BMJ Health & Care Informatics

IT risk management for medical devices in hospital IT networks: a catalogue of measures and indicators

Stefan Richter , Elske Ammenwerth

To cite: Richter S, Ammenwerth E. IT risk management for medical devices in hospital IT networks: a catalogue of measures and indicators. *BMJ Health Care Inform* 2023;**30**:e100639. doi:10.1136/bmjhci-2022-100639

Received 04 July 2022
Accepted 07 January 2023

Institute of Medical Informatics, UMIT TIROL - Private University for Health Sciences and Health Technology, Hall in Tirol, Austria

Correspondence to
Dr Stefan Richter;
stefan.richter@umit-tirol.at

ABSTRACT

Objectives Connecting medical devices to hospital IT networks can create threats that must be covered by IT risk management. In practice, implementing such risk management is not trivial because the IEC 80001-1, as the existing state-of-the-art, do not describe sufficiently concrete implementation measures or evaluation indicators. The aim of the present work was to develop and evaluate a catalogue of measures and indicators to help hospitals implement and evaluate risk management in accordance with IEC 80001-1.

Methods We conducted a Delphi study with 22 experts. In the first round, we performed interviews to identify implementation measures and evaluation indicators using qualitative content analysis. In the second round, a quantitative experts' survey confirmed the results of the first survey round and identified relationships between the measures and indicators. Based on these results, we then developed a catalogue containing the identified measures and indicators. Finally, we performed a case study to verify the practicability of this catalogue.

Results We developed and verified a catalogue of 49 measures and 18 indicators to help hospitals implement and evaluate risk management following IEC 80001-1. The case study confirmed the practicability of the catalogue.

Discussion Compared with IEC 80001-1, our catalogue goes into further detail to offer hospitals a stepwise implementation and evaluation approach. However, the catalogue must be tested in further case studies and evaluated in terms of generalisation.

Conclusions The catalogue will enable hospitals to overcome recent difficulties in implementing and evaluating IT risk management for medical devices according to IEC 80001-1.

WHAT IS ALREADY KNOWN ON THIS TOPIC

⇒ Before this study, there was little research on how to implement and evaluate IT risk management for medical devices connected to IT networks. The IEC 80001-1 standard existed, but a problem in practice was that no practical knowledge existed on how to implement the standard effectively and efficiently.

WHAT THIS STUDY ADDS

⇒ Our study provides a catalogue of 49 measures and 18 indicators to help hospitals implement and evaluate risk management for medical devices connected to a hospital IT network.

HOW THIS STUDY MIGHT AFFECT RESEARCH, PRACTICE OR POLICY

⇒ For IT risk managers in hospitals, the catalogue that we have developed enables a specific and step-by-step implementation and evaluation of IT risk management for medical devices connected to hospital IT networks.

INTRODUCTION

More and more processes in modern healthcare are digitalised. Looking at current trends (eg, telemedicine, artificial intelligence, medical apps), this level of digitalisation will continue to increase in the coming years. Digitalisation also affects medical technology. Today's medical devices are designed to exchange data with other medical devices and clinical information systems. Incorporating medical devices into hospital IT networks is therefore essential as it contributes to the effectiveness of clinical processes and safe patient care.[1 2]

However, digitalisation and the networking of medical devices can pose new risks that could jeopardise the effectiveness of clinical processes or patient safety.[3 4] Technical failures, unauthorised actions, compromised information or functions, deliberate actions or organisational failures, among other things, are fundamental threats to be aware of when integrating medical devices into hospital IT networks. For this reason, hospitals need to establish specific IT risk management procedures for medical devices to deal with these potential IT threats.[5–7]

Numerous standards[8 9] and scientific works[10] exist for IT risk management. IEC 81001-5-1[11] defines security activities in the product life cycle for health software and health IT systems and is therefore primarily intended for developers. IEC 80001-1 and the associated technical reports represent the current state of the art for risk management to control hazards that may arise from

incorporating medical devices into IT networks. The standard, which is mainly intended for operators of medical IT networks (eg, hospitals), was initially published in 2010[12] and updated with a second edition in 2021.[13] IEC 80001-1 has also been adopted as a European standard and in various national standards (eg, DIN EN 80001-1:2011 for Germany).

However, implementing IEC 80001-1s is not trivial.[5] First, risk managers face the practical problem that IEC 80001-1 is often considered too complicated and too complex to implement.[14–16] One reason for its complexity is that the standard does not describe any concrete implementation measures. Even the associated technical reports (eg, IEC/TR 80001-2-1:2012 or ISO/TR 80001-2-7:2015) and the 2021 edition of IEC 80001-1[13] do not solve this problem. Compared with the first version of IEC 80001-1 from 2010, the current version from 2021 formulates more concrete implementation recommendations. This is achieved primarily through the more detailed requirement descriptions in Annex A (IEC 80001-1 requirements mapping table) and B (Guidance for accompanying document Information). The complexity in the practical implementation is thereby reduced, but not completely eliminated. IEC/TR 80001-2-1 focuses on 10 steps to help in the application of risk management. Still, it does not provide a full outline or explanation of all requirements covered by IEC 80001-1 (eg, organisational aspects). IEC/TR 80001-2-7 provides guidance for hospitals to self-assess their conformance with IEC 80001-1, but it does not introduce any requirements in addition to those expressed in IEC 80001-1 (eg, priority of requirements, critical success factors). Another factor in German-speaking countries is that risk management is often based only on the translated national standards of IEC 80001-1. The national standards are still based on the first, superseded version of IEC 80001-1 (eg, DIN EN 80001-1:2011 in Germany), and most of the associated technical reports are not even available in German. Second, the standards do not define the importance and practicability of the different steps that help apply IEC 80001-1. In addition, the specific interpretation and implementation of the requirements described in general in IEC 80001-1 vary depending on the region in which the hospital is located and relevant regulatory requirements.[16] Third, the standards do not describe specific methods to evaluate the achievement of the intended effects of IT risk management. The intended effects on information security, the effectiveness of processes and the safety of patients are generally assumed but not systematically reviewed. Therefore, the effectiveness of IEC 80001-1 with regard to contemporary cybersecurity is unknown.[17] The lack of methods for evaluating and reviewing the correctness and efficacy is often observed in health and medical informatics and is described as a general problem.[18]

Some non-scientific guidelines[19] and a few scientific papers[16] have tried to address the aforementioned difficulties in the implementation of IEC 80001-1. In comparison to these approaches, we wanted to go into further detail in order to offer hospitals a kind of 'cookbook' for IEC 80001-1 implementation and evaluation.

Therefore, the present work aimed to develop and verify a catalogue of measures to help hospitals implement risk management in accordance with IEC 80001-1. The catalogue should also provide indicators that allow hospitals to evaluate the impact of the implemented measures. It should also describe implementation measures and indicators in as much detail as possible, explaining the importance of each measure and indicator as well as the resources (technical, organisational, financial) that should be expected for their implementation. Finally, the catalogue should consider the abovementioned challenges of implementing IEC 80001–1 in German-speaking countries.

METHODS

Approach

IT risk management, in general, can mainly be assigned to the technical sciences, information sciences and economics. Quantitative and qualitative research methods have been established in these scientific disciplines. Since we aimed to identify measures and indicators essential for implementing and evaluating risk management according to IEC 80001-1, observations, experiences and interpretations of experts are especially important. So, we identified an expert survey in the form of a Delphi study, where qualitative and quantitative methods should be combined, as a suitable methodology. Therefore, we conducted a study consisting of three research steps (see figure 1). In the first two research steps, we used the Delphi technique to gather the collective opinion of experts through a systematic and multistage process. In the first research step, we interviewed experts to develop a catalogue with the desired measures and indicators. We interviewed the experts again in the second research step to reach a consensus on which measures and indicators should be included in the catalogue in the end. In the third step, we evaluated the catalogue for practicability in a case study with the help of additional experts.

1st research step: development of a catalogue of measures and indicators

In the first step of the Delphi study, we conducted 2 qualitative oral interviews and 20 qualitative written interviews with experts on health IT and medical devices. This first research step aimed to develop a catalogue of measures and indicators for implementing and evaluating IT risk management for medical devices connected to a hospital IT network.

We invited professionals with several years of professional and practical experience in IT security, medical technology and medical informatics to be our experts. We contacted approximately 50 experts personally via telephone, email or located them via social media to invite them to our study.

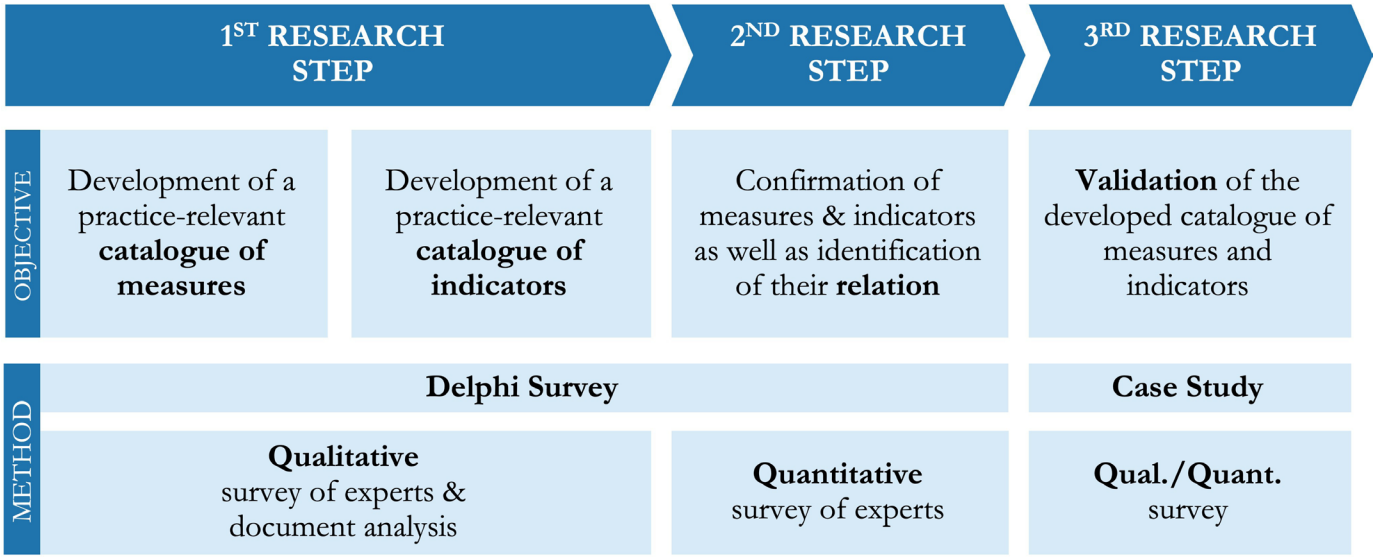

Figure 1 The three research steps with their objectives and methods.

Initially, only oral interviews were planned, but most participants wished for a fully anonymous written interview. Two interviews were therefore conducted orally and 20 interviews in written form. The interviews included 10 open questions on personal views, opinions and experiences regarding the threats posed by operating medical devices in hospital IT networks.

All interviews were analysed using structured qualitative content analysis, according to Mayring.[20] The 22 data sets were coded according to the two main categories of 'measures' and 'indicators'. Within these main categories, further subgroups were formed. In addition, relevant documents (standards, laws and reports) named by the interview partners were analysed using qualitative content analysis.

2nd research step: confirmation of measures and indicators and their relationships

A total of 13 experts from the first research step declared their willingness to continue their participation. So, a quantitative study of 13 experts was conducted as a second research step to confirm the results of the first survey round and to identify the relationships between the identified measures and indicators.

This survey was conducted online, and the response was 100%. The survey comprised 20 closed questions divided into three sections: First, the experts had to rate the measures from the first survey round on a four-point scale between '1=no importance at all' and '4=very high importance'. Second, the experts had to rate the indicators from the first survey round. Measures and indicators were classified as 'important' and included in the catalogue if the mean rating of all experts for a given measure or indicator was 2.5 or higher (given a range from 1 to 4); they were rated as 'very important' if the mean rating was 3.25 or higher. In the catalogue, these findings were represented in the criteria 'priority'. The important measures and indicators are marked with a single star symbol, and the 'very important' measures and indicators are with two stars. Third, the experts had to rate the possible relationship between groups of measures and groups of indicators on a five-point scale (see figure 2). The groupings were predefined and based on the researcher's assumptions, prior knowledge and practical experience. A relationship was rated as 'confirmed' if the mean rating of all experts was 2.5 or higher.

3rd research step: validation of measures and indicators in a case study

We conducted a case study to validate the catalogue of measures and indicators developed in the earlier steps. The case study was conducted in an Austrian hospital with

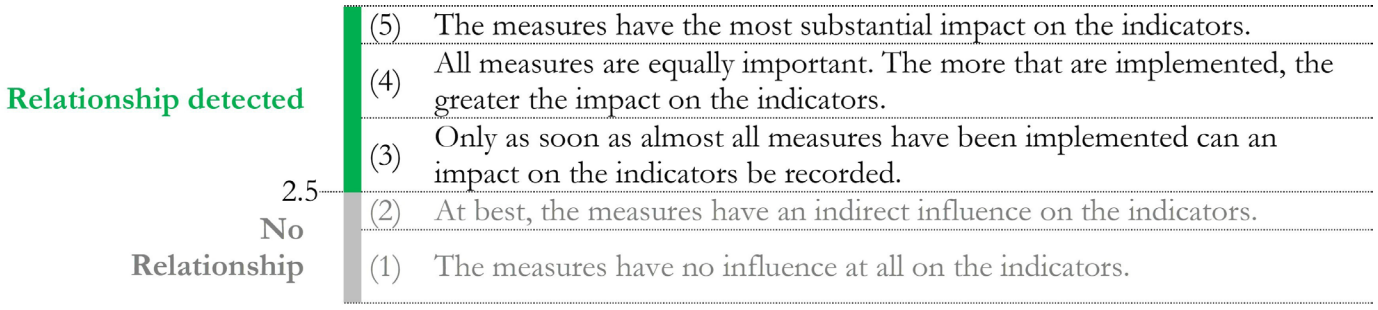

Figure 2 The scale for assessing the relationship between measures and indicators.

Table 1 The three criteria (including questions) for evaluation of the catalogue

Factor	Question	Rating
Effectiveness	Was it possible to implement a selected measure or indicator?	Binary Rating Scale (yes, no)
Complexity	How complex was the implementation of a given measure or indicator?	Three-part rating scale (low, moderate, high)
Satisfaction	How satisfied were the users with the descriptions and instructions for a given measure or indicator?	Binary Rating Scale (satisfied, not satisfied)

325 beds. The hospital had 17 medical devices integrated into its IT network but did not yet have risk management according to IEC 80001-1. The case study was conducted over 3 months.

The case study aimed to implement and evaluate the catalogue. Three health IT staff members at the hospital (head of IT, head of medical technology and an IT project manager) were asked to implement measures and indicators by following the implementation recommendations in the catalogue. Inspired by ISO 9241-11, which provides a framework for usability testing, we developed a written survey to evaluate the effectiveness, complexity and satisfaction of each implementation recommendation (see table 1). After implementing a measure or indicator, the three health staff IT members had to evaluate the implementation recommendation using these written surveys.

In addition to the written questionnaires, we performed an oral group interview with the three health IT staff members at the end of the case study. This guided group interview also aimed to validate effectiveness, efficiency and satisfaction; compared with the written questionnaires, however, the interview focused on the catalogue in general. The findings of the survey were incorporated into the results of the written survey by assigning them to the corresponding evaluation criteria of a specific measure or indicator. Knowledge about the complexity of implementing a measure or indicator was to be integrated into the catalogue; a traffic light symbol was therefore chosen to visualise the level of complexity (red=high complexity, orange=moderate complexity, green=low complexity).

RESULTS

Development of the catalogue of measures and indicators (research steps #1 and #2)

We used qualitative content analysis to code 723 units in the qualitative expert interviews. We identified 51 measures and 19 indicators in the first research step through abstraction, summarisation and elimination of duplicates. The experts confirmed these results in the second research step except for one single indicator and two measures.

The resulting 49 measures were categorised into six subgroups (see table 2). With these measures in place, including detailed implementation information for each measure (see figure 3), hospital IT risk managers should be able to implement IT risk management according to IEC 80001-1.

The resulting 18 indicators were categorised into four subgroups (see table 3). With these indicators in place, including detailed implementation information for each indicator (see figure 3), hospital IT risk managers should be able to evaluate the implemented measures.

To be able to make any conclusions about whether the implemented measures affect the indicators, it was necessary to define relationships between measures and indicators. Based on qualitative content analysis, we were able to identify six relationships between the defined subgroups of measures and subgroups of indicators. Figure 4 shows which groups of measures impact which groups of indicators: The more measures in a category are implemented, the more positive the expected effect on the indicators of the corresponding category.

To make our results available to IT risk managers in hospitals, we made the complete catalogue (81 pages) freely available in German.[21]

Validation of the catalogue (research step #3)

As planned, the catalogue was validated in a case study in an Austrian hospital. Overall, 38 of 49 measures were implemented, and 4 of 18 indicators were selected to evaluate the measure. (These measures and indicators are marked with an asterisk '*' in table 2 and table 3.) In our pilot study, we focused on those measures and indicators chosen as being relevant for the hospital; thus, we did not try to implement all of them. Figure 5 summarises the three main findings of the case study: The effectiveness of the catalogue was confirmed since 78% (n=38) of measures, and 100% (n=4) of the indicators could be implemented successfully. The satisfaction with the descriptions and instructions in the catalogue was also very high (96% for the measures, 100% for the indicators). The complexity of the implementation was mainly described as low (55%) for measures and exclusively low (100%) for indicators. Twenty-two per cent of measures needed moderate resources and only 6% were very complex to implement.

In the final group interview of the case study, all three health IT staff members stated that the catalogue is an effective and efficient tool to develop, implement and operate risk management for IT networks that incorporate medical devices.

DISCUSSION

Answering the research question

Based on the empirical data of our study, we developed and validated a catalogue of 49 measures and 18 indicators to help hospitals implement and evaluate risk management for medical devices connected to a hospital

Table 2 The 49 measures to implement risk management, including the priority and complexity of each measure

Subgroup	Measure	Priority	Complexity
Organisation	External laws and regulations must be taken into account*	★★	●●●
	The users must learn the network functions of the medical device*	★☆	●●●
	Information technology (IT) standards and frameworks [Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), etc] must be integrated*	★☆	●●●
	A professionally qualified risk manager must be appointed*	★☆	●●●
	Roles and tasks of the risk manager must be clearly defined*	★★	●●●
	Roles and tasks of the manufacturers must be clarified*	★★	●●●
	Roles and tasks of users must be defined*	★☆	●●●
	Responsible leadership must be appointed*	★★	●●●
	Possible stakeholders must be identified and informed*	★☆	●●●
	Scopes must be defined*	★★	●●●
	Risk management processes must be developed and implemented*	★★	●●●
	Risk management activities must be evaluated regularly and improved if necessary	★★	●●●
	Interface between medical technology and IT department must be ensured*	★★	●●●
	A coordinated procurement process for medical devices must be established*	★★	●●●
	Reporting to the responsible management must be implemented*	★☆	●●●
	A risk management file must be created*	★★	●●●
	All networked medical devices/systems must be recorded and documented*	★★	●●●
	A complete network description and documentation must be kept*	★★	●●●
	Document guidance must be introduced*	★☆	●●●
Risk identification	Ask manufacturers about possible cyber risks of their medical device*	★★	●●●
	Ask users what impact a medical device failure has*	★★	●●●
	Ask the IT department about general IT threats	★☆	●●●
	Identify the purpose of the connection to the IT network and derive risk situations*	★★	●●●
	Identify critical clinical areas and automatically assume critical networking there*	★☆	●●●
	Identify data flows completely and derive possible errors and effects	★☆	●●●
	Create or adapt hazard catalogue*	★☆	●●●
Risk analysis	Define risk matrix*	★★	●●●
	Define probabilities of occurrence*	★☆	●●●
	Define implications for data and information security*	★★	●●●
	Define impact for process effectiveness*	★★	●●●
	Define implications for patient safety*	★★	●●●
	Assess risks for each potential hazard*	★☆	●●●
	Document risk analyses and evaluations*	★★	●●●
Risk minimisation	The medical IT network must be constantly monitored*	★☆	●●●
	Basic general IT security (eg, ISO 2700x) must be ensured*	★★	●●●
	Incident and event management must be developed and implemented	★☆	●●●
	Implement network segmentations based on risk analysis	★☆	●●●
	Interface and communication standards (eg, HL7, DICOM) must always be applied*	★☆	●●●
	The technical infrastructure must be continuously kept at state of the art*	★★	●●●

Continued

Table 2 Continued

Subgroup	Measure	Priority	Complexity
	Manual data processing procedures should be identified as possible workarounds*	★☆	
	Risk-minimising measures must be regularly reviewed and documented	★★	
	Catalogue for risk-minimising measures must be created and implemented	★★	
Residual risks	Residual risks must be systematically assessed and justified	★★	
	Residual risks must be documented in an understandable manner	★★	
	Residual risks must always be accepted by top management*	★☆	
Change management	Systematic change and configuration processes must be developed	★★	
	All changes and configurations must be approved by IT risk management*	★☆	
	Frequent changes should be defined as standard processes (routine)	★★	
	Significant changes or new installations should be organised as a project*	★★	

*Measures implemented in the case study.

IT network. The catalogue describes the importance of each measure and indicator and the resources (technical, organisational, financial) that are needed for their implementation. The catalogue should help information technology (IT) risk managers in hospitals to control the complexity of implementing IT risk management according to IEC 80001-1.

Strengths and weaknesses of the method

Due to the combination of qualitative and quantitative research methods within the Delphi method, the initially unclear knowledge about the measures and indicators sought could be operationalised and subsequently quantified and evaluated. In particular, the self-evaluating character of this method, that is, the anonymised feedback of the results within the expert group and the possibility for the experts to reflect and reconsider these results until a stable agreement or disagreement prevailed, was of outstanding importance for the quality of the data. However, the validity of a Delphi study, and thus also of the present study, is strongly influenced by the selection of experts. We, thus, invited experts with a considerable variation of professional backgrounds and much practical experience. The experts came exclusively from German-speaking countries, as risk management in these countries is performed based on similar regulatory requirements. Moreover, few German-language guidelines for IT risk management in hospitals exist. It must also be considered that German-speaking countries are strongly oriented towards the national adaptations of IEC 80001-1, which is still based on the first version of IEC 80001-1 published in 2010. The knowledge of the experts interviewed is, therefore, mostly based on these national implementations.

ID – Title of a measure or an indicator

Priority:	★★	**Complexity:**	
Purpose:	*Description of the purpose of a measure or indicator.*		
Implementation recommendation:	*Recommendation for the concrete implementation of a measure or an indicator.*		
	Example for the recommendation.		
Critical success factor:	*Description of factors that are important for the successful implementation of the measure or indicator.*		
Person:	*Description of the person who should implement a measure or indicator.*		
Output:	*Description of the result of a successful implementation.*		
Related indicator/measure:	*Description of the measure or action that is related to the measure or action described here.*		

Figure 3 Structure of the catalogue's descriptions of measures or indicators. *One star = important; two stars = very important; red = high, yellow = moderate, green= low complexity*

Table 3 The 18 indicators to evaluate risk management, including the priority and complexity of each indicator

Subgroup	Indicator	Priority	Complexity
Performance of connected medical devices	No of residual risks identified	★★	○○●
	No of risk control measures*	★★	○○●
	No of probable risks identified	★★	○○●
	No of potential risks identified	★★	○○●
Effectiveness of connected medical devices	No of incidents in which data was lost	★★	○●○
	No of incidents in which the required information technology (IT) service was not available	★★	○○●
	No of emergency operations caused by the connection to the IT network*	★★	○○●
	No of incidents in which patient data were not available	★★	○○●
	No of errors in patient data caused by the connection to the IT network	★★	○○●
Technical infrastructure	Average age of medical devices which are connected to IT network	★★	○●○
	No of malfunctions of medical devices which are connected to IT network	★★	○○●
	No of failures of the medical IT network*	★★	○○●
No of deliberate acts	No of data thefts and data protection incidents*	★★	○●○
	No of blackmail attempts	★★	○○●
	No of hacker attacks	★★	○●○
	No of unauthorised or undetected connections	★★	○●○
	No of malware activities (Trojans, worms, viruses, etc)	★★	○●○
	No of unauthorised data changes and accesses	★★	○●○

*Indicators evaluated in the case study.

Due to this geographical restriction, the catalogue was mainly developed for use in German-speaking countries. To assess its applicability in other countries, the catalogue should be validated with non-German-speaking experts.

We needed only two rounds of expert interviews in our Delphi study to reach a consensus. A third iteration was not necessary.

We conducted the case study in one hospital only. Further research is needed to validate the usefulness of the catalogue in further hospitals.

Meaning of the results

Our catalogue will help hospitals to set up and operate IT risk management according to IEC 80001-1 more simply and straightforwardly than the standard. We reached this aim as the catalogue (much like a cookbook) recommends a defined number of implementation measures and provides detailed information about them. IT risk managers can work through the catalogue step by step and do not have to interpret abstract specifications as

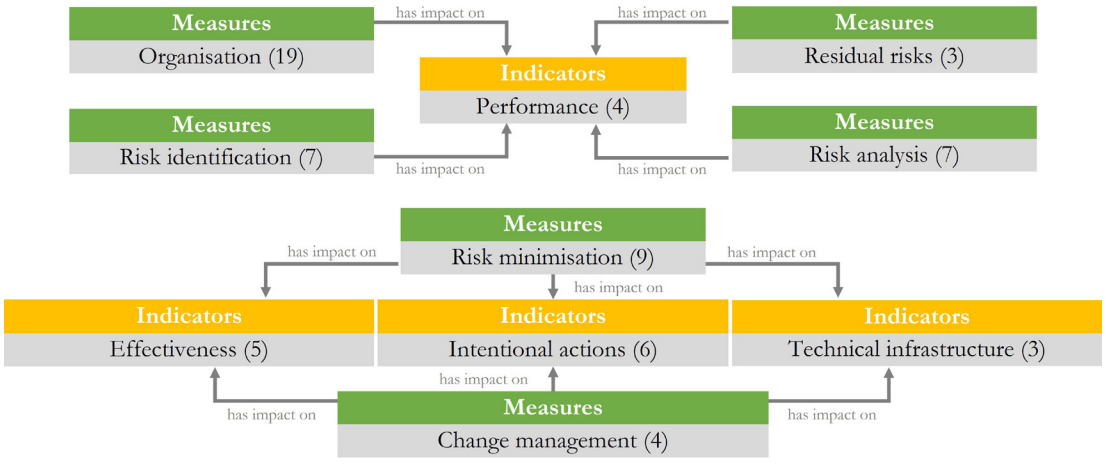

Figure 4 The identified relationships between groups of measures and indicators. (The numbers in parentheses represent the number of measures or indicators.).

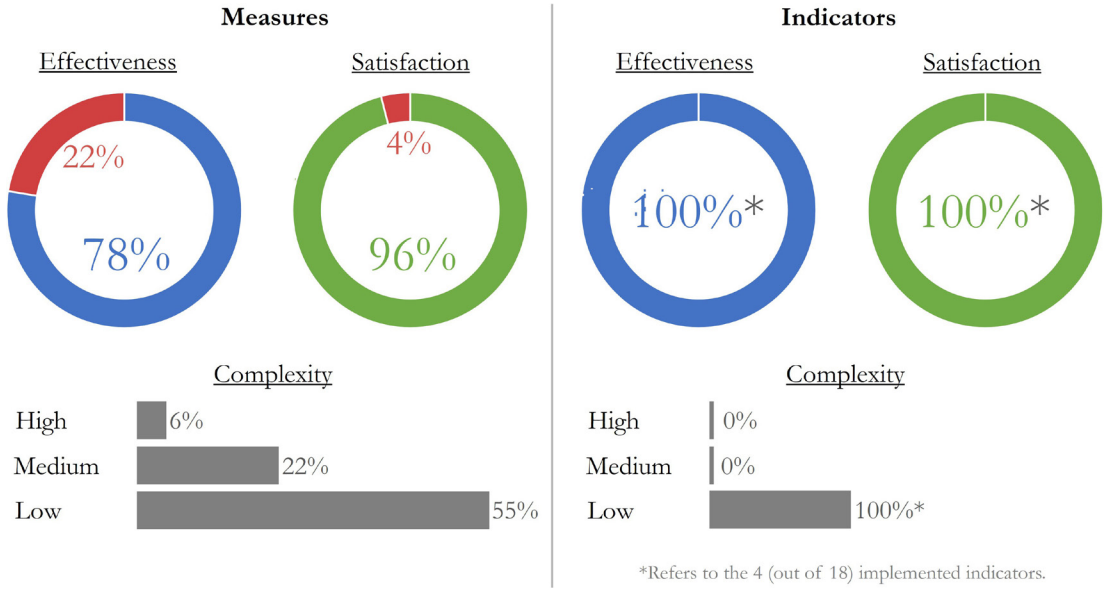

Figure 5 Results of case study. Successfully implemented measures and indicators (blue percentage value), the satisfaction of the study participants with the descriptions and instructions for implementing these measures and indicators (green percentage value), and the complexities of their implementation (grey percentage values).

is necessary with IEC 80001-1. There is also no need to purchase and understand the technical reports associated with the standard in order to achieve a high degree of IEC 80001-1 conformance. In addition, the measures described in the catalogue are based on the practical experience of experts.

The catalogue also proposes concrete indicators that hospitals can use to assess whether the implemented measures and, as a result, the implemented risk management have achieved the desired goals. We reached this as the catalogue defines relationships between groups of measures and indicators. It should be noted that the indicators represent estimates and assumptions based on expert opinions. The catalogue cannot offer a valid causal relationship between measures and indicators.

Reference to the state of the art

With the catalogue, we support hospitals in following the recommendation of experts that all medical devices integrated into an IT network must be covered by systematic risk management.[5–7] Compared with the first version of IEC 80001-1 and actual national implementations for German-speaking countries, which are still based on this first version from 2010, our catalogue thus helps IT risk managers in hospitals to deal with the complexity in implementing IT risk management.[5] This also applies to the current version of IEC 80001 from 2021. Although this version formulates clearer and more detailed implementation recommendations, these are not described in as much detail as in our catalogue. Our catalogue is influenced by both versions of IEC 80001-1, which is evident in the names of some of the measures. This is not surprising, as all of our experts know these standards. In comparison with existing non-scientific guidelines[19] or scientific papers[14], our catalogue goes into further detail. Our catalogue offers a stepwise implementation approach with detailed descriptions and recommendations. Furthermore, our catalogue informs of the complexity that should be expected in implementing a measure or indicator and of the priority of measures and indicators. In addition, our catalogue takes into account the special requirements in German-speaking countries (eg, medical device laws, organisational structures in hospitals, or focus on German-language literature in practice).

As the catalogue contains indicators to evaluate the impact of the implemented measures, this will meet the demand for more methods to evaluate and verify the correctness and effectiveness of interventions in health informatics.[18]

Outlook

New trends in digitalisation, such as artificial intelligence or the Internet of Things, are having an impact on the healthcare field.[22] These developments pose new challenges with regard to IT risk management and must therefore be taken into account in any future evolution of our catalogue. In addition to the case study, the catalogue was already actively communicated to three other hospitals. In further case studies, our catalogue must be tested for practicability and completeness. The aim is to involve as many different healthcare institutions as possible to identify and consider additional requirements. A larger sample of experts should be considered.

CONCLUSION

Our work's benefit is that with our catalogue of measures and indicators, hospitals may address recent difficulties in implementing and evaluating IT risk management for medical devices according to IEC 80001. In practice, IT risk

managers can use the catalogue to prioritise implementation measures and evaluation indicators by following the detailed descriptions and empirically based recommendations. Connecting medical devices to hospital IT networks is increasingly important for the effectiveness of medical processes and patient safety. IT risks arising from medical devices connected to IT networks (eg, unauthorised actions, compromise of functions, technical failures) must be covered by IT risk management. The catalogue we have developed may therefore assist in implementing and operating a powerful risk management system. However, it must be taken into account that our results relate very much to the German-speaking region due to the selection of experts, the location of the case study and the associated focus on the national implementation of IEC 80001. We expect that our results will be of relevance to other countries, but we still have to evaluate this.

Acknowledgements We thank all of the health IT experts for participating in our Delphi study. Without their support, this work would not have been possible.

Contributors SR had the idea for the study, planned it, conducted it and submitted this manuscript. EA supervised the study, contributed to its planning and revised the manuscript. SR acts as guarantor.

Funding This research was partially funded by a scientific scholarship from TÜV AUSTRIA (https://www.tuv.at/).

Competing interests None declared.

Patient consent for publication Not applicable.

Ethics approval Ethical clearance was obtained from the 'RCSEQ - Research Committee for Scientific Ethical Questions' of the Private University For Health Sciences and Health Technology (Hall in Tirol, Austria) with approval number 1717: No patients were involved in the study and no sensitive and data protection-relevant data were processed. The authors of this study have informed the participants (experts) in the Delphi study and in the case study regarding their rights.

Provenance and peer review Not commissioned; externally peer reviewed.

Data availability statement All data relevant to our study are included in the article or given as supplementary information.

ORCID iDs
Stefan Richter http://orcid.org/0000-0003-0620-113X
Elske Ammenwerth http://orcid.org/0000-0002-3244-6918

REFERENCES

1 Larsen E, Fong A, Wernz C, *et al*. Implications of electronic health record downtime: an analysis of patient safety event reports. *J Am Med Inform Assoc* 2018;25:187–91.
2 Ahlbrandt J, Röhrig R, Dehm J. Risikomanagement für medizinische Netzwerke in der Intensiv-und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1. In: *GMS Medizinische Informatik, Biometrie und Epidemiologie, 9*, 2013.
3 Kruse CS, Frederick B, Jacobson T, *et al*. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care* 2017;25:1–10.
4 Magrabi F, Ong MS, Coiera E. Health IT for patient safety and improving the safety of health IT. In: *Evidence-based health informatics: promoting safety and efficiency through scientific methods and ethical policy*, 2016.
5 Ahlbrandt J, Röhrig R. Safety first! managing risks for a daisy chain of medical devices connected to the IT-network-first experiences applying IEC 80001-1. In: *Studies in health technology and informatics*, 2013.
6 Williams PAH, Woodward AJ. *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, 8*. Medical Devices: Evidence and Research, 2015.
7 Alwi R, Prowse P, Gaamangwe T. Proactive Role of Clinical Engineering in the Adoption of ISO/IEC 80001-1 within Healthcare Delivery Organization. In: *Proceedings of the annual International Conference of the IEEE engineering in medicine and biology Society*. EMBS, 2020.
8 International Organization for Standardization. Risk management — guidelines (ISO 31000:2018), 2018. Available: https://www.iso.org/standard/65694.html [Accessed 21 Mar 2022].
9 International Organization for Standardization. Information technology — security techniques — information security risk management (ISO 27005:2018), 2018. Available: https://www.iso.org/standard/75281.html [Accessed 22 Mar 2022].
10 Sahu K, Rajshree KR. Risk management perspective in SDLC. *IJARCSSE* 2014.
11 International Organization for Standardization. Health software and health IT systems safety, effectiveness and security — Part 5-1: security — activities in the product life cycle (IEC 81001-5-1:2021), 2021. Available: https://www.iso.org/standard/76097.html [Accessed 25 Aug 2022].
12 International Organization for Standardization. Application of risk management for IT-networks incorporating medical devices — Part 1: roles, responsibilities and activities (IEC 80001-1:2010), 2010. Available: https://www.iso.org/standard/72026.html [Accessed 22 Mar 2022].
13 International Organization for Standardization. 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 (IEC 80001-1:2021), 2021. Available: https://www.iso.org/standard/72026.html [Accessed 24 Aug 2022].
14 MacMahon ST, Cooper T, McCaffery F. Revising IEC 80001-1: risk management of health information technology systems. *Comput Stand Interfaces* 2018;60:67–72.
15 Hegarty FJ, MacMahon ST, Byrne P, *et al*. Assessing a hospital's medical IT network risk management practice with 80001-1. *Biomed Instrum Technol* 2014;48:64–71.
16 MacMahon ST, McCaffery F, Keenan F. The MedITNet assessment method - development and validation using action design research. *Int J Adv Life Sci* 2016;8.
17 Anderson S, Williams T. Cybersecurity and medical devices: are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Comput Stand Interfaces* 2018;56:134–43.
18 Rigby M, Ammenwerth E. The need for evidence in health informatics. In: *Evidence-based health informatics: promoting safety and efficiency through scientific methods and ethical policy*, 2016.
19 Deutsche Krankenhausgesellschaft EV. *Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten (DIN en 80001-1:2011): Umsetzungshinweise für Krankenhäuser*. Stuttgart, 2012.
20 Mayring P. Techniken qualitativer Inhaltsanalyse. In: *Qualitative Inhaltsanalyse*. Weinheim und BAsel: Beltz Verlag, 2015: 50–114.
21 Richter S, Ammenwerth E. Maßnahmen und kennzahlen zur einführung, umsetzung und evaluierung eines risikomanagements für IT-netzwerke, die medizintechnische geräte beinhalten. *Research report* UMIT TIROL; 2022.
22 H. Almulihi A, Alassery F, Irshad Khan A, *et al*. Analyzing the implications of healthcare data breaches through computational technique. *Intell Autom Soft Comput* 2022;32:1763–79.