National Standards Authority of Ireland (NSAI), 2014. National Standards Authority of Ireland (NSAI). Available at: <http://www.nsai.ie/> [Accessed February 4, 2014].
- National Standards Authority of Ireland (NSAI), 2013. National Standards Authority of Ireland. Available at: <http://www.nsai.ie/About-NSAI.aspx> [Accessed November 19, 2013].
- Parahoo, K., 2001. *Nursing Research, Principles, Process and Issues.*, London UK: Macmillan.
- Pascal, A., Thomas, C. & Romme, A.G.L., 2013. Developing a human-centred and science-based approach to design: The knowledge management platform project. *British Journal of Management*, 24(2), pp.264–280.
- Polgar, S. & Thomas, S.A., 2008. *Introduction to Research in the Health Sciences*. 5th ed., Philadelphia USA: Churchill Livingstone Elsevier.
- Polit, D.F., Beck, C.T. & Hungler, B.P., 2001. *Essentials of Nursing Research: Methods, Appraisal and Utilization*. 5th ed., Philadelphia, USA: Lippincott Williams and Wilkins.
- Rakitin, S.R., 2006. Coping with defective software in medical devices. *Computer*, 39(4), pp.40–45.
- Rakitin, S.R., 2009. Networked medical devices: Essential collaboration for improved safety. *Biomedical Instrumentation & Technology*, 43(4), pp.332 – 338.
- Sadhu, A.R. et al., 2008. Economic benefits of intensive insulin therapy in critically ill patients: The targeted insulin therapy to improve hospital outcomes (TRIUMPH) project. *Diabetes Care*, 31(8), pp.1556–1561.

- Scalise, D., 2006. Poised for growth: Point of care testing. *Hospital and Health Networks*, 80(9), pp.77–83.
- Sidebottom, C., 2011. Medical Device Manufacturer Perspective. In *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT Networks*. Virginia: Association for the Advancement of Medical Instrumentation, p. 4.
- The European Parliament & the Council of the European Union, 1993. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L169, 12.7.1993). Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF> [Accessed November 9, 2013].
- The European Parliament & the Council of the European Union, 1990. Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1990L0385:20071011:en:PDF> [Accessed February 5, 2014].
- The European Parliament & the Council of the European Union, 1998. Directive 98/79/EC of the European Parliament and of the Council on in vitro diagnostic medical devices. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:331:0001:0037:EN:PDF> [Accessed February 5, 2014].
- The Irish Critical Care Trials Group, 2008. Intensive care for the adult population in Ireland: a multicentre study of intensive care population demographics. *Critical Care*, 12(5), p.R121.
- The Joint Commission, 2008. Safely Implementing Health Information and Converging Technologies. *Sentinel Event Alert*, (42).
- The Joint Commission on Accreditation of Healthcare Organizations, 2000. Medical Errors, Sentinel Events and accreditation. A report to the Association of Anaesthesia Program Directors. JCAHO.
- The National Committee for Clinical Laboratory Standards (NCCLS)NCCLS, 2001. Point-of-Care Connectivity; Approved Standard. POCT1-A.
- Thede, L.Q. & Sewell, J.P., 2009. *Informatics and Nursing: Competencies and applications*. 3rd ed., New York: Wolters Kluwer.
- Tuffley, D., 2012. Modelling organisational behavior with process reference models. *International Journal of Software Engineering*, 2(2), pp.14–20.
- Tuffley, D. & Rout, T.P., 2009. Applying Behavior Engineering to Process Modeling. In *ISSEC: Improving Systems and Software Engineering Conference 2009*. Available at: <http://www98.griffith.edu.au/dspace/handle/10072/31748> [Accessed November 8, 2013].
- U.S. Department of Health & Human Services (DHHS) Office of the National Coordinator for Health Information Technology, 2008. The national alliance for health information technology report to the Office of the National Co-ordinator for Health Information Technology on defining key health information technology terms. Available at: http://www.nahit.org/images/pdfs/HITTermsFinal_Report_051508.pdf [Accessed March 22, 2013].

- U.S. DHHS FDA, 2002. General Principles of Software Validation; Final Guidance for Industry and FDA Staff. US DHHS FDA.
- Urwyler, N. et al., 2009. Is perioperative point-of-care prothrombin time testing accurate compared to the standard laboratory test? *Thrombosis and Haemostasis*, 4(102), pp.779–786.
- US FDA, 2005. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing off-the-shelf (OTS) Software. US DHHS FDA. Available at: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf> [Accessed January 25, 2014].
- Wagar, E.A., Yasin, B. & Yuan, S., 2008. Point-of-Care Testing: Twenty Years' Experience. *Laboratory Medicine*, 39(9), pp.560–563.
- Ward, L. et al., 2012. Data entry errors and design for model-based tight glycemic control in critical care. *Journal of Diabetes Science and Technology*, 6(1), pp.135–143.
- West Health Institute, 2013. The Value of Medical Device Interoperability: Improving patient care with more than \$30billion in annual healthcare savings. West Health Institute.

Appendices

Appendix A ISO Standard Development Process

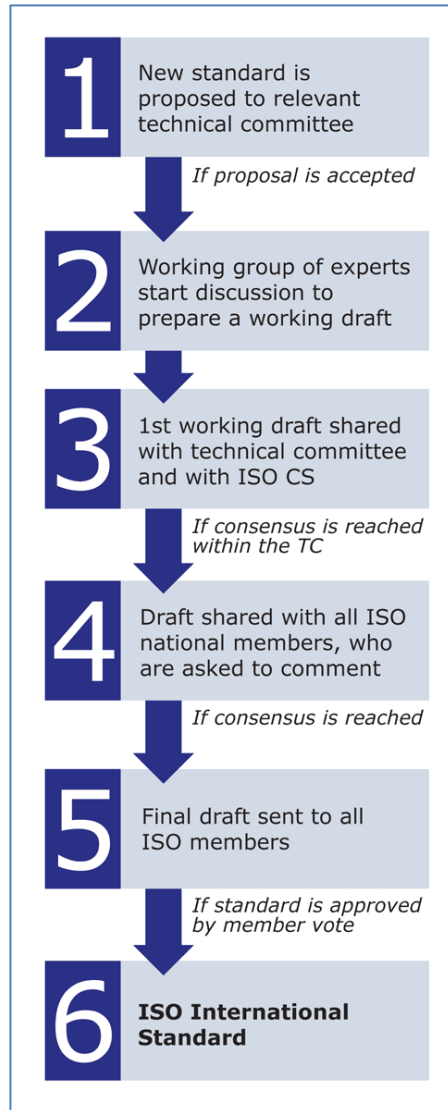


Figure 18 ISO Standard Development Process

Available from: http://www.iso.org/iso/home/standards_development.htm

[Accessed 5 February 2014]

Appendix B Sample Process from IEC 80001-1 PAM

Name:	Go-Live
Context:	This process allows the responsible organisation to manage the Go-Live Phase of the project and to consider the decision to go live in terms of the residual risk.
Purpose:	The purpose of the Go-Live Process is to allow the responsible organisation to manage the transition of the IT network to the live environment and to allow the responsible organisation to manage the risk management activities associated with the Go-Live phase of the project.
Outcomes:	As a result of the successful implementation of Go-Live Process : 1. Medical IT-network residual risk is reviewed prior to going live. 2. Residual risk summaries are reviewed for acceptability of risks associated with interactions of recent or pending projects or changes. 3. The specified change to the medical IT-network is approved prior to go-live by the medical IT-network risk manager. 4. The approval of the medical-IT network residual risk is documented in the medical IT-network risk management file.
Base Practices	CRCM.3.BP1: Review residual risk. Review Medical IT Network residual risk summaries for acceptability of risk associated with interactions of recent or pending projects or changes, prior to going live. [Outcome: 1, 2].
	CRCM.3.BP2: Approve specified change. Approval is given for the specified change by the medical IT Network Risk Manager prior to go-live. [Outcome: 3].
	CRCM.3.BP3: Document approval of residual risk. Document the approval of the medical IT Network residual risk in the Medical IT network risk management file. [Outcome: 4].
Inputs:	
	13-03 Risk Benefit Analysis Record [CRCM.3, BP1, 2] [Expected Result 1, 2, 3]
Outputs:	
	08-02 Change Request Approval Record [CRCM.3, BP.2, 3] [Expected Result 3, 4]
	16-02 Medical IT network Risk Management File [CRCM.3, BP.3] [Expected Result 4]

Table 13 Sample Process from IEC 80001 PAM

(MacMahon et al. 2013c)

Appendix C Methodology Overview – Detailed Description of Steps to be undertaken

Step 1: Perform Literature Review

The literature review performed to inform the methodology is outlined in chapter 2 and chapter 3 section 3.2.

Step 2: Develop question set & guidance – based on the base practices for processes in the IEC 80001-1 Process Assessment Model

In order to perform an assessment against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) a process reference model (PRM) and process assessment model (PAM) and an assessment method are required as outlined in chapter 2 Section 2.11.6.

The second step in this study methodology will be the development of the assessment method (comprising of a question set and guidance document) based on the base practices for all risk management processes in the validated IEC 80001-1 PAM and PRM developed by MacMahon *et al.* (2013b). This step is linked to the concept of design research with the creation of an innovative artefact as explained in section 3.2.2. This step will follow the standards for development of an assessment method based on International standards outlined by MacMahon *et al.* (2013b) and comply with the process outlined in the process assessment standard ISO/IEC 15504-2 (International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) 2003). The base practices are the risk management activities undertaken to achieve the purpose and outcomes of each of the risk management processes. A question development workshop will be undertaken at which these base practices will be jointly examined (by this researcher and the developer of the PAM) and converted into question format. Guidance from the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) will also be included to clarify the questions and facilitate discussions during an assessment. Once all the questions have been developed, these will be reviewed both individually and jointly focusing on usability in context, and guidance in the standard IEC 80001-1 and other related technical reports. Using the validated Process Assessment Model (PAM) and Process Reference Model (PRM) for the development of the assessment questions will ensure content validity of the assessment questions in terms of the IEC 80001-1 standard (International Electrotechnical Commission (IEC) 2010). The output from this step will achieve research objective 1 and will be used in Step 4.

Step 3: Identify the Medical IT Network Modification Project to be the focus of the assessment

A medical IT-network modification project in a healthcare organisation for which the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) is applicable will be identified. IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) takes a life cycle approach to risk management of the medical IT-network and therefore is applicable on inception of the medical IT-network, addition of medical device(s) on an IT network, when medical devices already on a medical IT-network are changed/modified or undergo maintenance, when medical devices are removed from an IT-network and when the network is decommissioned (International Electrotechnical Commission (IEC) 2010). The identified medical IT-network modification project will be the focus of the assessment in order to use the assessment method in context, a requirement of design research and validation of contextual use. This is also linked to the research approach of *Pragmatism* in that the culture, language and context of the healthcare organisation is an important aspect of this study. Members of the IT network modification project team using purposive sampling will be invited to participate in the study as outlined in the sampling strategy in section 3.3. In this way experience of using the assessment method will provide participants with the knowledge to provide feedback on its' suitability as a means of assessment against IEC 80001-1 (International Electrotechnical Commission (IEC) 2010).

Step 4: Identify the subset of questions & associated guidance appropriate to the identified network modification project

The next step is to prepare the assessment document to be used in the assessment of the medical IT-network modification project in a healthcare organisation. As this will be the first assessment against IEC 80001-1 (IEC 2010) in the healthcare organisation, it would be unreasonable to expect the IT-network modification project selected for assessment to be compliant with all 84 base practice questions. Therefore a subset of the questions will be derived by examining each process and selecting questions based on key base practices within each process, ensuring a minimum of one question from each process is included. Refinement of the question set following design research methodology will ensure it can be used in a live environment context. The assessment questions document which will include: the names of each risk management process, questions for each process and response type, will be included in the information pack distributed to participants in advance of the assessment (Appendix D.5). The questions will include both closed response types (yes/no) and open (dialogue) responses to generate discussion. The researcher copy of the assessment document will also include guidance for each question to clarify requirements of the base practice (Appendix X).

Step 5: Validate subset of questions & ensure all processes are represented

The subset of questions will be reviewed to ensure each risk management process is represented.

Step 6: Develop the Questionnaire

The questionnaire to be used in the study will be developed and reviewed by an expert panel as outlined in section 3.4.1.2.

3.7.7 Step 7: Provide an overview of the Standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) & Process Assessment

Information regarding the standard will be included in the participant information sheet issued to participants prior to commencement of data collection (Appendix D.1). Also, personnel involved in the medical IT network modification project will be provided with an overview of the Standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) and process assessment in the pre-assessment PowerPoint presentation (Appendix X). Performance of step 7 will achieve research objective 6.

Step 8: Perform the assessment using the subset of questions

The next step will be the performance of the assessment to achieve research objective 2. The purpose of the assessment is the validation of an assessment method (question set) which has been developed to assess the risk management processes related to a medical IT-network modification project referred to in the standard IEC 80001-1 (IEC 2010). This validation takes into account the context of use in an actual medical IT-network modification project in a healthcare organisation as described in design research. Indeed, Hevner *et al.*, (2004) advocate that any evaluation must include an in-depth study of the artefact in a real organisation environment. It is anticipated that the assessment will identify the risk management processes employed for the IT-network modification project and assess them against the requirements of the standard IEC 80001-1. In this way strengths, weaknesses, opportunities and threats related to the risk management of the medical IT-Network modification project will be identified.

As the risk management process is a collaborative process between Information Technology (IT), Clinical Engineering (CE) clinical informatics staff and clinical users (with input from the manufacturer of the medical devices) it is appropriate to undertake the assessment using a focus group semi structured interview. It is expected that the focus group will provide a rich source of insight and interpretation from participants (Polgar and Thomas, 2008). Additionally, because the standard IEC 80001-1 (International Electrotechnical Commission (IEC) 2010) advocates greater collaboration among risk management stakeholders, it is anticipated that joint participation in the assessment will encourage this collaboration process. Indeed, (Tuffley 2012), also used a focus group

methodology for a review cycle of Process Reference Model development. A focus group interview schedule along with the assessment document (assessment questions) will be used for the assessment (Appendix D.5). Participants in the assessment will include personnel involved in the IT network modification project and the organisation's risk manager. The assessment will be audio recorded and the researcher and a research assistant will take notes.

Step 9: Post Assessment Questionnaire Distribution/Completion

Following the assessment, participants will be asked to provide feedback on the assessment by completing the post assessment questionnaire (Appendix D.4). This feedback will be used to achieve research objective 5 refinement of the criteria question set. This 2nd data collection method (a component of this study's mixed methodology) will generate quantitative and qualitative data.

Step 10: Assessment Data Analysis

The assessment data recordings will be replayed numerous times and will be transcribed verbatim. This will facilitate both immersion in and engagement with the data and reflection on the meaning therein. Data will be coded and categorised to form common themes. A SWOT analysis of the assessment data identifying strengths, weaknesses, opportunities and threats will be undertaken. The literature will be consulted to ascertain how to undertake a SWOT analysis prior to undertaking same.

Step 11: Preparation of a Findings Report

The results of the SWOT analysis along with the recommendations identified will be presented to participants in a findings report (Appendix X) fulfilling research objective 3. The findings report will be used to draft the interview schedule and form the basis of the discussion during the individual interviews. The results of the SWOT analysis are outlined in chapter 5.

Step 12: Questionnaire Data Analysis

Quantitative data from the questionnaires will be inputted into excel and analysed using descriptive statistics. Qualitative data from the questionnaires will be analysed using thematic analysis.

Step 13: Refinement of the assessment question set (Research Objective 5)

The question set will be refined/ revised based on the results of the assessment analysis and the questionnaire analysis (section 5.6) using the iteration feedback loop of design research.

Step 14: Individual Interview Schedule Development

An interview schedule to guide the individual interviews will be developed (Appendix E).

Step 15: Individual Interviews Data Collection

Individual interviews will be undertaken with assessment participants to discuss the findings report, validate recommendations and identify which participant(s) will assume responsibility for implementing each recommendation. Interviews will be audio recorded. Data collected with this 3rd data collection method (mixed methodology) will include qualitative narrative (transcripts of recordings) and quantitative responses (Yes/No). Performance of this step will achieve research objective 4: to validate recommendations arising from the assessment of the IT modification project.

Step 16: Individual Interviews Analysis

Recordings from the individual interviews will be transcribed and analysed. Interview notes will be typed and reviewed. Quantitative data from the individual interviews will be inputted into excel and analysed for descriptive and inferential statistics. Qualitative data from the individual interviews will be analysed using codes and categories and emerging themes will be reflected on.

Step 17: Project Review Post Go-Live

A project review post Go-Live (of the IT-network modification) will be undertaken to identify any unforeseen consequences and incorporate feedback into the question set. The status of implementation of recommendations will also be reviewed. Implementation of recommendations will result in achievement of research objective 7: Improvement of risk management processes related to a medical IT-network modification project.

3.7.18 Step 18: Review of the findings in light of the published literature

The findings will be reviewed and discussed in light of published literature in Chapter 6.

Appendix D Information Pack for Participants

Appendix D.1 Participant Information Sheet

The Title of this Study is:

“Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)”.

Researcher: Lucy Kielty

Research Supervisor: Dr Damon Berry

Invitation to the Participants

You are invited to participate in a research study which is being completed in part fulfilment of an MSc in Health Informatics in Trinity College Dublin. Before you decide whether to take part or not please read the information provided below carefully. It is important that you understand the benefits and risks of taking part in this study so that you can decide if participation or otherwise is right for you, you do not have to take part in this study, you can change your mind about taking part even after the study has commenced and you do not have to give a reason for opting out.

Declaration of Conflict of Interest

Please note that as the researcher is a colleague of some participants there is a potential conflict of interest in relation to conducting this research study. However, it is my intention to adhere to the ethical code of good practice for research at all times. As a colleague whether you participate or not will not have any adverse consequences for our working relationship. I accept your right and decision to agree to participate (or not) voluntarily.

What is the Background Context of the Research & its Relevance?

There is increasing use of networked interoperable medical devices linked to electronic health records and clinical information systems. The incorporation of medical devices into the organisation’s IT network creates a Medical IT network and leads to new risks to quality and patient safety. The International Standard IEC 80001-1 (2010) identifies the key properties of medical IT networks as: safety, effectiveness, and data & system security. In order to safeguard these properties the risks must be managed. The standard recognises that devices are incorporated into IT networks to achieve the benefits of interoperability (increased effectiveness, reduced cost, improved productivity) and defines the roles/ responsibilities & activities for risk management of medical IT networks. The standard also advocates a life cycle approach to risk management of the network and identifies healthcare organisations as the organisations responsible for managing the risks associated with incorporating medical devices onto the network. Implementation of the standard has been slow, possibly due to the fact that currently there is no means for healthcare organisations to assess their risk management processes against IEC 80001-1 to determine strengths, weaknesses, opportunities, threats (MacMahon *et al.* 2013). This study seeks to develop and validate an assessment method (Question set) to assess risk management activities against IEC 80001-1 (2010). This study will contribute to research in progress by MacMahon *et al* which focuses on the development and validation of an Assessment Framework incorporating a Process Reference Model (PRM), Process Assessment Model (PAM) and assessment method which will inform one of the IEC 80001-1 technical reports supporting implementation of the standard by healthcare organisations.

What are the Aims of the Research Study?

The study aims are:

- To contribute to the standard IEC 80001-1 “Application of Risk Management for IT Networks Incorporating Medical Devices” (2010).
- To develop the assessment criteria to assess health service provider Medical IT network risk management activity against IEC 80001-1 (2010).
- To raise awareness of the standard among healthcare personnel.
- To improve risk management of IT networks incorporating medical devices.

Where is the study being carried out?

The study is being carried out in a large academic teaching hospital where you are employed. Two departments involved in IT network modification projects will be involved in the study (one of which is the critical care units).

Why have I been chosen / selected to take part?

You have been asked to participate as you have been identified as a risk management stakeholder in the Medical IT Network modification project related to the acquisition and integration of the new arterial blood gas analysers to the Medical IT Network incorporating the clinical information system in the critical care units. Alternatively, you have been asked to participate as you have been identified as a risk management stakeholder in another departmental Medical IT Network modification project.

Is Participation Voluntary?

Yes, participation is entirely voluntary; you may decline to participate at any stage. You have the right to withdraw at any time even after the study has commenced and for any reason without penalty. Individual questions on the questionnaire may be omitted if you so wish.

How will the study be conducted?

The study will be conducted in the form of an assessment of risk management processes related to the change to the Medical IT network (removal of 3 ABG analysers and addition of 8 new ABG analysers). The assessment focus will be the validation of a number of questions which have been developed to assess the risk management processes referred to in the standard. Following the assessment a findings report will be prepared which may include recommendations to address any weaknesses identified in the assessment.

What will happen if I agree to take part?

If you agree to participate you will be invited to attend an assessment in the form of a focus group /semi-structured interview, at the start of which the IEC 80001-1 standard and study will be explained. The interview will take place at a time and location that is suitable to all participants. It is likely to occur in the department involved in the IT modification project(s) (eg critical care unit). You will be asked to sign a consent form to indicate your willingness to participate prior to the commencement of the interview. The interview will take approximately 2 hours and an audio recording will be made. You will be asked to complete a questionnaire following the interview which can be returned via email to the researcher. You will be given an opportunity to review the recommendations in the findings report to agree whether the recommendations are valid and whether or not they could or would be implemented. You may be contacted by email if the need arises to verify direct quotations and their contextual appropriateness.

What is the duration of my involvement?

It is anticipated that the various data collection phases of the study will be completed within a two month period (Dec/Jan).

Are there any Risks?

Participation in this study is entirely voluntary; you are free to withdraw at any stage without any repercussions. In the extremely unlikely event that illicit activity is identified during the focus group interview or reported on the questionnaire, I will be obliged to report it to the appropriate authorities. Risks to privacy and confidentiality will be managed by the researcher in terms of protecting the data from unauthorised access and ensuring that no individual participant or the study site is identifiable in any publications or conference presentations.

Are there any Benefits?

Participation in the study is likely to increase your awareness of the IEC 80001-1 standard and raise your understanding of the requirements of the standard. The results of this study will contribute to the framework that will enable healthcare organisations to assess themselves against IEC 80001-1. The framework will inform one of the technical reports for the IEC 80001-1 family of standards, this standard is internationally applicable to all healthcare organisations. It may also identify areas of strength, weakness, opportunity and threats and possible recommendations which if implemented may improve risk management processes for IT network modification projects at both the department and hospital level at the study site.

How will Confidentiality be maintained?

Participant and third-party anonymity will be preserved in analysis, publication and presentation of resulting data and findings by the researcher. The identity of individual participants and the study site will not be revealed in any subsequent publications or conference presentations and the identity of participants and the site will remain confidential. No individual will be identifiable from the study data. No audio recordings will be made available to anyone other than the research team, nor will any such recordings be replayed in any public forum or presentation of the research. Any recordings will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (conferences etc). All data pertaining to the study will be stored

on a password protected PC, hard copy questionnaires will be stored in a locked filing cabinet and requirements of the Data Protection Act 2003 will be strictly adhered to.

What are the debriefing arrangements?

The researcher can be contacted at any stage (see contact details below). In addition, the employee assistance programme (EAP) is a free counselling service available to hospital staff if you feel you have been affected in any way by participating in the study. Details of this service are available on the Intranet.

Where can I get further information?

If you have any further questions about the study now or in the future please contact the researcher (details below).

Contact Details

For further information regarding this study,

Lead/ Principal Investigator: Lucy Kielty

Contact Telephone Number: 086 8329239 / 01 4103495

Contact email: kieltyl@tcd.ie

Appendix D.2 Informed Consent Form

LEAD RESEARCHER: Lucy Kielty

BACKGROUND OF RESEARCH

There is increasing use of networked interoperable medical devices linked to electronic health records / clinical information systems. These medical devices are being incorporated into the organisation's IT network leading to new and unforeseen consequences and risks to quality and patient safety. The International Standard IEC 80001-1 (2010) identifies the key properties of medical IT networks incorporating medical devices as: safety, effectiveness, and data & system security. In order to safeguard these properties risks must be managed. The Standard recognises that devices are incorporated into IT networks to achieve the benefits of interoperability and defines the roles/ responsibilities & activities for risk management of medical IT networks. The standard also takes a life cycle approach to risk management of the network and identifies healthcare organisations as the organisation responsible for managing the risks associated with incorporating medical devices onto the network. Implementation of the standard has been slow; currently there is no means for healthcare organisations to assess their risk management processes against IEC 80001-1 to determine strengths, weaknesses, opportunities, threats (MacMahon *et al.* 2013). This study is contributing to research being undertaken by MacMahon *et al.* (2013) in this area in Dundalk Institute of Technology. This study seeks to contribute to the development and validation of an assessment method (Question set) to assess risk management activities against IEC 80001-1 (2010). The study aims are:

- To contribute to the standard IEC 80001-1 "Application of Risk Management for IT Networks Incorporating Medical Devices" (2010).
- To develop the assessment criteria to assess health service provider Medical IT network risk management activity against IEC 80001-1 (2010).
- To raise awareness of the standard among healthcare personnel.
- To improve risk management of IT networks incorporating medical devices.

PROCEDURES OF THIS STUDY

Participants will be invited to participate in a focus group assessment / semi-structured interview of approximately 2 hours duration. The interview will be audio recorded. A post assessment questionnaire will be provided in hard copy format for completion. A findings report which will include recommendations will be prepared and participants will be invited to review same (via brief individual interviews – 15 minutes). Confidentiality and anonymity will be maintained, neither individual participants nor the study site will be identifiable in any subsequent publications or conference proceedings. All data will be stored and destroyed in compliance with the Data Protection Act 2003 (password protected PC, encrypted memory sticks, locked filing cabinet).

PUBLICATION

The research may be published in peer reviewed journals; however participants or the study site will not be named in any subsequent publications. The study may also be presented at national and international healthcare & health related conferences and participants and study site anonymity will be maintained. Individual results will be aggregated anonymously and research reported on aggregate results.

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal & ethical rights.

- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- <If the research involves viewing materials via a computer monitor> I understand that if I or anyone in my family has a history of epilepsy then I am proceeding at my own risk. ?
- I have received a copy of this agreement.

PARTICIPANT'S NAME: _____

PARTICIPANT'S SIGNATURE: _____ **Date:** _____

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS:

For further information regarding this study,

Lead/ Principal Investigator: Lucy Kielty

Contact Telephone Number: 086 8329239 / 01 4103495

Contact email: kieltyl@tcd.ie

RESEARCHER / INVESTIGATOR'S NAME: Lucy Kielty

RESEARCHER / INVESTIGATOR'S SIGNATURE: _____ **Date:** _____

Appendix D.3 Focus Group Assessment Interview Schedule

- Introductions -
- Explanation of Interview Format
- Consent Form Completion
- Brief overview presentation of the standard IEC 80001-1 (2010) – 10 Minutes
- Assessment
- Closing Remarks
- Post Assessment Questionnaire - Completion

Appendix D.4 Post Assessment Questionnaire

The assessment focus is the validation of a number of questions (assessment method) which have been developed to assess the risk management processes referred to in the standard IEC 80001-1 (2010).

I would appreciate if you could please take the time to complete this questionnaire designed to capture your feedback on the assessment. **Insert to indicate your response or use the free text boxes provided.**

The information provided will be treated confidentially. Participation is completely voluntary.

Each question is optional. Feel free to omit a response to any question; however the researcher would be grateful if all questions are responded to. Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.

Section 1 Standards

Q1 (a)	I have used standards in a professional capacity previously.				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q1 (b)	If you have used standards please indicate the standards that you have used <i>(If you have not used standards skip to question 2).</i>	N/A
		<input type="checkbox"/>

Q2 (a)	Please indicate your level of awareness of the standard IEC 80001-1 prior to participating in the assessment using a scale of 0 – 5 where 0 = not aware and 5 indicates very aware (circle answer).					
	0	1	2	3	4	5

Q2 (b)	Please indicate your level of awareness of the standard IEC 80001-1 after participating in the assessment using a scale of 0 – 5 where 0 = not aware and 5 indicates very aware (circle answer).					
	0	1	2	3	4	5

Section 2 Pre assessment Presentation

Q3	The pre assessment presentation was clear.				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q4	The pre assessment presentation provided enough information on the standard.				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q5	The pre assessment presentation provided enough information on process assessment.				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Post Assessment Questionnaire

Each question is optional.

Feel free to omit a response to any question; however the researcher would be grateful if all questions are responded to.

Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.

Q6 (a) The pre assessment presentation could have provided additional information.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q6 (b) What additional information did you feel was missing *(If you did not feel there was any additional information necessary skip to question 7)*

N/A

Section 3 Assessment

Q7 (a) The assessment questions were clear and easy to understand.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q7 (b) If the assessment questions were not clear and easy to understand please comment below.

N/A

Q8 (a) The assessment questions adequately addressed the risk management processes.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q8 (b) If the assessment questions did not adequately address the processes please indicate why below.

N/A

Post Assessment Questionnaire

Each question is optional.

Feel free to omit a response to any question; however the researcher would be grateful if all questions are responded to.

Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.

Q9 (a) Participating in the assessment increased my knowledge and understanding of IEC 80001-1.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q9 (b) I can use my increased knowledge & understanding of IEC 80001-1 in my work.

N/A

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q10 I feel participating in the assessment has informed me of the risk management activity requirements of the standard.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Q11 The assessment method seemed appropriate.

Strongly Agree

Agree

Neither Agree nor Disagree

Disagree

Strongly Disagree

Section 4 Comments

Q12 Do you have any additional comments or suggestions?

Thank you for completing this questionnaire.

Please return to Lucy Kielty, ICIP Office GICU, St James's Hospital or via email: lkielty@tcd.ie

Appendix D.5 Focus Group Assessment Interview Questions

The following questions will be asked, however it may be necessary to probe responses with additional questions to clarify responses

Process Name / Question	Response Type
Medical IT Network Risk Management	
Q1 Do you have a Medical IT Network Risk Management File?	Yes/No
Q2 Have risk management resources been assigned?	Yes/No
Q3 Are risk management activities performed according to the risk Management Plan and process?	Yes/No
Q4 Are the key properties of the network considered during the performance of risk management activities?	Yes/No
Q5 Are risk management activities documented?	Yes/No
Risk Analysis & Evaluation	
Q6 How do you identify likely safety hazards for individual devices?	Dialogue
Q7 How do you analyse the system as a whole to identify likely safety hazards?	Dialogue
Q8 How do you consider the impact of the device on the environment, effectiveness, data security & system security?	Dialogue
Q9 Do you have a procedure for estimating risk?	Yes/No, Dialogue
Q10 How do you identify possible consequences of harm?	Dialogue
Risk Control	
Q11 Are proposed risk control measures identified for every risk?	Yes/No, Dialogue
Q12 How are risk control measures considered in relation to the key properties and prioritised?	Dialogue
Q13 Are selected risk control measures implemented?	Yes/No, Dialogue
Q14 Is the implementation and effectiveness of risk control measures verified and documented?	Yes/No
Residual Risk	
Q15 Is residual risk reviewed and assessed for acceptability?	Yes/No, Dialogue
Q16 Is the decision on whether or not to approve the residual risk based on the documented risk/benefit analysis?	Yes/No, Dialogue

Change Release & Configuration Management

Q17 Is Configuration Management process documented and applied during the risk management of change release management?	Yes/No, Dialogue
Q18 Is the Change/Release Process documented?	Yes/No
Q19 Are the acceptability of changes determined using the risk management process?	Yes/No
Q20 Are action plans implemented following the Change/Release Management Process?	Yes/No

Decision on the application of Risk Management

Q21 Is the Change-Release Management Process implemented?	Yes/No
Q22 Has the nature of the change been identified?	Yes/No
Q23 Has a project plan been established & revised to reflect changes to the project?	Yes/No

Go-Live

Q24 Is residual risk reviewed in the context of recent or pending changes prior to go-live?	Yes/No
Q25 Have the specified changes been approved prior to go-live?	Yes/No

Monitoring

Q26 Has a process for monitoring of the live network been established?	Yes/No, Dialogue
Q27 Are requirements for monitoring included in the risk management plan?	Yes/No, Dialogue

Event Management

Q28 Has an event management process been established?	Yes/No, Dialogue
Q29 Are negative events captured and documented?	Yes/No

Medical IT Network Planning

Q30 Has the risk management plan been maintained and updated when a project changes an existing medical IT network?	Yes/No, Dialogue
---	------------------

Medical IT Network Documentation

Q31 Has additional documentation for the connection of a medical device to an IT network been provided /obtained?	Yes/No, Dialogue
Q32 Has a risk relevant asset description been maintained?	Yes/No

Responsibility Agreements

Q33 Has the need for a responsibility agreement(s) been determined?

Yes/No

Risk Management Policy

Q34 Has a risk management policy been established?

Yes/No

Q 35 Does the risk management policy Include description of or reference to processes applying to Medical IT Networks?

Dialogue

Organisational Risk Management

Q 36 Has a risk management process been established and maintained which takes into account the defined use of the medical IT-network?

Dialogue

Q37 Is the performance of the risk management process reported to Top Management?

Yes/No

General Comments

Q 38 Any general comments related to assessment?

Dialogue

Appendix E Individual Interview Schedule

Interview Questions Re Findings Report

Q1 Have you had time to read the findings report?

Q2 Do you agree with the recommendations outlined?

Q3 Can the recommendations be implemented?

Q4 Which recommendations will you take ownership of?

Q5 Do you have any other Comments?

Appendix F Individual Interview Transcripts (see enclosed CD)

Appendix G Ethics Approval from the School of Computer Science & Statistics (SCSS)

From: Tricia Fowler <Tricia.Fowler@scss.tcd.ie>
Date: 9 December 2013 10:38
Subject: RE: Research Ethics Application Form and Outline Research Proposal L. Kielty MSc Health Informatics - 025/14
To: Lucy Kielty <kieltyl@tcd.ie>
Cc: Research Ethics <research-ethics@scss.tcd.ie>

Hi Lucy

Thank you for these additions. The Research Ethics Committee have reviewed and approved your application. You may proceed with this study.

We wish you success in your research.

Kind Regards
Tricia
Tricia Fowler
Executive Officer – Research Unit
School of Computer Science & Statistics
O'Reilly Institute
Trinity College
Dublin 2
Tel: + 353 1 896 1445

From: Lucy Kielty [mailto:kieltyl@tcd.ie]
Sent: 04 December 2013 14:27
To: Tricia.Fowler@scss.tcd.ie
Subject: Re: Research Ethics Application Form and Outline Research Proposal L. Kielty MSc Health Informatics

Hi Tricia,

Please find attached SCSS Ethics application supporting documentation as follows:

- Permission to access lab. staff
- Permission to access Intensive care unit staff
- Permission to access IT / MPBE staff
- Response from SJH Ethics Committee
- Hospital Information Sheet (for Management)
- Hospital Consent Form - signed
- Designated Research Approval Form - signed

Kind Regards,
Lucy Kielty
MSc Health Informatics Student
086 8329239

On 3 December 2013 12:30, Tricia Fowler <Tricia.Fowler@scss.tcd.ie> wrote:

Hi Lucy

Thank you for your application. Before it can be considered by the Research Ethics Committee can you please include a Board of Management Information Sheet and Consent Form. As the

research is to be carried out in a teaching hospital, permission must be sought from the management before research commences.

Kind Regards

Tricia

Tricia Fowler

Executive Officer – Research Unit

School of Computer Science & Statistics

O'Reilly Institute

Trinity College

Dublin 2

Tel: + 353 1 896 1445

From: Lucy Kiely [mailto:kielyl@tcd.ie]

Sent: 01 December 2013 17:49

To: research-ethics@scss.tcd.ie

Subject: Research Ethics Application Form and Outline Research Proposal L. Kiely MSc Health Informatics

Dear Ethics Committee,

Please find attached completed SCSS Ethics application form and Outline Research Proposal for your review / consideration. I have included the participant information sheet, consent form, focus group interview protocol, questionnaire, and interview questions in the appendices of the application form. My proposal includes a focus group interview assessment of an IT network modification project prior to the project Go-Live with a possible Go-Live date of the 16/12/2013). The advantage of undertaking the data collection prior to Go-Live would be to maximise potential benefits for the participants and organisation and add to this study's robustness. I would be grateful for your approval at your earliest convenience.

Yours Sincerely,

Lucy Kiely

Student Number: 02165988

Appendix H Permission to Access Participants from Corporate Management & Heads of Department

Appendix H.1 Permission to access Hospital Staff (Approval of Designated Research Activity Proposal Pages 1-7)

3. PROJECT DETAILS

Title of Project: *Development & Validation of an Assessment Method to Assess against International Standard IEC 80001-1 Application of Risk Management for IT Network*
Brief description of the proposed research activity including the number of patients to be recruited for the study: *patients = 0, incorporating medical devices*

Focus group semi structured Interview - 5-8 Staff participants recruited using purposive sampling selected for involvement in Risk Management activities of IT Network projects. One project in ICU has been identified, a possible 2nd project will use another dept. possibly endoscopy.

Proposed Date for commencing data collection	13/12/13	
Proposed Date for completing data collection	13/02/14	x depends on if 2nd dept is involved
Proposed Date for completion of research	24/6/14	
Proposed Date research submitted/published	24/6/14	

4. **RESOURCE USAGE**

- Will the proposed research activity involve use of Hospital resources?

YES NO

- If Yes, please describe the extent of such resource use under the following headings:

Accommodation: Meeting Room in GICU for 2hr focus group x 2

Equipment: PC - powerpoint presentation
PC - email invite/meeting request

Procedures: None

Diagnostic/Physiological tests: None

Staff: 5-8 participants per focus group/Semi structured interview
1-2 focus group Semi structured interviews x 2 hrs each

Consumables: None - will use personal stationery/paper

Other:

Where resource use involves combined service/research mix, please estimate related approximate distribution.

SERVICE: ____% RESEARCH: ____% N/A

5. FUNDING ARRANGEMENTS

Is the proposed research activity to be supported or sponsored by grant/funding assistance from external individual(s), organisation(s) or companies?

YES

NO

MSc funded by SSH.

If YES: please complete the following:

- List/name sponsors: *N/A*
- Details of grant/funding arrangements to apply (*to contain details of total grant/funding to be made available and basis for calculation*) *N/A*
- In calculating grant/funding levels to apply, are sponsors making provision for envisaged use of Hospital resources? *N/A*
YES NO
- If Yes - please clearly outline provisions if these are not evident in information already furnished above.
- Please outline how grants/funds allocated are to be utilised in the proposed research project: *N/A*
- Into which account will the monies be paid?: *N/A*
Is this a Hospital account?
If not, please state account holder:
- Where grants/funding are to be utilised to employ additional personnel, please specify the extent to which such staff will contribute to hospital services. *N/A*

- Please outline in general terms the benefits likely to accrue to the hospital arising from this research activity.

It is anticipated that the focus group will identify strengths, weaknesses, opportunities and threats & the findings Report will include recommendations which if implemented will improve Risk Mgt activities. The study will also improve Compliance with the standard

6. **FINANCIAL ACCOUNTING AND CONTROL ARRANGEMENTS** IFL 80001-1/2010

Please outline financial and accounting control provisions to be effected with respect to the proposed research activity as follows:

N/A

- Name/Address of Financial Accounting Agency:

- St. James's Hospital Finance Department
- Trinity College
- Other

If other, please furnish details:

Where the accounting agency is not St. James's Hospital, please confirm production and availability to the Hospital of the following accounting documentation:

- Income & Expenditure Accounts
- Audited Accounts
- Control provisions in position for Research Fund Accounts
- Transaction details of Research Fund Accounts

Do you wish the Hospital's Finance Department to undertake these Financial Accounting and Control provisions for the proposed research activity?

N/A

YES NO

(Note: A nominal administrative charge will apply to this service).

7. DATA CONTROL AND PROTECTION

In what form will data be collected and held?

Research notes, Hard copy / electronic questionnaires, Audio Recordings
All data will be held on password protected PC & locked filing cabinet

How long is collected data intended to be retained? Duration of study and until publication. The Hospital and participants will not be named in any subsequent publications.

What protections will be in place in relation to personal data collected?

No personal data will be collected

Who is the Data Controller for the research project? Lucy Kielty

Will collected data be transferred outside of the Hospital computer system?

No Hospital Computer System data will be transferred.
Internal email will be used for return of questionnaires

If Yes:

a) What transfers are envisaged? None

b) What agreements are in place/planned?

8. INDEMNIFICATION

In general, where a sponsoring agent is involved, it is necessary for that agent to provide indemnification cover to the hospital. The HSE indemnification documentation should be submitted in the standard Hospital format with this approval form. The research activity may not proceed in the absence of this indemnity.

9. RESEARCH ETHICS COMMITTEE APPROVAL

Please attach evidence of formal approval from the relevant Research Ethics Committee for the proposed Research Activity.

YES NO N/A

10. IRISH MEDICINES BOARD APPROVAL

Please attach evidence of formal approval from the Irish Medicines Board, if relevant.

YES NO N/A

11. DECLARATION

I confirm that the information provided herein and attached is accurate and discloses the complete resource implications and grants/funding provisions applicable to the specified proposed research activity.

Lucy Kielly 25/11/13
Applicant and Principal Investigator Date

12. APPROVAL

SIGNED: *Neilieann O'Brien*
~~Deputy CEO/Operations Manager~~
Legal Insurance Manager

DATE: 25/11/13
Date

Appendix H.2 Permission to access IT & MPBE staff

IMS / MPBE Departments,
St James's Hospital,
James's St.
04/12/2013

2 Belgree Court,
Kilbride,
Dublin 15

Re Research Study entitled: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)

Dear Lucy,

Thank you for your letter requesting access to Information Management Services (IMS) and Medical Physics & Bioengineering (MPBE) department staff involved in medical IT network modification projects. Thank you for the research proposal and supporting documentation (questionnaire, interview questions etc) outlining the study details which include the following:

Study Aims:

- To contribute to the standard IEC 80001-1 "Application of Risk Management for IT Networks Incorporating Medical Devices" (2010).
- To develop the assessment criteria to assess health service provider Medical IT network risk management activity against IEC 80001-1 (2010).
- To raise awareness of the standard among healthcare personnel.
- To improve risk management of IT networks incorporating medical devices.

IT and MPBE staff participation

Staff from two medical IT network modification projects (one of which is the replacement of arterial blood gas analysers in the critical care units).

Data collection

Focus group interview, questionnaire, individual interview and group project review.

Confidentiality

Confirmation that confidentiality and anonymity of participants and the hospital will be safeguarded and the study will be conducted in compliance with the Data Protection Act 2003.

I am happy to grant you permission to access IMS and MPBE staff as outlined in your proposal.

Yours Sincerely,



Prof. Neil O Hare
Director of Health Informatics
IMS / MPBE Dept.

Appendix H.3 Permission to access Laboratory staff

Permission to access Laboratory Staff at St James's Hospital

From: Gibbons, John (Lab Manager)
Sent: 03 December 2013 07:47
To: Kielty, Lucy
Subject: RE: Re permission to access Lab staff

Yes Lucy that is fine. Good luck with the project.

Regards

John Gibbons
Laboratory Manager

From: Kielty, Lucy
Sent: 02 December 2013 14:11
To: Gibbons, John (Laboratory Manager)
Subject: Re permission to access Lab staff

Hi John,
Further to my letter dated 01/12/2013 and discussion this morning regarding your permission to access laboratory staff for the purposes of my research study entitled: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010), Please find enclosed soft copy of information attached as requested. Attachments as follows:

- Letter requesting access
- Outline Proposal
- Questionnaire
- Interview questions

Kind Regards,
Lucy

Lucy Kielty
Clinical Informatics Manager
Phone: 01 410 3495
Email: lkielty@stjames.ie

Appendix H.4 Permission to access Intensive Care Unit staff

Appendix H.4.1 Permission to access Intensive Care Unit Nursing staff



OSPIDÉAL NAOMH SÉAMAS
ST JAMES'S HOSPITAL



Nursing Research Access Committee,
Date: 29th May 2014
Our ref: NRAC 124

Ms. Lucy Kielty,
2 Belgree Court,
Kilbride,
Co. Meath,

RE: Study: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)

Dear Lucy,

The Nursing Research Access Committee has reviewed your request for access to the nursing staff at St. James's Hospital. The committee note the study involves the following:

Participants: Selected Nurses (professional development facilitator & clinical informatics nurses) working in Critical Care Units

Data Collection: Focus Group Semi-structured interview & individual interviews

Gatekeeper: NA

The committee require the following provisions:

- Staff participation is voluntary, interviews/focus groups to be completed in participants' own time.
- Ensure anonymity and confidentiality of participants & hospital is maintained.
- Agree procedures with the local gatekeeper identified (NA)
- Inform the Nursing Research Access Committee when data collection and thesis submission is complete.
- A copy of the thesis must be forwarded to the committee on completion – submitted theses will subsequently be archived in the Centre for Learning & Development & listed on Intranet.
- All portable devices (USB, Laptop) used for this study must be password protected and encrypted in line with the Data Protection Act and compliance with the Ethical Approval granted.

You are hereby granted **permission to access the nursing staff** working in Critical Care Units as outlined in your proposal, once the above provisions have been completed.

Please note that the Nursing Research Access Committee **does not** confer ethical approval. It is the applicant's responsibility to ensure appropriate Ethics Committee approval is obtained. The committee acknowledge receipt of Ethical Approval letter (dated 9th December).

On behalf of the Nursing Research Access Committee I would like to take this opportunity to thank you for your application and I wish you success with your research. I look forward to receiving a copy of the study on completion. Also a MDT research seminar is held annually and you will be invited to participate and present your findings.

Yours Sincerely,

Mr. Paul Gallagher
Director of Nursing / Chairperson Nursing Research Access Committee
CC: Ms. Catherine Tobin ADoN Critical Care Services

Appendix H.4.2 Permission to access Intensive Care Unit Nursing staff



OSPIDÉAL NAOMH SÉAMAS ST. JAMES'S HOSPITAL



Ospidéal Naomh Séamas, Sráid Shéamais, Baile Átha Cliath 8.

St. James's Hospital, James's Street, Dublin 8.

+353 1 410 3000 www.stjames.ie

2 Belgree Court
Kilbride
Dublin 15

5th December 2013

Re: Research Study Entitled: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)

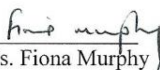
Dear Lucy,

Thank you for your letter regarding your research study. The aims of the study are clearly outlined as is the staff involvements required.

I am very happy to grant you permission to access the Intensive Care Unit Nursing staff to carry out your research.

I wish you well with your research and if you require my assistance during the course of the study please do not hesitate to contact me at any time.

Yours sincerely,


Ms. Fiona Murphy
Operations Manager Surgery & Anaesthesia Directorate

Ospidéal Ollscoile Choláiste na Tríonóide, Baile Átha Cliath.
University Hospital of Trinity College Dublin.



Appendix H.4.3 Permission to access Intensive Care Unit staff

Permission to Access Intensive Care Staff at St James's Hospital

From: Collins, Danny

Sent: 02 December 2013 14:59

To: Kielty, Lucy

Subject: Danny Collins re; Development and Validation of an Assessment Method to Assess against IEC 80001-1.

Dear Lucy

Thank you for your communication on the above topic as a component of your MSc in Health Informatics. I take note of your approval from the Risk and Legal Office in SJH and the fact the SJH/AMNCH Research Ethics Committee believe the study does not require ethical approval. Thank you for the copy of the full research proposal, together with focus group questions and questionnaire. Everything is satisfactorily explained and it has my full support and permission to proceed in the Intensive Care.

Sincere regards

Danny Collins

Director of Intensive Care

Saint James's Hospital.

Appendix I Hospital Information Sheet & Consent from Corporate Management

Appendix I.1 Hospital Information Sheet

Hospital Information Sheet

Title of Research Study: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)

Researcher: Lucy Kielty

Research Supervisor: Dr Damon Berry

Background to the Study

There is increasing use of networked interoperable medical devices linked to electronic health records / clinical information systems. These medical devices are being incorporated into the organisation's IT network leading to new and unforeseen consequences and risks to quality and patient safety. The International Standard IEC 80001-1 (2010) identifies the key properties of medical IT networks incorporating medical devices as: safety, effectiveness, and data & system security. In order to safeguard these properties risks must be managed. The Standard recognises that devices are incorporated into IT networks to achieve the benefits of interoperability and defines the roles/ responsibilities & activities for risk management of medical IT networks. The standard also advocates a life cycle approach to risk management of the network and identifies healthcare organisations as the organisation responsible for managing the risks associated with incorporating medical devices onto the network. Implementation of the standard has been slow, currently there is no means for healthcare organisations to assess their risk management processes against IEC 80001-1 to determine strengths, weaknesses, opportunities, threats (MacMahon *et al.* 2013).

Purpose of the Study

This study is a component of an MSc in Health Informatics, which I am undertaking in Trinity College Dublin.

This study will feed into current research being conducted in this area by MacMahon *et al.* (2013). This study seeks to develop and validate an assessment method (Question set) to assess risk management activities against IEC 80001-1 (2010).

The aims of the study are:

- To contribute to the International Standard IEC 80001-1 “Application of Risk Management for IT Networks Incorporating Medical Devices”.
- To develop the assessment criteria to assess health service provider Medical IT network risk management activity against IEC 80001-1 (2010).
- To raise awareness of the standard among healthcare personnel.
- To improve risk management of IT networks incorporating medical devices.

Location for Study

The study is being carried out in a large academic teaching hospital. Two departments in St James’s Hospital involved in IT network modification projects will be involved in the study (one of which is the critical care units).

Participants

The study will involve staff with risk management responsibilities related to 2 medical IT network modification projects (example: nursing, medical physics & bioengineering, IT, Laboratory staff and the risk manager). The total number of hospital staff involved will be approximately 20 (1 or 2 from each discipline from each project depending on the numbers involved in the project). The 1st project is the upcoming modification of the IT network to incorporate new arterial blood gas analysers onto the hospital IT network linked to the clinical information system (ICIP) in the critical care units. There are four nurses (including myself), two IT personnel, and two laboratory personnel involved in this project. The 2nd project has yet to be identified but will likely include 1- 2 (max of 3 per discipline).

Research Approach

This research takes a design research approach, which was selected for its iterative cycle methodology whereby feedback gained from the assessment will be used to refine the question subset, feedback gained from the findings report will inform the recommendations and impact the likelihood of implementation of same.

Data Collection

The study involves mixed methods of data collection using a combination of a focus group /semi-structured interview for the assessment, post assessment questionnaire, individual interviews to review the findings report recommendations and a post Go Live review.

Study Procedures

The study will be conducted in the form of an assessment of risk management processes related to the change to the Medical IT network (1st project is the removal of 3 ABG analysers and addition of 8 new ABG analysers). At the start of the assessment the standard IEC 80001-1 standard and study will be explained. The assessment interview will take place at a time and

location that is suitable to all participants. It is likely to occur in the department involved in the IT modification project(s) (eg critical care unit). Participants will be asked to sign a consent form to indicate their willingness to participate prior to the commencement of the interview. The interview will take approximately 2 hours and an audio recording will be made.

The assessment focus will be the validation of a number of questions which have been developed to assess the risk management processes referred to in the standard.

Participants will be asked to complete a questionnaire following the interview which can be returned via email to the researcher.

Following the assessment a findings report will be prepared which may include recommendations to address any weaknesses identified in the assessment. Participants will be given an opportunity to review the recommendations in the findings report to agree whether the recommendations are valid and whether or not they could or would be implemented.

Confidentiality

All information received will be kept confidential and anonymous. The findings will be presented in a manner ensuring the participants' identity and the study site is not identified.

Benefits

I hope by carrying out this study that the results will benefit the organisation in terms of improved risk management processes related to IT network modification projects in line with the International standard. Participation in the study is likely to increase participants' awareness of the IEC 80001-1 standard and raise their understanding of the requirements of the standard. The results of this study will contribute to the framework that will enable healthcare organisations to assess themselves against IEC 80001-1. The framework will be incorporated into the IEC 80001-1 family of standards, this standard is internationally applicable to all healthcare organisations.

Risks

Participation in this study is entirely voluntary; participants are free to withdraw at any stage without any repercussions. In the extremely unlikely event that illicit activity is identified during the focus group interview or reported on the questionnaire, the researcher will be obliged to report it to the appropriate authorities. Risks to privacy and confidentiality will be managed by the researcher in terms of protecting the data from unauthorised access and ensuring that no individual participant or the study site is identifiable in any publications or conference presentations

Approval

I have received approval to undertake the study from the Risk and Legal Office. I have been informed by the Joint SJH/AMNCH Research Ethics Committee that the study does not require hospital ethical approval as there are no patients involved; however, the study will undergo approval by the Trinity College Ethics Committee prior to commencement. This study is due for completion by the year ending June 2014.

Contact Details

For further information regarding this study,

Lead/ Principal Investigator: Lucy Kielty

Contact Telephone Number: 086 8329239 / 01 4103495

Contact email: kieltyl@tcd.ie

Appendix I.2 Hospital Consent Form Signed

CONSENT FORM

Title of Research Study: Development and Validation of an Assessment Method to Assess against IEC 80001-1: Application of Risk Management for IT Networks Incorporating Medical Devices (2010)

LEAD RESEARCHER: Lucy Kielty

SUPERVISOR: Dr. Damon Berry

RESEARCH STUDY AIMS

- To contribute to the standard IEC 80001-1 "Application of Risk Management for IT Networks Incorporating Medical Devices" (2010).
- To develop the assessment criteria to assess health service provider Medical IT network risk management activity against IEC 80001-1 (2010).
- To raise awareness of the standard among healthcare personnel.
- To improve risk management of IT networks incorporating medical devices.


PROCEDURES OF THIS STUDY

Participants will be invited to participate in a focus group assessment / semi-structured interview of approximately 2 hours duration. The interview will be audio recorded. A post assessment questionnaire will be provided in hard copy format for completion. A findings report which will include recommendations will be prepared and participants will be invited to review same (via brief individual interviews – 15 minutes).

DECLARATION:

- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and I understand the description of the research that is being provided to me.
- I agree that data may be used for scientific purposes and I have no objection that the data is published in scientific publications in a way that does not reveal the participants' or organisations' identity.
- I understand confidentiality and anonymity will be maintained
- I have been assured that all data will be stored and destroyed in compliance with the Data Protection Act 2003 (password protected PC, encrypted memory sticks, locked filing cabinet).
- I have received a copy of this agreement.

APPROVER NAME: Prof Neil O Hare

APPROVER SIGNATURE:  **Date:** 4/12/13
On behalf of St James's Hospital

Statement of researcher's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and have fully answered such questions. I believe that the individual understands my explanation and has freely given informed consent.

RESEARCHER NAME: Lucy Kielty

RESEARCHER SIGNATURE:  **Date:** 4/12/13

RESEARCHERS CONTACT DETAILS:

Lucy Kielty, Phone: 086 8329239 / 01 4103495, Email: kieltyl@tcd.ie

Appendix J Assessment Questions & Guidance Document (Assessment Tool)

Semi Structured Focus Group Assessment Questions & Guidance

Process Name / Question	Response Type	Guidance
Medical IT Network Risk Management		
Q1 Do you have a Medical IT Network Risk Management File?	Yes/No	Consider whether Medical IT Network Risk Management File contains all relevant risk management information – refer to work products in the PAM. Consider the document management procedure for the file – file access, storage, update back up, version control etc.
Q2 Have risk management resources been assigned?	Yes/No	Consider top management input into risk management process and ensure that the relevant risk management resources are assigned. Resources can include hardware, software and personnel etc.
Q3 Are risk management activities performed according to the risk Management Plan and process?	Yes/No	Consider whether risk management activities are performed during the supervision, operation, installation and maintenance of Medical IT Network(s) throughout the life cycle. Consider whether risk management activities are being performed according to the RM plan and process.
Q4 Are the key properties of the network considered during the performance of risk management activities?	Yes/No	Consider the impact to the network in terms of safety, effectiveness and data and system security throughout the life cycle.
Q5 Are risk management activities documented?	Yes/No	Consider the appropriateness of the approach to documenting risk management activities according to the scope of the medical IT network project.
Risk Analysis & Evaluation		
Q6 How do you identify likely safety hazards for individual devices?	Dialogue	Consideration must be given to the identification of hazards of individual devices when establishing a new medical IT network, adding a device to the IT network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment. Consider the impact of the device activities on the: a) devices and system which are part of the medical IT network b) devices and system

Process Name / Question	Response Type	Guidance
		which are not part of the medical IT network
Q7 How do you analyse the system as a whole to identify likely safety hazards?	Dialogue	Consideration must be given to the identification of hazards of individual devices when establishing a new medical IT network, adding a device to the IT network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment . Consider the impact of the device activities on the: a) devices and system which are part of the medical IT network b) devices and system which are not part of the medical IT network .
Q8 How do you consider the impact of the device on the environment, effectiveness, data security & system security?	Dialogue	Consideration must be given to the identification of hazards and their impact on the system as a whole when establishing a new medical IT network, adding a device to the IT network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment . Hazards in this context are from the perspective of the ENVIRONMENT - Consider impact to the environment from the perspective of the impact in terms of ceasing or impairing functionality . Hazards in this context are from the perspective of the EFFECTIVENESS - effectiveness of the device is the ability of the device to produce the intended result for the patient and the responsible organisation. Hazards in this context are from the perspective of the DATA & SYSTEM SECURITY . Consider the impact of the device activities on the: a) devices and system which are part of the medical IT network b) devices and system which are not part of the medical IT network . In Terms of Effectiveness consider the impact of the device activities: a) from the perspective of the patient , b) from the perspective of the responsible organisation . In terms of DATA & SYSTEM SECURITY consider the impact of the device activities a) the confidentiality of the data , b) the integrity of the data , c) the availability of the data .

Process Name / Question	Response Type	Guidance
Q9 Do you have a procedure for estimating risk?	Yes/No, Dialogue	What is the treatment of identified risks once they have been identified? Is there a procedure for how the risks are estimated ? Is this a documented policy ?
Q10 How do you identify possible consequences of harm?	Dialogue	In cases where it is not possible to estimate the probability of occurrence of harm, how do you identify possible consequences of harm ? Are consequences documented ?
Risk Control		
Q11 Are proposed risk control measures identified for every risk?	Yes/No, Dialogue	Risk control measures should be used in the following order -1) inherent control by design, 2) protective measures, and 3) information for assurance. Consider key properties in the following order - 1) safety, 2) effectiveness, and 3) data and systems security when considering risk control options.
Q12 How are risk control measures considered in relation to the key properties and prioritised?	Dialogue	Risk control measures should be used in the following order -1) inherent control by design, 2) protective measures, and 3) information for assurance. Consider key properties in the following order - 1) safety, 2) effectiveness, and 3) data and systems security when considering risk control options.
Q13 Are selected risk control measures implemented?	Yes/No, Dialogue	Implement selected risk control measures.
Q14 Is the implementation and effectiveness of risk control measures verified and documented?	Yes/No	Verify the implementation and effectiveness of all risk control measures in the operational system and document in the medical IT Network Risk Management File.
Residual Risk		
Q15 Is residual risk reviewed and assessed for acceptability?	Yes/No, Dialogue	Persons responsible for reviewing and accepting residual risk do so in co-operation with the Medical IT Network Risk Manager.
Q16 Is the decision on whether or not to approve the residual risk based on the documented risk/benefit analysis?	Yes/No, Dialogue	Make a decision on whether or not to approve the residual risk on the basis of the documented risk/benefit analysis.

Process Name / Question	Response Type	Guidance
Change Release & Configuration Management		
Q17 Is Configuration Management process documented and applied during the risk management of change release management?	Yes/No, Dialogue	Document configuration management process and apply during the risk management of change release management.
Q18 Is the Change/Release Process documented?	Yes/No	Document and apply change-release management (including Risk Management).
Q19 Are the acceptability of changes determined using the risk management process?	Yes/No	Determine the approval and acceptability of changes using the results of the risk management process during the change-release process.
Q20 Are action plans implemented following the Change/Release Management Process?	Yes/No	Implement action plans following the Change-Release management process. For each change to the medical IT Network, The change Release Process is implemented.
Decision on the application of Risk Management		
Q21 Is the Change-Release Management Process implemented?	Yes/No	Implement the Change-release management process for any new medical IT-Network or a change to an existing medical IT-Network.
Q22 Has the nature of the change been identified?	Yes/No	Consider the nature of the change to decide if the change can be made by an applicable change permit or if a medical IT network project is initiated.
Q23 Has a project plan been established & revised to reflect changes to the project?	Yes/No	Establish project plan for specific circumstances that have the potential to introduce new risk (not covered by change permit). Maintain project plan and revise to reflect changes to the project.
Go-Live		
Q24 Is residual risk reviewed in the context of recent or pending changes prior to go-live?	Yes/No	Review Medical IT Network residual risk summaries for acceptability of risk associated with interactions of recent or pending projects or changes, prior to going live.
Q25 Have the specified changes been approved prior to go-live?	Yes/No	Approval is given for the specified change by the medical IT Network Risk Manager prior to go-live.

Process Name / Question	Response Type	Guidance
Monitoring		
Q26 Has a process for monitoring of the live network been established?	Yes/No, Dialogue	Establish a process which outlines the monitoring requirements as part of the risk management plan to monitor each installed medical IT Network.
Q27 Are requirements for monitoring included in the risk management plan?	Yes/No, Dialogue	Include monitoring requirements as part of the risk management plan. Examples of what to monitor are: a) environment changes (including local/connected environment as well as relevant network or component DATA AND SYSTEMS SECURITY vulnerabilities); b) operational/performance feedback e.g., user feedback, speed problems, high error rates, failure, malicious software attacks; c) information about the incorporated components; d) information about similar MEDICAL IT-NETWORKS; e) reported events; and f) auditing of non-technical RISK CONTROL measures such as organizational policies and procedures.
Event Management		
Q28 Has an event management process been established?	Yes/No, Dialogue	Establish Event Management Process. Establish Event Management process to ensure that negative events are captured and documented.
Q29 Are negative events captured and documented?	Yes/No	Establish Event Management Process. Establish Event Management process to ensure that negative events are captured and documented.
Medical IT Network Planning		
Q30 Has the risk management plan been maintained and updated when a project changes an existing medical IT network?	Yes/No, Dialogue	Risk Management plan is maintained and updated when a project introduces changes to an existing medical IT network.
Medical IT Network Documentation		
Q31 Has additional documentation for the connection of a medical device to an IT network been provided /obtained?	Yes/No, Dialogue	Obtain (Responsible organisation) /Provide (medical device manufacturer) instructions for implementing the connection of a medical device to an IT network.
Q32 Has a risk relevant asset description been maintained?	Yes/No	Maintain risk relevant asset description , including a list of assets of IT networks interfacing with medical devices, as part of the risk management process.

Process Name / Question	Response Type	Guidance
Responsibility Agreements		
Q33 Has the need for a responsibility agreement(s) been determined?	Yes/No	Determine the need for one or more documented responsibility agreements whenever a medical device is incorporated into an IT network or the configuration of such a connection is changed.
Risk Management Policy		
Q34 Has a risk management policy been established?	Yes/No	Risk Management policy outlines criteria for determining acceptable risk , taking into account relevant international standards and national or regional regulations.
Q 35 Does the risk management policy Include description of or reference to processes applying to Medical IT Networks?	Dialogue	Description of or reference to processes applying to Medical IT Networks to include: Event Management, Change - Release Management, Configuration Management & Monitoring.
Organisational Risk Management		
Q 36 Has a risk management process been established and maintained which takes into account the defined use of the medical IT-network?	Dialogue	Establish & maintain Risk Management Process. Establish and maintain a risk management process which takes into account the defined use of the medical IT-network.
Q37 Is the performance of the risk management process reported to Top Management?	Yes/No	Report (made by Medical IT Network Risk Manager) on the performance of the risk management process to Top Management .
General Comments		
Q 38 Any general comments related to assessment?	Dialogue	

Appendix K Pre-Assessment Presentation

Study Title:

**Development & Validation of
Assessment Method to assess
against IEC 80001-1**

**Pre Assessment Presentation
&
Study Outline**

- Lucy Kielty 13/12/2013

1

Background

- Increasing use of networked interoperable medical devices linked to electronic health records / clinical information systems
- Medical devices are being incorporated into the organisation's IT network leading to unforeseen consequences and risks to quality and patient safety

2

**IEC 80001-1 (2010) "Application
of Risk Management for IT
Networks incorporating Medical
Devices"**

• International Standard developed to address the risks involved in incorporating medical devices on IT network

*International Electrotechnical Committee

3

IEC 80001-1 (2010)

Identifies the key properties of medical IT networks incorporating medical devices as:

- Safety,
- Effectiveness,
- Data & system security

To safeguard these properties risks must be managed

4

IEC 80001-1 (2010) Definitions

Safety: Freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or environment

Effectiveness: Ability to produce the intended result for the patient & responsible organisation.

Data and Systems Security: An operational state of a medical IT-Network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability.

5

IEC 80001-1 (2010)

- Recognises that devices are incorporated into IT networks to achieve interoperability benefits
- Defines the roles/ responsibilities & activities for risk management (mgt) of medical IT networks
- Takes life cycle approach to risk management of network
- Identifies healthcare organisations as responsible for managing the risks

6

IEC 80001-1 Risk Management Processes (14)

- Medical IT Network Risk Management
- Risk Analysis & Evaluation
- Risk Control
- Residual Risk
- Change Release & Configuration Mgt
- Decision on How to apply Risk Mgt
- Go- Live

7

IEC 80001-1 Risk Management Processes

- Monitoring
- Event Management
- Medical IT Network Planning
- Medical IT Network Documentation
- Responsibility Agreements
- Risk Management Policy
- Organisational Risk Mgt Process

8

IEC 80001-1 (2010)

- Implementation of the standard has been slow (Hegarty et al 2013)
- Currently there is no means for healthcare organisations to assess their risk management processes against IEC 80001-1 to determine strengths, weaknesses, opportunities, threats (MacMahon et al 2013)

9

Process Assessment

- **Process - Definition**
set of interrelated or interacting activities which transforms inputs into outputs.
IEC 80001-1 (2010) & ISO 14971 (2007)

Inputs  Outputs

- **Assessment - Definition**
is the systematic collection, review, & use of information undertaken for the purpose of implementing improvements.

10

Process Assessment - Method

- The Method for performing a Process Assessment is outlined in International Standard IEC 15504-2 (2003)
- Includes:
 - Process Reference Model (PRM),
 - Process Assessment Model (PAM) &
 - Assessment Framework (AF)

11

Study Context 1

- A Process Reference Model (PRM) & Process Assessment Model (PAM) have been developed for IEC 80001-1 (MacMahon et al 2013)
- PRM - processes, context, purpose & outcomes
- PAM - base practices, inputs/outputs

12

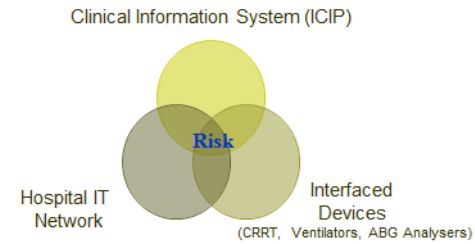
Study Context 2

- Development of a process assessment framework (compliant with IEC 15504) is underway (MacMahon et al 2013)
- This study will contribute to the framework which will be incorporated into an IEC 80001-1 technical report

13

IT Network Modification Project

Removal of Roche ABG Analysers(3) adding Siemens Analysers (8)



14

Assessment - Purposes

- Validate the question set developed to assess against IEC 80001-1 (2010)
- Identify strengths, weaknesses, opportunities & threats related to the IT Network Modification Project
- Research component of MSc

15

Next Steps

- Assessment
- Questionnaire
- Findings Report & Review
- Recommendations Implementation
- Post Go-Live Review

Questions ?

16

Appendix L Assessment Findings Report

IEC 80001-1 (2010) "Application of Risk Management to IT Networks incorporating Medical Devices" Assessment Findings Report

1.0 Background

There is increasing use of networked interoperable medical devices linked to electronic health records and clinical information systems. The incorporation of medical devices into the organisation's IT network creates a Medical IT network and leads to new risks to quality and patient safety. The International Standard IEC 80001-1 (2010) "Application of Risk Management to IT Networks incorporating Medical Devices" identifies the key properties of medical IT networks as: safety, effectiveness, and data & system security. In order to safeguard these properties the risks must be managed. The standard recognises that devices are incorporated into IT networks to achieve the benefits of interoperability (increased effectiveness, reduced cost, improved productivity) and defines the roles/ responsibilities & activities for risk management of medical IT networks. The standard also advocates a life cycle approach to risk management of the network and identifies healthcare organisations as the organisations responsible for managing the risks associated with incorporating medical devices onto the network. Implementation of the standard has been slow, possibly due to the fact that currently there is no means for healthcare organisations to assess their risk management processes against IEC 80001-1 to determine strengths, weaknesses, opportunities, threats (MacMahon *et al.* 2013). An assessment tool was developed to enable healthcare organisations to assess against the standard.

An assessment against IEC 80001-1 (2010) of a live Medical IT Network modification project was undertaken. The purposes of the assessment were 1) to validate the question set developed to assess against the Standard IEC 80001-1, 2) to identify any strengths, weaknesses, opportunities, and threats related to the risk management of the Medical IT modification project. Following the assessment the results were reviewed and a SWOT analysis undertaken to identify strengths, weaknesses, opportunities and threats. This findings report provides an outline of the IT Network Modification Project and the assessment and summarises the strengths, weaknesses, opportunities and threats identified during the assessment of the Medical IT Network modification project. It also outlines recommendations which if implemented could improve risk management activities related to the IT network modification project.

2.0 Outline of the Medical IT Network Modification Project

The Medical IT network modification project was undertaken in a large academic teaching hospital. It involves the removal of three Roche Arterial Blood Gas (ABG) Analysers from the Medical IT Network incorporating the Clinical Information System (Intellivue Clinical Information Portfolio - ICIP) in the Critical Care units & Theatre 1 & 2 and the addition of eight Siemens ABG analysers along with the addition of supporting software CONWORXs and RapidComms for remote control and monitoring. It also includes interfaces to the hospital Laboratory Information System, Patient Administration System and the Critical Care Clinical Information System (ICIP).

3.0 Assessment - Method

An assessment tool to assesses against the requirements of IEC 80001-1 (2010) was developed. An assessment against the requirements of IEC 80001-1 (2010) was undertaken on 13/12/2013. The participants in the assessment represented the various risk management stakeholders and disciplines involved in the project. These included: Point of Care Testing (POCT) personnel x 2 (one of which is the project lead), IT personnel x 2, Medical Physics &

Bioengineering (MPBE) x 1, Clinical Informatics personnel x 2, Clinical User x 1, ABG device manufacturer x 1, Clinical Information System Supplier x 1, healthcare organisation risk manager x 1. The assessment was conducted by the researcher (also a clinical informatics manager), a research assistant took notes during the assessment and the assessment was audio recorded.

4.0 Strengths, Weaknesses, Opportunities & Threats (SWOT) Analysis

A SWOT analysis was undertaken.

4.1 SWOT Analysis Method

The steps involved included the following:

- Review and transcription of assessment recordings.
- Review of researcher's and research assistant's notes from assessment.
- Review of IEC 80001-1 (2010) Standard requirements against responses (notes & recordings) to determine which requirements are met.
- Identification of strengths, weaknesses, opportunities and threats.
- Compilation of recommendations.

The findings are outlined below.

5.0 Findings

The following findings in terms of strengths, weaknesses, opportunities and threats were identified.

5.1 Strengths

Included in the strengths are requirements of the Standard IEC 80001-1 which were met.

- Risk management resources are in place (though informally)
- Involvement of multiple diverse stakeholders (all relevant disciplines involved)
- Many of the stakeholders involved work or have worked together previously which facilitated better engagement in the project.
- Contribution of stakeholder's combined extensive expertise, knowledge, experience and skills to the project.
- Identification of potential problems and safety hazards and planning for same was based on project member's prior experience.
- Change release processes were followed.
- Negative events are captured and documented as required.
- Biological and chemical risk assessments in terms of safety hazards were undertaken & documented.
- There is IT standards in place eg security standards that must be complied with before items are added to the network.
- Risks were identified:
 - Data download failure
 - User picks incorrect Medical Record Number (MRN) or manual data entry error
 - User fails to mark sample as venous
 - Risk of transcription error in event of failed download due to power issues
 - Results are only available in ICU, they aren't available outside ICU
- Risk control measures were identified:
 - Transcription of the test result in the event of a download failure
 - Audit of MRN-mismatches & feedback of results to raise awareness of error rates
 - Training to reduce errors
 - Scan of patient & staff ID to reduce errors of data entry
 - Use of Bar-coded syringes when available is being considered
 - Provision of access to results via EPR in areas outside ICU is being considered

- Regular (monthly) audits of incorrect MRNs (one of the identified risks) is undertaken by POCT personnel and the results are fed back to relevant personnel.
- The nature of the change was identified – project
- An event management process is in use.
- An installation plan for connection of the analysers to the network was provided by the manufacturer.
- The project leader/manager was identified and the role responsibilities were clarified.
- The need for a responsibility agreement was previously determined.
- The risk management process includes a corporate risk register which is fed to the board quarterly.

5.2 Weaknesses

- Assessment participants suggested that it would have been highly beneficial to have had the assessment at the start of the project which would have informed personnel of the standard requirements and increased the likelihood of meeting these requirements.
- Separate project plans for components of the project related to different disciplines / personnel reduced overall project transparency in terms of the project tasks / deliverables and timeframes for same.
- Prior to the assessment there was a lack of clarity on who was the project leader and the roles and responsibilities of the project leader.
- As many participants worked / work together previously this resulted in informal communication in lieu of more formal communication regarding the project at times.
- There is no Medical IT Network Risk Manager or Medical IT Network Risk Management File for this network modification project (requirements of IEC 80001-1 standard).
- There is no formal risk management plan & process (requirements of IEC 80001-1 standard).
- Risk management processes were not addressed in a formal manner, although risk management templates such as risk assessment matrix are available from the organisation's risk manager, many participants were unaware of availability of same and hence they were not used.
- Risk management activities are documented informally.
- Healthcare organisation's risk manager was not involved in the project – the project may have benefited from his/her expertise.

5.3 Opportunities

The opportunities arising from the project include the following:

- Improvements in practice with the review and revision of workflow in relation to ABG analysis.
- Standardisation of analysers in use with associated benefits (ease of use, simplified training, improved traceability & monitoring of clinical end users, Interface to laboratory and clinical information systems with automatic result downloads to the critical care clinical information system, elimination of analysers which are not interfaced (don't download results).
- Provision of staff training ensuring all staff are up to date with current best practice and use of the new analysers.
- Review of practices and procedures related to:
 - Medical IT network modification
 - Clinical Information System configuration changes
 - Interface works
 - Validation (Laboratory & Interface).
 - Risk management aspects of individual roles & record of same

5.4 Threats

The main threats to the completion of the project in the expected timeframe are:

- Availability of Product supplier & Clinical Information System personnel to undertake interface works.
- Availability of personnel to undertake Validation works.
- Availability of CIS Configuration personnel to undertake configuration changes.
- Holiday period during the project affecting availability of relevant personnel.
- Co-ordination of various personnel above to ensure works are completed to enable the contingent works to be undertaken when required.
- Lack of an overall project plan (encompassing all disciplines / tasks etc) could have contributed to project delays / over run.

6.0 Recommendations

- Review and revise workflow in relation to ABG analysis in line with new analyser functions (such as use of scanning of patient and staff identification to input data and reduce errors).
- Review project plan and update to incorporate all major tasks / activities from various personnel / disciplines (include completed tasks and pending tasks with timeframes, and pre-go-Live approval of change).
- Include post Go-Live monitoring in project plan.
- Review of practices and procedures related to Medical IT network modification & implement identified improvements (if applicable).
- Review of practices and procedures related to Clinical Information System configuration changes & implement identified improvements (if applicable).
- Review of practices and procedures related to Interface works & implement identified improvements (if applicable).
- Review of practices and procedures related to Validation (Laboratory & Interface) & implement identified improvements (if applicable).
- Review of practices and procedures related to risk management aspects of individual roles
- Document risk management plan – Record Risk assessments using risk assessment matrix template indicating probability, consequence/impact, control measure(s) for each identified risk, & personnel responsible. Include residual risk acceptance.
- Document a description of risk relevant assets –
 - Software (in analysers, Conworxs, RapidComms),
 - Hardware (analysers, servers, PCs, UPSs),
 - Network
 - Ancillary items.
- The Assessment Tool (Appendix 1) could be useful as a checklist for future projects.
- Document system architecture – components & interfaces showing data transfer.
- Amend the existing change control/release process to address areas highlighted at assessment and include action plan therein.
- Include the change release process in the ICIP policy.
- An installation plan for CONWORXS is required.
- Plan & arrange Pre Go –Live Review – meeting or conference call.
- Plan & arrange Post Go-Live Review – meeting or conference call.
- Distribute Findings report to assessment participants for feedback on recommendations to:
 - determine agreement with recommendations,
 - identify any additional recommendations
 - ascertain if same can be implemented
 - allocate / agree tasks to / with relevant personnel

7.0 Conclusion

It is anticipated that implementation of the recommendations identified will improve risk management activities of this Medical IT Network Project and positively influence future projects.

Findings Report Appendix 1 Assessment Tool - **Assessment Questions & Guidance (See Appendix J)**

Appendix M Revised Question set & Guidance

Assessment Questions & Guidance – Revised. See 7, 8, 28, 29 Additional text highlighted, deleted text shown by strikethrough text

Process Name / Question	Response Type	Guidance
Medical IT Network Risk Management		
Q1 Do you have a Medical IT Network Risk Management File?	Yes/No	Consider whether Medical IT Network Risk Management File contains all relevant risk management information – refer to work products in the PAM. Consider the document management procedure for the file – file access, storage, update back up, version control etc.
Q2 Have risk management resources been assigned?	Yes/No	Consider top management input into risk management process and ensure that the relevant risk management resources are assigned. Resources can include hardware, software and personnel etc.
Q3 Are risk management activities performed according to the risk Management Plan and process?	Yes/No	Consider whether risk management activities are performed during the supervision, operation, installation and maintenance of Medical IT Network(s) throughout the life cycle. Consider whether risk management activities are being performed according to the RM plan and process.
Q4 Are the key properties of the network considered during the performance of risk management activities?	Yes/No	Consider the impact to the network in terms of safety, effectiveness and data and system security throughout the life cycle.
Q5 Are risk management activities documented?	Yes/No	Consider the appropriateness of the approach to documenting risk management activities according to the scope of the medical IT network project.
Risk Analysis & Evaluation		
Q6 How do you identify likely safety hazards for individual devices?	Dialogue	Consideration must be given to the identification of hazards of individual devices when establishing a new medical IT network, adding a device to the IT network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment. Consider the impact of the device activities on the: a) devices and system which are part of the medical IT network b) devices and system

Process Name / Question	Response Type	Guidance
		which are not part of the medical IT network
Q7 How do you analyse the system as a whole to identify likely safety hazards?	Dialogue	<p>Consideration must be given to the identification of hazards of individual devices when establishing a new medical IT network, adding a device to the IT network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment. Consider the impact of the device activities on the system as a whole in terms of: a) devices and system which are part of the medical IT network b) devices and system which are not part of the medical IT network c) overall medical IT-network. [Additional text highlighted]</p>
Q8 How do you consider the impact of the device on the environment, effectiveness, data security & system security?	Dialogue	<p>Consideration must be given to the identification of hazards from individual devices and their impact on the system as a whole when establishing a new medical IT-network, adding a device to the IT-network, changing or modifying a device on the network, performing maintenance activities or removing a device from the network. Hazards in this context are from the perspective of SAFETY - that is causing physical injury to the patient or the user of the device or harm to the environment. Hazards in this context are from the perspective of the ENVIRONMENT - Consider impact to the environment from the perspective of the impact in terms of ceasing or impairing functionality. Hazards in this context are from the perspective of the EFFECTIVENESS - effectiveness of the device is the ability of the device to produce the intended result for the patient and the responsible organisation. Hazards in this context are from the perspective of the DATA & SYSTEM SECURITY. Consider the impact of the individual device activities on the: a) devices and system which are part of the medical IT-network b) devices and system which are not part of the medical IT-network. In Terms of Effectiveness consider the impact of the individual device activities: a) from the perspective of the patient, b) from the perspective of the responsible organisation. In terms of DATA & SYSTEM SECURITY consider the impact of the device activities a) the confidentiality of the data, b) the integrity of the data, c) the availability of the data [Additional text highlighted]</p>

Process Name / Question	Response Type	Guidance
Q9 Do you have a procedure for estimating risk?	Yes/No, Dialogue	What is the treatment of identified risks once they have been identified? Is there a procedure for how the risks are estimated? Is this a documented policy?
Q10 How do you identify possible consequences of harm?	Dialogue	In cases where it is not possible to estimate the probability of occurrence of harm, how do you identify possible consequences of harm? Are consequences documented?
Risk Control		
Q11 Are proposed risk control measures identified for every risk?	Yes/No, Dialogue	Risk control measures should be used in the following order -1) inherent control by design, 2) protective measures, and 3) information for assurance. Consider key properties in the following order - 1) safety, 2) effectiveness, and 3) data and systems security when considering risk control options.
Q12 How are risk control measures considered in relation to the key properties and prioritised?	Dialogue	Risk control measures should be used in the following order -1) inherent control by design, 2) protective measures, and 3) information for assurance. Consider key properties in the following order - 1) safety, 2) effectiveness, and 3) data and systems security when considering risk control options.
Q13 Are selected risk control measures implemented?	Yes/No, Dialogue	Implement selected risk control measures.
Q14 Is the implementation and effectiveness of risk control measures verified and documented?	Yes/No	Verify the implementation and effectiveness of all risk control measures in the operational system and document in the medical IT Network Risk Management File.
Residual Risk		
Q15 Is residual risk reviewed and assessed for acceptability?	Yes/No, Dialogue	Persons responsible for reviewing and accepting residual risk do so in co-operation with the Medical IT Network Risk Manager.
Q16 Is the decision on whether or not to approve the residual risk based on the documented risk/benefit analysis?	Yes/No, Dialogue	Make a decision on whether or not to approve the residual risk on the basis of the documented risk/benefit analysis.
Change Release & Configuration Management		

Process Name / Question	Response Type	Guidance
Q17 Is Configuration Management process documented and applied during the risk management of change release management?	Yes/No, Dialogue	Document configuration management process and apply during the risk management of change release management.
Q18 Is the Change/Release Process documented?	Yes/No	Document and apply change-release management (including Risk Management).
Q19 Are the acceptability of changes determined using the risk management process?	Yes/No	Determine the approval and acceptability of changes using the results of the risk management process during the change-release process.
Q20 Are action plans implemented following the Change/Release Management Process?	Yes/No	Implement action plans following the Change-Release management process. For each change to the medical IT Network, The change Release Process is implemented.
Decision on the application of Risk Management		
Q21 Is the Change-Release Management Process implemented?	Yes/No	Implement the Change-release management process for any new medical IT-Network or a change to an existing medical IT-Network.
Q22 Has the nature of the change been identified?	Yes/No	Consider the nature of the change to decide if the change can be made by an applicable change permit or if a medical IT network project is initiated.
Q23 Has a project plan been established & revised to reflect changes to the project?	Yes/No	Establish project plan for specific circumstances that have the potential to introduce new risk (not covered by change permit). Maintain project plan and revise to reflect changes to the project.
Go-Live		
Q24 Is residual risk reviewed in the context of recent or pending changes prior to go-live?	Yes/No	Review Medical IT Network residual risk summaries for acceptability of risk associated with interactions of recent or pending projects or changes, prior to going live.
Q25 Have the specified changes been approved prior to go-live?	Yes/No	Approval is given for the specified change by the medical IT Network Risk Manager prior to go-live.
Monitoring		

Process Name / Question	Response Type	Guidance
Q26 Has a process for monitoring of the live network been established?	Yes/No, Dialogue	Establish a process which outlines the monitoring requirements as part of the risk management plan to monitor each installed medical IT Network.
Q27 Are requirements for monitoring included in the risk management plan?	Yes/No, Dialogue	Include monitoring requirements as part of the risk management plan. Examples of what to monitor are: a) environment changes (including local/connected environment as well as relevant network or component DATA AND SYSTEMS SECURITY vulnerabilities); b) operational/performance feedback e.g., user feedback, speed problems, high error rates, failure, malicious software attacks; c) information about the incorporated components; d) information about similar MEDICAL IT-NETWORKS; e) reported events; and f) auditing of non-technical RISK CONTROL measures such as organizational policies and procedures.
Event Management		
Q28 Has an event management process been established?	Yes/No, Dialogue	Establish Event Management Process. Establish Event Management process outlining how to ensure that negative events are captured and documented. [Additional text highlighted] [Strike through deleted text]
Q29 Are negative events captured and documented as per event management process? [Additional text highlighted]	Yes/No	Establish Event Management Process. Establish Event Management process to ensure that negative events are captured and documented. [Strike through deleted text] Review negative events documentation record. [Additional text highlighted]
Medical IT Network Planning		
Q30 Has the risk management plan been maintained and updated when a project changes an existing medical IT network?	Yes/No, Dialogue	Risk Management plan is maintained and updated when a project introduces changes to an existing medical IT network.
Medical IT Network Documentation		
Q31 Has additional documentation for the connection of a medical device to an IT network been provided /obtained?	Yes/No, Dialogue	Obtain (Responsible organisation) /Provide (medical device manufacturer) instructions for implementing the connection of a medical device to an IT network.
Q32 Has a risk relevant asset description been maintained?	Yes/No	Maintain risk relevant asset description, including a list of assets of IT networks interfacing with medical devices, as part of the risk management process.

Process Name / Question	Response Type	Guidance
Responsibility Agreements		
Q33 Has the need for a responsibility agreement(s) been determined?	Yes/No	Determine the need for one or more documented responsibility agreements whenever a medical device is incorporated into an IT network or the configuration of such a connection is changed.
Risk Management Policy		
Q34 Has a risk management policy been established?	Yes/No	Risk Management policy outlines criteria for determining acceptable risk, taking into account relevant international standards and national or regional regulations.
Q 35 Does the risk management policy Include description of or reference to processes applying to Medical IT Networks?	Dialogue	Description of or reference to processes applying to Medical IT Networks to include: Event Management, Change - Release Management, Configuration Management & Monitoring.
Organisational Risk Management		
Q 36 Has a risk management process been established and maintained which takes into account the defined use of the medical IT-network?	Dialogue	Establish & maintain Risk Management Process. Establish and maintain a risk management process which takes into account the defined use of the medical IT-network.
Q37 Is the performance of the risk management process reported to Top Management?	Yes/No	Report (made by Medical IT Network Risk Manager) on the performance of the risk management process to Top Management.
General Comments		
Q 38 Any general comments related to assessment?	Dialogue	

Appendix N Recommendations Review Post Go-live

Post assessment medical It-Network modification project relating to installation & networking of new ABG analysers - Recommendations Review 05/06/2014. All complete except No 9 & 14 which are in progress.

	Recommendation	Status/ Comment
1.	Review and revise workflow in relation to ABG analysis in line with new analyser functions (such as use of scanning of patient and staff identification to input data and reduce errors).	Complete
2.	Review project plan and update to incorporate all major tasks / activities from various personnel / disciplines (include completed tasks and pending tasks with timeframes, and pre-go-Live approval of change).	Complete
3.	Include post Go-Live monitoring in project plan.	Complete
4.	Review of practices and procedures related to Medical IT network modification & implement identified improvements (if applicable).	Complete
5.	Review of practices and procedures related to Clinical Information System configuration changes & implement identified improvements (if applicable).	Complete
6.	Review of practices and procedures related to Interface works & implement identified improvements (if applicable).	Complete
7.	Review of practices and procedures related to Validation (Laboratory & Interface) & implement identified improvements (if applicable).	Complete
8.	Review of practices and procedures related to risk management aspects of individual roles.	Complete
9.	Document risk management plan – Record Risk assessments using risk assessment matrix template indicating probability, consequence/impact, and control measure(s) for each identified risk, & personnel responsible. Include residual risk acceptance.	Risk management document was compiled listing risks (pre-analytical, analytical, and post analytical) & control measures for each (Appendix R). Further work is required to include consequence/ impact and personnel responsible.
10.	Document a description of risk relevant assets	Complete
11.	The Assessment Tool could be useful as a checklist for future projects.	Participants agreed to use the checklist in future projects.
12.	Document system architecture – components &	Complete

	interfaces showing data transfer.	
13.	Amend the existing change control/release process to address areas highlighted at assessment and include action plan therein.	Complete
14.	Include the change release process in the ICIP policy.	Policy in progress
15.	An installation plan for CONWORXS is required.	Installation plan received
16.	Plan & arrange Pre Go –Live Review – meeting or conference call.	Pre-Go-Live meeting held
17.	Plan & arrange Post Go-Live Review – meeting or conference call.	Post-Go-Live meetings (X 3) held
18.	Distribute Findings report to assessment participants for feedback on recommendations to:	Findings report distributed
	▪ determine agreement with recommendations,	Agreement confirmed
	▪ identify any additional recommendations	No additional recommendations identified
	▪ ascertain if same can be implemented	Agreement to implement
	▪ allocate / agree tasks to / with relevant personnel	Recommendations accepted by participants for implementation & implemented

Table 14 Review of Implementation of Recommendations Post Go-Live

Appendix O NSAI Acknowledgement of ISO TR 80001-2-7 Comment Review Submission



20/05/2014

To Ms. Lucy Kielty

Dear Lucy,

On behalf of NSAI, I would like to thank you for your very substantial, informed, and constructive contribution to the development of ISO TR 80001-2-7 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.

As you know, commenting on draft standards is the process of adding to and modifying or fine tuning text, in order to ensure a final document is comprehensive, comprehensible, useful and serves the purpose within the scope originally proposed. Your comments represented an invaluable in-depth study of a user of this standard. Such input is rare and difficult to obtain. It is highly valued among standard writers and developers. It is very obvious from your comments that you have a unique insight into the practicalities of using this standard. As it is a very practical Technical Report, it is likely to be used a lot by I.T. managers in hospital settings in the future. Such an input will certainly make the document more useful and usable and will be appreciated by all users.

Your contribution was also very substantial and consisted of approximately 275 comments. When all comments were compiled, these comments were 88% of all comments submitted. This means that your deliberations will contribute to and shape this document before final publication.

I hope that you will continue to engage in the world of developing and contributing to emerging standards. Standards development depends highly on input such as yours. Wherever your future career takes you, I would appreciate your keeping in touch and I look forward to working with you in the future.

Yours Sincerely,

Chrissie Keane

Chrissie Keane
Standards Officer, NSAI

Digitally signed by Chrissie Keane
DN: cn=Chrissie Keane, o=National Standards
Authority of Ireland, ou=Standards
Development, email=chrissie.keane@nsai.ie,
c=IE
Date: 2014.05.20 15:35:27 +01'00'

HEAD OFFICE
1 Swift Square,
Northwood, Santry,
Dublin 9, Ireland
T + 353 1 807 3800
F + 353 1 807 3838
E info@nsai.ie

NSAI.ie



Irish National
Member of ISO



Irish National
Member of CEN

Appendix P Standard Operating Procedure (SOP) RapidPoint 500 POCT ABG Analysis Procedure

An arterial blood sample is used for analysis. In the event that an arterial blood sample is not attainable ensure that there is no force pulling on the vacuum tube when obtaining a venous sample.

Following collection of blood from patient and transportation to the blood gas analyser (BGA) the blood sample must be mixed gently prior to introduction into the system. This is done by rolling the sample between the palms of the hands for 15 seconds. The blood should then be pushed gently up into the tip of the syringe barrel and onto a paper towel. This will ensure that any small fibrin clot or air bubble will be expelled onto the paper towel.

1. Ensure that the status message in the top left corner indicates "Ready" and all parameters required are available for use.
2. Select the sample type on the left-hand list (Default is syringe of arterial blood).
3. Insert the syringe into the sample port.
4. Press the 'start' button.
5. Remove the sample when prompted and press the 'continue' arrow button.
6. Enter the patient demographics. These fields are mandatory and must be completed. MRN, Surname, First Name. Optional entries include FiO2 and Temperature.
7. Check all information is correct before proceeding by pressing the 'continue' arrow.
8. When the analysis is complete the results will be printed
9. Press the 'continue' button when done.

ST. JAMES'S HOSPITAL LABMED DIRECTORATE			
Edition No.:	00	Biochemistry Department	Doc No: LP-POC-0018
Author: Brian Murray		Date: 30/12/13	Date of issue: 30/12/13
Authorised By: Felicity Dempsey		Date: 30/12/13	

Reissued By/Date: _____
(Only to be used if there are no modifications at review)

Standard Operating Procedure (SOP) RapidPoint 500 POCT ABG Analysis (Extract page 8)

Appendix Q SWOT Analysis Tables

Appendix Q.1 SWOT Analysis - Strengths

Strengths (requirements of the Standard IEC 80001-1 which were met are Included)

1. Risk management resources are in place (though informally)
2. Involvement of multiple diverse stakeholders (all relevant disciplines involved)
3. Many of the stakeholders involved work or have worked together previously which facilitated better engagement in the project.
4. Contribution of stakeholder's combined extensive expertise, knowledge, experience & skills to the project.
5. Identification of potential problems & safety hazards and planning for same was based on project member's prior experience.
6. Change release processes were followed.
7. Negative events are captured and documented as required.
8. Biological & chemical risk assessments in terms of safety hazards were undertaken & documented.
9. There are IT standards in place e.g. security standards that must be complied with before items are added to the medical IT-network.
10. Risks were identified:
 - Data download failure
 - User picks incorrect MRN or manual data entry error
 - User fails to mark sample as venous
 - Risk of transcription error in event of failed download due to power issues
 - Results are only available in ICU, they aren't available outside ICU
11. Risk control measures were identified:
 - Transcription of the test result in the event of a download failure
 - Audit of MRN-mismatches & feedback of results to raise awareness of error rates
 - Training to reduce errors

- Scan of patient & staff ID to reduce errors of data entry
 - Use of Bar-coded syringes when available is being considered
 - Provision of access to results via EPR in areas outside ICU is being considered
12. Regular (monthly) audits of incorrect MRNs (one of the identified risks) are undertaken by POCT personnel and the results are fed back to relevant personnel.
 13. The nature of the change was identified – project
 14. An event management process is in use.
 15. An installation plan for connection of the analysers to the network was provided by the manufacturer.
 16. The project leader/manager was identified and the role responsibilities were clarified.
 17. The need for a responsibility agreement was previously determined.
 18. The risk management process includes a corporate risk register which is given to the board quarterly.
 19. The project leader reported that risk management activities are documented.

Table 15 SWOT Analysis - Strengths

Appendix Q.2 SWOT Analysis – Weaknesses

SWOT Analysis - Weaknesses

1. Assessment participants suggested that it would have been highly beneficial to have had the assessment at the start of the project which would have informed personnel of the standard requirements and increased the likelihood of meeting these requirements.
2. Separate project plans for components of the project related to different disciplines / personnel reduced overall project transparency in terms of the project tasks / deliverables and timeframes for same.
3. Prior to the assessment there was a lack of clarity on who was the project leader and the roles and responsibilities of the project leader.
4. As many participants worked / work together previously this resulted in informal communication in lieu of more formal communication regarding the project at times.
5. There is no Medical IT-network Risk Manager or Medical IT-network Risk Management File for this network modification project (requirements of IEC 80001-1 standard).
6. There is no formal risk management plan & process (requirements of IEC 80001-1 standard).
7. Risk management processes were not addressed in a formal manner, although risk management templates such as risk assessment matrix are available from the organisation's risk manager, many participants were unaware of availability of same and hence they were not used.
8. Risk management activities are documented informally – meeting minutes.
9. Healthcare organisation's risk manager was not involved in the project – the project may have benefited from his/her expertise.

Table 16 SWOT Analysis – Weaknesses

Appendix Q.3 SWOT Analysis – Opportunities

SWOT Analysis - Opportunities

1. Improvements in practice with the review and revision of workflow in relation to ABG analysis.
2. Standardisation of analysers in use with associated benefits (ease of use, simplified training, improved traceability & monitoring of clinical end users, Interface to laboratory and clinical information systems with automatic result downloads to the ICU clinical information system, elimination of analysers which are not interfaced (don't download results).
3. Provision of staff training ensuring all staff are up to date with current best practice and use of the new analysers.
4. Review of practices and procedures related to:
 - Medical IT-network modification
 - Clinical Information System configuration changes
 - Interface works
 - Validation (Laboratory & Interface).
 - Risk management aspects of individual roles & record of same

Table 17 SWOT Analysis – Opportunities

Appendix Q.4 SWOT Analysis - Threats

SWOT Analysis - Threats

1. Availability of Product supplier & CIS personnel to undertake interface works.
2. Availability of personnel to undertake Validation works.
3. Availability of CIS Configuration personnel to undertake configuration changes.
4. Holiday period during the project affecting availability of relevant personnel.
5. Co-ordination of various personnel above to ensure works are completed to enable the contingent works to be undertaken when required.
6. Lack of an overall project plan (encompassing all disciplines / tasks etc) could have contributed to project delays / over run.

Table 18 SWOT Analysis - Threats

Appendix R Hazards & Potential Problems (POCT ABG Analysis)

Pre-analytical, Analytical & Post analytical Problems are outlined below.

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Pre analytical				
Poor Sampling Technique	Aortic area may not be cleaned. Flush may not be discarded from arterial line. If using stab sample vein may be stabbed instead of artery. Insufficient sample may be obtained. Poor technique may lead to clots /air forming in sample.	Guidelines/protocol for arterial sampling available.; Guidelines for Arterial Stab technique available	ORIAN Guideline no 032. ?Competency document for Arterial Sampling. ?Competency document for Arterial Stab Sampling.	Residual Risk of Human Error
Incorrect patient may be identified for sampling, Poor compliance with labelling	Sample not labelled at all or incorrectly	Poster re labelling at analysers. Labelling issues constantly highlighted and discussed at POCT Meetings.		Sample should be labelled with 2 identifiers. Pre Bar coded syringes which can be scanned along with the Operator ID, & Patient MRN at the analyser will be available this year.
Multiple samples may be taken for analysis at the one time	Mix up in MRN's if each sample is not labelled correctly.	Single sampling only should be practised.		This improvement should be audited for compliance
Operator Training	Operator may not be trained and may use another operator's password for the analysers.	Operators lock out on analyser in place. Importance of this procedure covered in training. All operators are trained before their password is enabled on the analyser.	LP-POC-0018;Competency Testing on the Blood Gas Analyser Edition 01 Password Management and downloads from RapidComm	

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Pre analytical				
Delays in transport to analyser		Covered in training.	LP-POC-0018;Competency Testing on the Blood Gas Analyser Edition 01	
			EX-POC-055; Minimising Pre Analytical Errors in Blood Gas Sampling EX-POC-005 Transport/Handling of Blood Gas Samples	This document could be posted on SJH Intra Net
Preparation of sample at analyser pre analysis, mixing/expelling air/clots.		Covered in Training.	LP-POC-0018;Competency Testing on the Blood Gas Analyser Edition 01	
Patient Data entry at Analyser prone to error. Incorrect entry of patient data could occur. Result may go to wrong patient record.		Analyser has mandatory entry for Patient ID. Operator ID, Temp, FIO2.This information can be scanned or entered manually	LP-POC-0018;Competency Testing on the Blood Gas Analyser Edition 01 EX-POC-055; Minimising Pre Analytical Errors in Blood Gas Sampling	All information should be scanned. If ID cards do not scan contact security for new card. LIS connection will improve this step
Instructions for use available?		SOP available in Equipment Log Book at Analyser. Working instructions available on wall at each analyser.	LP-POPC-0018; Operation of the RapidPoint 500 Blood Gas Analyser WI-POC-0025; Blood Gas Analysis on the RapidPoint 500	Working instructions will be edited to include simple troubleshooting techniques and transport /delay times for a viable sample result.

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Analytical				
Analyser out of action, (1) QC or Cal out of specification. (2) All, parameters not available	Unable to analyse sample. Results not available for all parameters	There are 9 Blood Gas Analysers in the hospital .All operators have access to all Blood Gas Analyser in the hospital. All Biochemistry On Call staff are trained in basic trouble shooting techniques. (1)QC and Cal lock out in place on analyser (2)Parameter fail on QC or Cal is locked out to ensure accuracy of results. Daily monitoring recorded on RapidComm by POCT Team	LP-POC-0018 Operation of the RapidPoint 500 Blood Gas Analyser	
Measurement Cartridges could be empty or expired.	Unable to analyse sample	POCT Scientist maintains stock control, batch acceptance. Spare cartridge kept in all fridges located at Blood Gas Analysers. Main stock kept in Biochemistry Fridge 79-BIO-003. Stock Check is part of Daily Monitoring recorded on RapidComm by POCT Team.	LF-POC-0008 Phase 1C POCT Stock Sheet	
Measurement Cartridge could be incorrectly stored.	Potential incorrect results.	Temperature Monitoring in place in Biochemistry Fridge/room areas. Air Conditioning in place in some areas.	TBD	Temperature Monitoring to be put in place in local areas of Analysers
Analyser not ready due to calibration running.	Unable to analyse sample	Stat mode available. Cal can be interrupted.		
Chemical Risk from Measuring Cartridges	Harm to users	Safety data sheets available in Equipment Folder. Risk assessments carried out by POCT Scientist. Risk instructions available in Equipment Folder.	RA-POC-C011; POCT Chemical Risk Assessment for Virkon. RA-POC-013;R500 Auto QC Cartridge, RA-POC-C014;R500 Wash/Waste Cartridge,RI-POC -011; Risk Instruction for POCT Analyser.	

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Analytical				
Biological Risk from blood	Harm to users	Safety data sheets available in Equipment Folder. Risk assessments carried out by POCT Scientist. Risk instructions available in Equipment Folder.	RA-POC-B013; POCT Biological Hazards RI-POC -011; Risk Instruction for the use of the POCT Blood Gas Analyser EX-POC-005 Transport/Handling of Blood Gas Samples	
Environmental Risk	Harm to users	Safety data sheets available in Equipment Folder. Risk assessments carried out by POCT Scientist. Risk instructions available in Equipment Folder.	RA-POC-018; General Risk Assessment for the ED blood gas analyser. RA-POC-019; General Risk Assessment for the KSICU blood gas analyser. RA-POC-020; General Risk Assessment for the ICU blood gas analyser. RA-POC-021; General Risk Assessment for the JH blood gas analyser. RA-POC-022; General Risk Assessment for the Theatre blood gas analyser. RA-POC-023; General Risk Assessment for Room CPL 46A RI-POC -011; Risk Instruction for the use of the POCT Blood Gas Analyser. REF-GEN-0007 Safety, Health and Welfare at Work Act 2005 SJH COR (P) 014; Health and Safety Statement	

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Post Analytical				
Print out not available Paper out. If ICIP/EPR/LIS is down paper result is necessary.	If LIS/EPR/ICIP is down print out is necessary.	POCT Scientist maintains stock control, batch acceptance. Spare paper kept in all presses located at Blood Gas Analysers. Main stock kept in Biochemistry Room 46A. Stock Check is part of Daily Monitoring recorded on RapidComm by POCT Team.	LF-POC-0008 Phase 1C POCT Stock Sheet	BG results on EPR.
Result printout must be distinguishable from main lab results in charts etc.	Mix up of results from Lab and BG analysers possible	Printout is headed with the serial no of the analyser and location. Results on ICIP are clearly marked from the Blood Gas Analyser. Report of all results to RapidComm also which can be printed if necessary		Audit of results going correctly to RapidComm / Conworxs / ICIP should be put in place quarterly.
Transcription of results from print out when ICIP/Network is down	Errors in data entry	None		Recommend results be entered into chart by 2 staff members, both of whom should sign off.
Verification of result.		Results may for a number of reasons not go into the right patients chart mainly due to pre analytical errors.	EX-POC-055; Minimising Pre Analytical Errors in Blood Gas Sampling	If results are not what is expected or there is any suspicion of error about a result the sample must be repeated and if necessary alert the ICIP team if applicable /requesting doctor / POCT Scientist

Risk Event	Risk	Risk Management in place.	Associated Documents if available	Further Risk Prevention desirable
Post Analytical				
Interpretation of results				Results should be interpreted in the light of the patient's clinical details, previous results, treatment. Any queries should be directed to the POCT Scientist.
Download delay or failure	If patient details were entered incorrectly previously results are held in RapidComms until verified	Daily monitoring of result downloads to ICIP to identify any manual entries or deleted entries x 8 weeks and perform root cause analysis	Spread sheet of errors identified & resultant actions/ resolution, risk forms completed & followed up for each event.	Monitoring thereafter to be done monthly by ICIP team.
	Network failure – manual entry of result in ICIP	Users to report any failed downloads to POCT / ICIP Team		
	Server connectivity loss	Password set to never expire, Monitoring in place		
Download to incorrect chart in ICIP	Incorrect treatment based on erroneous result	Users instructed to verify result and repeat if there is any doubt that the result is belonging to the patient		Users instructed to report to POCT / ICIP & complete risk form. Errors can be corrected on the analyser & EPR by POCT team & on ICIP by ICIP team.

Table 19 Hazards & Potential Problems with POCT ABG Analysis

Appendix S IEC 80001-1 Focus Group Assessment Transcript (see enclosed CD)

Appendix T Questionnaire Question 12 Additional Comments

Q12 Do you have any additional comments or suggestions?

- Comment 1 There was overlap in many of the questions, documentation is present but not in the format required by the standard (Participant 3)
- Comment 2 Got a very good understanding of the standard & will be more aware & confident to use the standard in the next project of a similar nature (Participant 4)
- Comment 3 Very interesting & informative process, Thank You (Participant 6)
- Comment 4 No Comment (Participant 7)
- Comment 5 The questions were thought provoking & it seems that while the formal structures / documents were not in place, everyone was involved / aware of the risks, managed risk & consequences of the risk. I learned that there is always an acceptable level of risk with every process (Participant 10)
- Comment 6 The assessment was useful in the formal review of what happens to some degree in an informal way already. The challenge will be to deal with the standard and how to apply same in a formal way without being caught up too much in the various recording and documentation requirements in an already stretched working environment (Participant 11)

Table 20 Additional Comments or suggestions

Appendix U Recommendations from Findings Report

Recommendations from Assessment Findings Report

1. Review and revise workflow in relation to ABG analysis in line with new analyser functions (such as use of scanning of patient and staff identification to input data and reduce errors).
2. Review project plan and update to incorporate all major tasks / activities from various personnel / disciplines (include completed tasks and pending tasks with timeframes, and pre-go-Live approval of change).
3. Include post Go-Live monitoring in project plan.
4. Review of practices and procedures related to Medical IT-network modification & implement identified improvements (if applicable).
5. Review of practices and procedures related to Clinical Information System configuration changes & implement identified improvements (if applicable).
6. Review of practices and procedures related to Interface works & implement identified improvements (if applicable).
7. Review of practices and procedures related to validation (Laboratory & Interface) & implement identified improvements (if applicable).
8. Review of practices and procedures related to risk management aspects of individual roles.
9. Document risk management plan – Record Risk assessments using risk assessment matrix template indicating probability, consequence/impact, control measure(s) for each identified risk, & personnel responsible. Include residual risk acceptance.
10. Document a description of risk relevant assets:
 - Software (in analysers, Conworxs*, RapidComms**),
 - Hardware (analysers, servers, PCs, UPSs***),
 - Network
 - Ancillary items.
11. The Assessment Tool (Appendix J) could be useful as a checklist for future

projects.

12. Document system architecture – components & interfaces showing data transfer.
13. Amend the existing change control/release process to address areas highlighted at assessment and include action plan therein.
14. Include the change release process in the ICIP [Intellivue Clinical Information Portfolio the CIS in use at the study site] policy.
15. An installation plan for CONWORXS* is required.
16. Plan & arrange Pre Go –Live Review – meeting or conference call.
17. Plan & arrange Post Go-Live Review – meeting or conference call.
18. Distribute Findings report to assessment participants for feedback on recommendations to:
 - determine agreement with recommendations,
 - identify any additional recommendations
 - ascertain if same can be implemented
 - allocate / agree tasks to / with relevant personnel

Table 21 Recommendations from Assessment Findings Report

Note 1: *Conworxs is the company that supplies the data manager integration engine called Poccelerator (a component of the POCT analyser network configuration) that has the capability to include all POCT devices and link them to the laboratory system / patient administration system at the study site.

Note 2: **RapidComms is the software in the networked POCT analysers that interacts with Poccelerator.

Note 3: ***UPSs – uninterrupted power supplies used to maintain power to critical systems in the event of a power outage.

Appendix V Allocation of Recommendations from Findings Report

Allocation of Recommendations among the Interviewees	
Role of Participant	Q4 Which Recommendations will you take ownership of?
Clinical user	1, 3, 5, 8, 9, 11, 14, 16, 17, 18
Laboratory IT	2, 4, 6, 8, 9, 11, 12, 14, 15, 16, 17, 18
Project Leader/ POCT	1, 2, 3, 7, 8, 9, 10, 11, 15, 16, 17, 18
CIS Configurator	1, 3, 4, 5, 6, 8, 9, 11, 14, 16, 17, 18
Medical Device (POCT) Supplier	9, 15, 16, 17, 18
Clinical Engineering	1, 3, 4, 7, 8, 11, 14, 16, 17, 18
Another team member (POCT)	13

Other project team members were also identified as being involved in implementation of many of the recommendations.

Table 22 Which recommendations will you take ownership of?