TECHNICAL REPORT

ISO/TR 80001-2-7

First edition
2015-04-01

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

Application du management du risque aux réseaux des technologies de l'information contenant les dispositifs médicaux — Conseils pour les applications —

Partie 2-7: Directives de prestation de soins de santé organisations sur la façon de s'auto-évaluer leur conformité avec la norme IEC 80001-1

Reference number
ISO/TR 80001-2-7:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/TC 215, *Heath informatics*.

ISO/IEC/TR 80001 consists of the following parts, under the general title *Application of risk management for IT-networks incorporating medical devices:*

— *Part 1: Roles, responsibilities and activities*

— *Part 2-1: Step-by-step risk management of medical IT-networks; Practical applications and Examples*

— *Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

— *Part 2-3: Guidance for wireless networks*

— *Part 2-4: General implementation guidance for Healthcare Delivery Organizations*

— *Part 2-5: Application guidance — Guidance for distributed alarm systems*

— *Part 2-6: Application guidance — Guidance for responsibility agreements*

— *Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*

The following parts are under preparation:

— *Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*

Introduction

This part of ISO/TR 80001 provides guidance for a Healthcare Delivery Organization (HDO) that wishes to self-assess its implementation of the processes of IEC 80001-1. This part of ISO/TR 80001 can be used to assess Medical IT-Network projects where IEC 80001-1 has been determined to be applicable. This part of ISO/TR 80001 provides an exemplar assessment method which includes a set of questions which can be used to assess the performance of risk management of a Medical IT-Network incorporating a medical device. This assessment method can be used in its presented form or can be tailored to meet the needs of a specific HDO. A Process Reference Model (PRM) and an example Process Assessment Model (PAM) that meet the requirements of ISO/IEC 15504-2 are included in the Appendices of this part of ISO/TR 80001. The PRM and PAM can be used to provide a standardized basis for tailoring the exemplar assessment method where required.

This part of ISO/TR 80001 can be used in a number of ways including the following.

a) The assessment method can be used to perform an assessment to determine conformance against IEC 80001-1.

b) In instances where conformance has been established, the assessment method can also be used to assess risk management processes and determine the capability level at which these processes are being performed.

c) Based on the context of the HDO being assessed, the assessment method can be tailored to address the individual HDO use, needs and concerns.

The results of the assessment will highlight any weaknesses within current risk management processes and can be used as a basis for the improvement of these processes. Where necessary, modification of the assessment method can be undertaken with reference to the PRM and PAM for IEC 80001-1 which are also included in this part of ISO/TR 80001. This approach allows for a lightweight assessment approach to which more rigour can be added if required. For example, a re-assessment may be required in instances where an initial assessment revealed weaknesses in the current risk management processes and improvements have subsequently been made which require re-assessment to assess their impact on conformance. A re-assessment may also be performed in instances where confirmation is required that process improvement measures which have been undertaken have resulted in the achievement of a higher capability level.

This part of ISO/TR 80001 provides the following:

— guidance for a HDO to self-assess implementation of the processes of IEC 80001-1;

— an exemplar assessment method which

  — includes a set of questions,

  — can be used to assess the performance of risk management of a Medical IT-Network incorporating a medical device,

  — can be used in its presented form, and

  — can be tailored on a standardised basis using the included PRM and PAM;

— a PRM that meet the requirements of ISO/IEC 15504-2;

— an example PAM that meet the requirements of ISO/IEC 15504-2.

NOTE This part of ISO/TR 80001 contains original material that is © 2013, Dundalk Institute of Technology, Ireland. Permission is granted to ISO and IEC to reproduce and circulate this material, this being without prejudice to the rights of Dundalk Institute of Technology to exploit the original text elsewhere.

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

1 Scope

The purpose of this part of ISO/TR 80001 is to provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1.

The purpose of this part of ISO/TR 80001 is to

a) provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1,

b) provide an exemplar assessment method which can be used by HDOs in varying contexts to assess themselves against IEC 80001-1,

c) define a PRM comprising a set of processes, described in terms of process purpose and outcomes that demonstrate coverage of the requirements of IEC 80001-1, and

d) define a PAM that meets the requirements of ISO/IEC 15504-2 and that supports the performance of an assessment by providing indicators for guidance on the interpretation of the process purposes and outcomes as defined in IEC 80001-1 (PRM) and the process attributes as defined in ISO/IEC 15504-2.

This part of ISO/TR 80001 does not introduce any requirements in addition to those expressed in IEC 80001-1.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Members of ISO and IEC maintain registers of currently valid International Standards.

IEC 80001-1:2010, *Application of Risk Management for IT-Networks incorporating Medical Devices — Part 1: Roles, responsibilities and activities*

ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

ISO/IEC 15504-2:2003, *Information technology — Process assessment — Part 2: Performing an assessment*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15504-1 and IEC 80001-1 apply.

4 Assessment Method

4.1 Prerequisites

In order to perform an assessment, an assessor is required. When performing an assessment, it is preferable to have more than one assessor. In cases where the assessment is performed by more than one assessor, a lead assessor should be nominated. The need for multiple assessors is determined by the context of the HDO and the system under assessment. The context of the HDO and the scope of the assessment also determine the need for the modification of the presented exemplar assessment method. In addition, to performing the assessment, the assessor should consider interacting with all relevant risk management stakeholders both those internal and external to the HDO. The assessor should also have access to all relevant materials related to the performance of risk management activities.

4.2 Assessment Method Overview

The use of an assessment method allows assessments to be performed in a consistent and repeatable manner. The assessment method which is presented in this part of ISO/TR 80001 is based on the processes and practices as defined in the PRM and PAM which are presented in the appendices of this part of ISO/TR 80001. Figure 1 shows the 14 processes and their respective process categories which are contained in the PAM. The PAM, which can be found in Annex C, provides a full description of these processes including the activities (base practices) which must be performed to successfully achieve the purpose of the process. The assessment method consists of an approach to performing the assessment and a set of questions which allows the assessor to collect objective evidence to support an assessment of how each of the activities are being performed (and support the assignment of a capability rating to each process). On the basis of the evidence gathered during the assessment, the strengths and weaknesses of the processes can be identified and recommendations can be made to improve risk management practices and conformance with IEC 80001-1.

PAM Processes:

Medical IT Network Risk Management Process Group (MRM)	
MRM.1	Medical IT Network Risk Management Process
MRM.1.1	Risk Analysis & Evaluation
MRM.1.2	Risk Control
MRM.1.3	Residual Risk

Change Release Management & Configuration Management Process Group (CRCM)	
CRCM.1	Change Release & Configuration Management
CRCM.2	Decision on how to apply Risk Management
CRCM.3	Go Live

Live Network Risk Management Process Group (LNRM)	
LNRM.1	Monitoring
LNRM.2	Event Management

Medical IT Network Documentation and Planning Process Group (MDP)				
MDP.1	Medical IT Network Planning		MDP.4	Risk Management Policy
MDP.2	Medical IT Network Documentation		MDP.5	Organisational Risk Management Process
MDP.3	Responsibility Agreements			

Figure 1 — PAM Processes — Assessment Method

4.3 Assessment Stages

In order to produce a repeatable and consistent approach to assessment, the assessment is carried out in a number of stages. A seven-stage procedure for the performance of the assessment has been defined. Each of the stages is described in the following sections of this clause:

4.3.1 Stage 1 — Defining Assessment Scope

This is the initial planning stage of the assessment. During this stage of the assessment, the lead assessor meets with Top management and the scope of the assessment is defined. This stage can be used to define to which Medical IT-Networks IEC 80001-1 is applicable. The system (or IT network modification project) which is to be the focus of the assessment is defined and the context of the system is understood. Risk management stakeholders should be identified. Risk management stakeholders are both internal (e.g. clinical engineering) and external (e.g. medical device manufacturers) to the HDO. The lead assessor should ensure that Top management sponsors the assessment and that all relevant risk management stakeholders are available to participate for the duration of the assessment process.

4.3.2 Stage 2 — Stakeholder Involvement

Having secured the commitment of all relevant risk management stakeholders to participate in the assessment process, the lead assessor meets with risk management stakeholders to explain the assessment method. The lead assessor explains the agreed scope of the assessment and explains how the assessment is to be conducted and how findings from the assessment are to be communicated. As risk management stakeholders consist of members from a cross disciplinary team, the lead assessor ensures that all stakeholders are clear on what their participation in the assessment involves.

A sample template which can be used to record the information collected in stages 1 and 2 of the assessment process is provided in A.2.2.

4.3.3 Stage 3 — Information Collection and Evaluation

During this stage of the assessment, the lead assessor interviews various risk management stakeholders using a set of scripted questions (for the exemplar assessment questions, see A.1) and evaluates the responses. Group interviews should be used where possible to gain an understanding of risk management processes from varying stakeholder perspectives. A combination of individual and group interviews may be used. To facilitate the recording of the responses, a second assessor may be used to take notes on the interviews. Additional questions may be required if clarification is necessary. The assessor uses the questions to promote discussion on risk management practices which are currently in place. At this stage, the lead assessor can also inspect work products related to risk management activities and evaluate these work products on the basis of the assessment questions.

A sample template which can be used to record the information collected during the interviews which are performed in stage 3 of the assessment process is provided in A.2.3.

4.3.4 Stage 4 — Findings Report

A findings report is drafted based on the data gathered during stage 3. The lead assessor reviews the interview notes and evaluates the responses to the scripted questions and any available work products. Having reviewed the evidence gathered during the assessment, the lead assessor generates a rating for the response to the questions based on the Process Attribute Rating Scale as detailed in 4.4. In the case of an assessment to assess conformance, the findings report should state whether conformance to the standard (based on an assessment of all 14 processes) has been achieved. On the basis of the evidence gathered during the assessment, the lead assessor identifies strengths and weaknesses within the current risk management practices. The lead assessor includes in the findings report a set of recommendations to address identified issues and which can be implemented in order to improve risk management practices and facilitate the improvement of risk management processes.

A sample template which can be used to draft the findings report which is prepared during stages 3 of the assessment process is provided in A.2.3.

4.3.5 Stage 5 — Presentation of Findings

The findings report is presented by the lead assessor to Top management and risk management stakeholders who have taken part in the assessment. At this stage, a date for a reassessment can be agreed.

Stages 1 to 5 above complete the assessment process. Where a follow-up assessment is required, stages 6 and 7 below can be performed. A reassessment can be used to confirm that the recommendations for improvements to the risk management process have improved risk management processes as envisaged.

4.3.6 Stage 6 — Improvement Plan (optional)

Having allowed time for the findings report to be read and understood, the lead assessor meets with Top management and risk management stakeholders to review the findings of the report. On the basis of the report, a plan for improvements to the risk management process is agreed. The plan should include specific improvement objectives and discussion and timelines for the implementation of the identified improvements.

4.3.7 Stage 7 — Follow-up Assessment (optional)

A follow-up assessment can be performed to ensure that improvements to the risk management processes have been implemented. The reassessment, if required, can be performed on the same project or on a similar Medical IT-Network project to assess if improvements to the process have been made and the impact of these improvements. For example, a reassessment can be initiated in instances where conformance was not determined to have been achieved in the previous assessment and improvements have been made to address the weaknesses. The reassessment determines if the implemented improvements have achieved conformance. A reassessment can also be initiated to confirm that improvements (identified and implemented as a result of the previous assessment) have resulted in the achievement of a higher capability level for a specific process or processes. The scope of the reassessment depends on the weaknesses highlighted in the previous assessment and as such can address all processes or a subset of processes.

4.4 Process attribute rating scale

4.4.1 Rating of process attributes

When performing an assessment of the capability of risk management processes, each of the base practices is reviewed using objective evidence gathered during assessment interviews and through examination of work products. On the basis of this review, each of the base practices can be assigned a rating. The capability level of the process is based on the average rating of the base practices related to the process. ISO/IEC 15504-2 defines six capability levels from Level 0 (Incomplete Process) to Level 5 (Optimizing Process) and defines attributes of the process that are associated with the achievement of each of the capability levels. An assessment of conformance seeks to confirm that all processes are being performed at Capability Level 1 (Performed Process). For achievement of Capability Level 1, it must be determined during the assessment that risk management processes (as defined within the PAM in Annex C) are being performed in a manner that the purpose of all processes has been achieved. Process performance and capability attributes as defined in ISO/IEC 15504-2 are discussed in detail in C.2.2.3, Table C.1. When performing an assessment of risk management processes at all capability levels, the process attribute rating scale as defined in ISO/IEC 15504-2 should be used.

The extent of achievement of a process attribute is measured using an ordinal scale of measurement as defined 4.4.2.

4.4.2 Process attribute rating values

The ordinal rating scale defined below shall be used to express the levels of achievement (process attribute rating values) of the process attributes.

N Not achieved

There is little or no evidence of achievement of the defined attribute in the assessed process.

P Partially achieved

There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable.

L Largely achieved

There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weakness related to this attribute may exist in the assessed process.

F Fully achieved

There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process.

The ordinal points defined above shall be understood in terms of a percentage scale representing extent of achievement.

The corresponding values shall be:

N	Not achieved	0 to 15 % achievement
P	Partially achieved	>15 % to 50 % achievement
L	Largely achieved	>50 % to 85 % achievement
F	Fully achieved	>85 % to 100 % achievement

4.5 Capability Levels

The exemplar assessment method which is provided in this part of ISO/TR 80001 allows HDO's to assess their current risk management processes. The focus of the exemplar assessment method is to allow for an assessment to be performed to identify areas of the risk management processes which are not being performed in accordance with the requirements of IEC 80001-1 (i.e. processes which have not achieved level 1 capability) and allow recommendations to be made to allow for a level 1 capability level to be achieved. The exemplar assessment method uses a set of scripted questions, each of which are related to specific base practices as outlined in the PAM, to review risk management processes and identify any weaknesses within the current processes in line with the achievement of level 1 capability. Through the identification of weaknesses in the current process and the implementation of recommendations to address these weaknesses, capability levels upper than 1 may be achieved. The exemplar assessment method provided can also be used to assess against capability levels upper than 1 through the use of the capability level assessment as outlined in the PAM in Annex C which contains a full explanation of all capability levels and the associated assessment indicators which can be reviewed in assessing against capability levels upper than level 1.

4.6 Tailoring the Assessment Method

The exemplar assessment method as outlined in this part of ISO/TR 80001 provides a sample set of questions for use in the assessment of IEC 80001-1 risk management processes. The set of questions provided is intended as a guide who can then be tailored for use in a specific HDO context. The questions should be reviewed on the basis of the context of the HDO in question and amendments made to take into account any variation that are specific to the HDO. The exemplar questions which are provided are based on the base practices as outlined within the PAM in Annex C. To tailor the assessment method questions, the base practices on which the questions are based should be reviewed by the assessor. The questions can then be modified, removed, or additional questions added as required by the individual context of the HDO. The assessor should ensure that they are fully aware of the HDO context in order to tailor the questions appropriately. The assessor should also ensure that the questions continue to be related to the base practices as described in the PAM. As the base practices within the PAM describe

high level activities that shall be performed in order to achieve the process purpose, they can be used as the basis for more specific questions related to the HDO context. Using this approach ensures that assessments take into account individual HDO context while performing a consistent approach to the assessment of the process purpose and the requirements of IEC 80001-1.

It should be noted that the assessment of a single base practice may require the use of more than one question. The use of the scripted questions in the assessment method is intended to be used as a tool to initiate a discussion on current risk movement processes and allow the assessor to collect objective evidence to support the achievement of a specific capability level. To facilitate the assessors ability to gain an understanding of current risk management processes, additional questions may be posed by the assessor which are not contained in the assessment method to support the judgement of the achievement of the capability level. The assessor may also review documentation which is generated by the performance of risk management activities at this stage.

Annex A
(informative)

Assessment Method

A.1 Exemplar Assessment Questions

A.1.1 General

This Annex contains a set of exemplar assessment questions for each of the 14 processes which are defined in the PRM and PAM contained in Annex B and C. The assessment questions are based on the base practices related to each process. For each process, the questions are provided along with some guidance for the assessor on points which should be considered when asking the questions. Where more information on a specific base practice is provided in other parts of IEC 80001, details of the technical report and the relevant section are provided. Details of the technical reports which have been published are provided in the bibliography section of this part of ISO/TR 80001. It should be noted that where a specific technical report is appropriate to the context of the network (e.g. a wireless network) then this part of ISO/TR 80001 should be consulted in full prior to the commencement of an assessment of the risk analysis processes related to this network. This set of questions is intended as a starting point for performing an assessment and are based on the base practices which are included in the PAM. Additional questions can be added to this set and asked during the assessment if clarification or additional information is required. This set of questions can also be modified to include questions which address the specific context of a particular HDO or a particular geographical region. These questions are intended to be used to perform an assessment against capability level 1. Additional questions can be added to address capability levels upper than 1. An explanation of capability levels is provided in the PRM and PAM which can be found in Annex B and Annex C.

Each question relates to a specific base practice within a specific process within the PAM. To facilitate traceability between the PAM and the assessment questions each question has a unique identifier, e.g. MRM.1 BP1 Q.1. The code consists of the process ID which is used in the PRM and PAM (e.g. MRM.1), the base practice number (e.g. BP1), and the question number (e.g. Q.1).

A.1.2 MRM.1 Medical IT-Network Risk Management Process

Table A.1 — MRM.1 BP1

MRM.1 BP1: Establish a Medical IT-Network Risk Management File. Establish a Medical IT-Network Risk Management file that serves as a central repository for all documentation as required to carry out risk management activities.	
Question:	**Guidance:**
MRM.1 BP1 Q.1 Do you have a Medical IT-Network Risk Management File? **MRM.1 BP1 Q.2** How is the file stored, accessed, and maintained?	A Medical IT-Network Risk Management File shall be established to act as a central repository for all documentation required to carry out risk management activities in line with this standard. In addition, the file shall contain all supporting documentation required for risk management activities. The file shall contain the current configuration management information for the Medical IT-Network either through explicit documentation or by reference, for example, to a live database.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures
IEC 80001–2-1	7.4.6.4 Re-evaluate RISK

Table A.1 *(continued)*

IEC 80001–2-1	7.4.6.5 RISK/benefit analysis
IEC 80001–2-1	7.4.7 Step 7 Implement RISK CONTROL measures
IEC 80001–2-1	7.4.8.2 VERIFICATION of effectiveness
IEC 80001–2-1	7.4.9 Step 9: Evaluate any new RISKS arising from RISK CONTROL
IEC 80001–2-1	7.4.10 Step 10: Evaluate and report overall RESIDUAL RISK (in reference to documenting individual residual risks and overall residual risk
IEC 80001–2-1	Figure 8 — Sample summary RISK ASSESSMENT register for the PACU example
IEC 80001–2-1	E.6 VERIFICATION of the design and execution of the RISK MANAGEMENT PROCESS
IEC 80001–2-1	Annex F RISK ANALYSING small changes in a MEDICAL IT-NETWORK (Figure F.1)
IEC 80001–2-4	4.1 Top management Responsibilities

Table A.2 — MRM.1 BP2

MRM.1 BP2: Assign Risk Management Resources. Ensure that adequate appropriately qualified resources (including Medical IT-Network Risk Manager) for management, performance of work, and assessment activities are assigned.	
Question:	**Guidance:**
MRM.1 BP2 Q.1 Have risk management resources been assigned?	Ensure that top management input into risk management process and ensure that adequate and relevant risk management resources are assigned (including Medical IT-Network Risk Manager) for the management, performance of work, and assessment activities are assigned. Personnel involved in the performance of risk management activities shall have the necessary qualifications, knowledge, and competence to perform risk management of the Medical IT-Network.
Technical Report:	**Section:**
IEC 80001–2-4	4.1 Top management Responsibilities
IEC 80001–2-4	4.2 Small Responsible Organization — points to consider
IEC 80001–2-4	4.3 Large Responsible Organization — points to consider
IEC 80001–2-4	5.3 Establish underlying risk framework
IEC 80001–2-4	5.4.1 Performing a Risk Assessment
IEC 80001–2-4	5.4.2.3 Large Responsible Organization — points to consider
IEC 80001–2-4	5.4.4 Manufacturer Identification

Table A.3 — MRM.1 BP3

MRM.1 BP3: Identify Risk Management Stakeholders and inform of their responsibilities. Identify people responsible for risk management and lifecycle management activities of medical devices incorporated into IT networks. Ensure resources are adequately informed of their responsibilities and that they co-operate with the Medical IT-Network Risk Manager.	
Question:	**Guidance:**
MRM.1 BP3 Q.1 Are risk management stakeholders identified and aware of their responsibilities?	Ensure that relevant risk management stakeholders are identified and informed of their responsibilities and that communication paths exist between the Medical IT-Network risk manager and risk management stakeholders. Risk management stakeholders shall co-operate with the Medical IT-Network Risk Manager in gathering, analysing, assessment, and storage of information needed for risk management; lifecycle management of medical devices incorporated into IT networks; choice and procurement of medical devices. Risk management activities require co-operation from management responsible for Medical IT-Networks, general IT networks, lifecycle management of medical devices connected to IT network, users of medical devices, and maintenance and technical support for medical devices.

Table A.3 *(continued)*

Technical Report:	**Section:**
IEC 80001–2-4	4.1 Top management Responsibilities
IEC 80001–2-4	4.2 Small Responsible Organization — points to consider
IEC 80001–2-4	4.3 Large Responsible Organization — points to consider
IEC 80001–2-4	5.3 Establish underlying risk framework
IEC 80001–2-4	5.4.1 Performing a Risk Assessment
IEC 80001–2-4	5.4.2.3 Large Responsible Organization — points to consider
IEC 80001–2-4	5.4.4 Manufacturer Identification
IEC 80001–2-4	5.4.5 External IT and bio-medical engineering support

Table A.4 — MRM.1 BP4

MRM.1 BP4: Manage the Medical IT-Network throughout the life cycle as per the Risk Management Plan and Process. Manage the supervision, operation, installation, and maintenance of Medical IT-Network(s) throughout the life cycle according to the Risk Management plan and follow the results of the IT-Network Risk Management Process. Maintain the key properties of the medical IT-network throughout the life cycle.	
Question:	**Guidance:**
MRM.1 BP4 Q.1 Is a life cycle approach taken to the management of the Medical IT-Network?	Consider whether risk management activities are performed during the supervision, operation, installation, and maintenance of Medical IT-Network(s) throughout the life cycle.
MRM.1 BP4 Q.2 Are risk management activities performed according to the risk Management Plan and process?	Consider whether risk management activities are being performed according to the RM plan and process
MRM.1 BP4 Q.3 Are the key properties of the network considered during the performance of risk management activities?	Consider the impact to the network in terms of safety, effectiveness, and data and system security throughout the life cycle.
Technical Report:	**Section:**
IEC 80001–2-4	All Sections

Table A.5 — MRM.1 BP5

MRM.1 BP5: Document Risk Management activities. Risk management activities of risk analysis, risk evaluation, risk control, residual risk evaluation, and reporting and approval are documented in the Risk Management File.	
Question:	**Guidance:**
MRM.1 BP5 Q.1 Are risk management activities documented?	Ensure that risk management activities of risk analysis, risk evaluation, risk control, residual risk evaluation, reporting, and approval are documented in the risk management file. Documentation related to these risk management activities can be documented directly within the file or can exist as separate documents. Consider the appropriateness of the approach to documenting risk management activities according to the scope of the Medical IT-Network project.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures