

Contraction the IRISH SOFTWARE RESEARCH CENTRE

Risk Management of Health Information Technology Systems: Lessons Learned through the Lifecycle of Standards Dr Silvana Togneri Mac Mahon















Overview

- Risk Management of Health Information Technology Systems
- Evolution of Standards
 - IEC 80001-1
 - ISO TR 80001-2-7
 - Revision of IEC 80001-1
- Lessons Learned Developing and Implementing Standards, Landscape and Foundations
- Conclusion



Risk Management of Health Information Technology Systems -Background

- The increased prevalence of chronic disease combined with an ageing population has presented a major challenge for healthcare systems and has changes the way in which healthcare is provided
- The provision of care has moved away from acute episodic periods of care to a longer ongoing relationship between patients and care givers
- This relationship is increasingly being supported through the use of IT and in particular through the use of Health Information Technology Systems (HITS)
- Risk Management Standards are responding to changing use of technology in Healthcare



3

Risk Management of Health Information Technology Systems -Standards

- Increasingly, medical devices are being designed to exchange electronic information with other devices, including medical devices.
- Traditionally, when a medical device was designed to be incorporated into a network, the provider of the device would also provide the network.
- To achieve full interoperability, medical devices are increasingly being incorporated into a healthcare provider's general IT network which can introduce additional risks.
- IEC 80001-1: 2010 Application of risk management for ITnetworks incorporating medical devices was developed to address these risks



4

IEC 80001-1 Overview



🗘 Lero

01/06/2022

Medical IT Network Risk Management

IEC 80001-1: 2010 Risk Management of IT Networks



IEC 80001-1: Impact?

- Adoption of the standard was low
 - HDOs vary in size and in the capability of their risk management processes and provide care in different regulatory environments
 - Effective risk management activities require interaction between different stakeholder groups
 - HDOs may be unprepared for the organisational changes that are required to facilitate this level of interaction among stakeholders who typically operate in silos.
 - This highlighted the need for an assessment framework providing HDOs with a flexible approach to assessing the capability of their current risk management processes relating to medical IT networks
 - Maybe some guidance was needed?......



Medical IT Network Risk Management





01/06/2022

ISO/TR 80001-2-7 Components





Addressing the Barriers to Adoption? – Action Design Research





Impact of Implementation*:

- Promoted understanding of the role of risk management stakeholders
- Common terminology and understanding of risk
- Improved documentation of risk management policy and process
- Raised awareness of the need for groups within the hospital to come together and address risk-related issues specific to network technology management

*Hegarty, F.J., MacMahon, S.T., Byrne, P. and McCaffery, F., 2014. Assessing a hospital's medical IT network risk management practice with 80001-1. *Biomedical instrumentation & technology*, *48*(1), pp.64-71.



Medical IT Network Risk Management





01/06/2022

Revision of IEC 80001-1: Revised Scope

IEC 80001-1 (2nd Ed), safety, effectiveness and security in the implementation and use of connected medical devices or connected health software.

This international standard provides general requirements for applying risk management to Health Information Technology (HIT) systems by addressing the key properties of safety, effectiveness and both data and system security (including privacy) while engaging appropriate stakeholders."



Revision of IEC 80001-1: Impact of Lessons Learned from Implementation

- Lack of Drivers to Motivate Top Management
- > HDO Organisational Challenges: IT and BME not aligned
- > 80001-1 standard is too complicated and complex to implement



High Level Initial Mapping – Annex SL to ISO TR 80001-2-7

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

🗘 Lero

01/06/2022

Lessons Learned - Revisited

- Lack of Drivers to Motivate Top Management
 - Certification, Knowledge of ISO 9001, Integration with existing processes
- > HDO Organisational Challenges: IT and BME not aligned
 - Common Language , Adoption of ISO 9001, Reference to TRs
- > 80001-1 standard is too complicated and complex to implement
 - Context, Organisational Maturity, Simplified Structure



Safe Health Software and Safe Health IT Systems **Design, Implementation & Clinical Use Design & Development Implementation & Clinical Use** (Responsibility of the Developer) (Responsibility of Health Service Organization) Implementation, Workflow Optimization, and Training Integration, Data Migration, Transition, and Validation Compliance) Installation, Customization, and Configuration Software Production, Release & Maintenance Testing, Verification, and Documentation **Concepts and Requirements Definition T** Systems Operation & Maintenance **Decommissioning and Disposal** Procurement (Including Manufacturer Development Design Foundation – Principles, Concepts & Definitions Organizational Culture, Roles & System and Software Lifecycle IT & IM Governance **Risk Management** Competencies Processes Safety Management Processes Human Factors, Usability & **Privacy & Security Quality Management** Across Software Lifecycle **Change Management** Management

Contract Lero

Revision of IEC 80001-1: Summary

- ► IEC 80001-1* has been revised:
 - With an extended scope
 - As a process standards to allow for capability of processes to be assesses and facilitate a stepwise approach to implementation
 - To facilitate greater integration with existing risk management standards
 - In closer alignment with management system standards Annex SL

*IEC 80001-1:2021 APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES — PART 1: SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE



Conclusion

- While IEC 80001-1:2010 assisted HDOs in managing the risk associated with placing a device onto an IT network, the standard was complex and difficult to implement
- To address this ISO/TR 80001-2-7 was developed and based on the experience of implementing the TR, IEC 80001-1 has been revised as a process standard within the "Temple"
- Using ADR or similar methodologies allows for authentic evaluation of standards during the development process aids implementation and fosters adoption – have your say!



20



Thank You! silvana.macmahon@dcu.ie

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094_2 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie)









European Union European Regional Development Fund