PD ISO/TR 80001-2-7:2015

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: PD ISO/TR 80001-2-7:2015

National foreword

This Published Document is the UK implementation of ISO/TR 80001-2-7:2015.

The UK participation in its preparation was entrusted by Technical Committee CH/62, Electrical Equipment in Medical Practice, to Sub-committee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015.

Published by BSI Standards Limited 2015

ISBN 978 0 580 83412 7

ICS 11.040.01, 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2015.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/TR 80001-2-7:2015

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)

Documents
Document Sharing Hub

© ISO 2015

Full document details: PD ISO/TR 80001-2-7:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 80001-2-7:2015

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Assessment Method ... **2**
4.1 Prerequisites ... 2
4.2 Assessment Method Overview ... 2
4.3 Assessment Stages ... 3
4.3.1 Stage 1 — Defining Assessment Scope ... 3
4.3.2 Stage 2 — Stakeholder Involvement ... 3
4.3.3 Stage 3 — Information Collection and Evaluation ... 3
4.3.4 Stage 4 — Findings Report ... 3
4.3.5 Stage 5 — Presentation of Findings ... 4
4.3.6 Stage 6 — Improvement Plan (optional) ... 4
4.3.7 Stage 7 — Follow-up Assessment (optional) ... 4
4.4 Process attribute rating scale ... 4
4.4.1 Rating of process attributes ... 4
4.4.2 Process attribute rating values ... 4
4.5 Capability Levels ... 5
4.6 Tailoring the Assessment Method ... 5
Annex A (informative) **Assessment Method** ... **7**
Annex B (informative) **Process Reference Model** ... **38**
Annex C (informative) **Process Assessment Model** ... **50**
Annex D (informative) **Abbreviations and Process Identifiers** ... **100**
Bibliography ... **102**

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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*

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 80001-2-7:2015

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

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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

© ISO 2015 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

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

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD ISO/TR 80001-2-7:2015

Table A.5 *(continued)*

IEC 80001–2-1	7.4.6.4 Re-evaluate RISK
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.6 — MRM.1 BP6

MRM.1 BP6: Review Risk Management Activities at defined intervals. Risk management activities, including Event Management, are reviewed at defined intervals.	
Question:	**Guidance:**
MRM.1 BP6 Q.1 Are risk management activities reviewed at defined intervals?	Ensure that risk management activities including event management are reviewed at defined intervals to ensure the continuing suitability and effectiveness of the risk management process.
Technical Report:	**Section:**
IEC 80001–2-4	4.1 Top management responsibilities

A.1.3 MRM 1.1 Risk Analysis and Evaluation Process

Table A.7 — MRM1.1 BP1

MRM.1.1 BP1: Identify likely hazards. Identify hazards that are likely to arise from the Medical IT-Network.	
Question:	**Guidance:**
MRM.1.1 BP1 Q.1 How do you identify likely hazards?	Identify hazards that are likely to arise from the Medical IT-Network 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. Consideration should be given to the Safety, Effectiveness, and Data and System security of the network when identifying hazards.
Technical Report:	**Section:**
IEC 80001–2-1	5.1 Figure 1 — Basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE
IEC 80001–2-1	5.2 Hazards
IEC 80001–2-1	5.3 HAZARDOUS SITUATIONS
IEC 80001–2-1	5.4 Foreseeable sequences of events and causes
IEC 80001–2-1	5.5 UNINTENDED CONSEQUENCE
IEC 80001–2-1	6.1 Overview of the steps — Steps 1, 2, 3 and 4
IEC 80001–2-1	6.2.2 Initial RISK — Steps 1-5 (Figure 2) — (Steps 1, 2, 3 and 4)
IEC 80001–2-1	7.4.1 Step 1: Identify HAZARDs and HAZARDOUS SITUATIONs
IEC 80001–2-1	7.4.2 Step 2: Identify causes and resulting HAZARDOUS SITUATIONS

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.7 *(continued)*

IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, Clause 4 to 4.4)
IEC 80001–2-1	Practical examples of steps 1 to 4 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3
IEC 80001–2-1	Annex A (informative) Common HAZARDS, HAZARDOUS SITUATIONS, and causes to consider in MEDICAL IT-NETWORKS
IEC 80001–2-1	A.1 Typical HAZARDS in MEDICAL IT-NETWORKS
IEC 80001–2-1	A.2 Types of HAZARDOUS SITUATIONS
IEC 80001–2-1	A.3 Common causes in MEDICAL IT-NETWORKS
IEC 80001–2-1	A.4 Relationship between required network characteristics and HAZARDs,
IEC 80001–2-1	A.5 Relationship between HAZARDS, foreseeable sequences, and causes
IEC 80001–2-1	Table A.2 — Relationship between HAZARDS, foreseeable sequences, and causes
IEC 80001–2-1	A.6 HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS
IEC 80001–2-1	Table A.3 — Relationship between HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS
IEC 80001–2-1	Annex B (informative)List of questions to consider when identifying HAZARDs of the MEDICAL IT-NETWORK
IEC 80001–2-1	Annex C (informative) Layers of MEDICAL IT-NETWORKS where errors can be found
IEC 80001–2-1	Annex D (informative) Probability, severity, and RISK acceptability scales used in the examples in this technical report
IEC 80001–2-1	Table D.1 — Probability scales used in the examples in this technical report.
IEC 80001–2-3	All sections (Wireless Networks)
IEC 80001–2-4	All Sections

Table A.8 — MRM1.1 BP2

MRM.1.1 BP2: Estimate, Analyse, and Evaluate associated risks. Evaluate associated risks using available information or data throughout the lifecycle for each identified hazard.	
Question:	**Guidance:**
MRM.1.1 BP2 Q.1 How do you estimate, analyse, and evaluate associated risk for each identified hazard throughout the life cycle?	Consider how to estimate, analyse, and evaluate associated risks using the available information or data throughout the lifecycle. For each identified hazard, associated risk shall be estimated using available information or data. Results of these activities shall be recorded in the Medical IT-Network Risk Management File.
Technical Report:	**Section:**
IEC 80001–2-1	5.7 Degrees of RISK
IEC 80001–2-1	6.1 Overview of the steps — Step 5
IEC 80001–2-1	6.2.2 Initial RISK — Steps 1-5 (Figure 2) — Step 5
IEC 80001–2-1	Figure 2 — Steps 1-5: HAZARD identification through RISK EVALUATION
IEC 80001–2-1	7.3 Note about RISK EVALUATION
IEC 80001–2-1	7.4.5 Step 5: Evaluate RISK
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, Clause 5)
IEC 80001–2-1	Practical examples of step 5 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3
IEC 80001–2-1	Table D.3 — RISK level matrix
IEC 80001–2-1	Figure D.1 — Application of Steps 5 and 6 with 3 levels of RISK acceptability

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: PD ISO/TR 80001-2-7:2015

Table A.9 — MRM1.1 BP3

MRM.1.1 BP3: List possible consequences of harm. List possible consequences of harm (where probability of occurrence cannot be estimated) for use in risk control.	
Question:	**Guidance:**
MRM.1.1 BP3 Q.1 How do you identify possible consequences of harm?	Where probability of occurrence of harm cannot be estimated, the possible consequences shall be listed for use in risk evaluation and control. Results of these activities shall be recorded in the Medical IT-Network Risk Management File

Table A.10 — MRM1.1 BP4

MRM.1.1 BP4: Record results of Risk Analysis and Evaluation activities. Record the results of these activities in the Medical IT-Network Risk Management file. Record instances where the estimated risk is so low that risk reduction need not be pursued (as per RM plan) in the Medical IT-Network Risk Management File.	
Question:	**Guidance:**
MRM.1.1 BP4 Q.1 How are the results of risk analysis and evaluation activities recorded?	Consider how risk analysis and evaluation activities are recorded throughout the life cycle. Record the results of these activities in the Medical IT-Network Risk Management file. Record instances where the estimated risk is so low that risk reduction need not be pursued (as per Risk Management plan) in the Medical IT-Network Risk Management File.
Technical Report:	**Section:**
IEC 80001–2-1	5.8 Checking wording (including Table 2 — Methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES)
IEC 80001–2-1	Figure 4 — Sample summary RISK ASSESSMENT register format
IEC 80001–2-1	7.2 Application of Subclause 4.4.2: Document all RISK MANAGEMENT elements
IEC 80001–2-1	Practical examples of Steps 1 to 5 are shown in sections 8.1 to 8.5
IEC 80001–2-1	Annex H (informative) Template for examples
IEC 80001–2-1	5.8 Checking wording (including Table 2 — Methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES)

A.1.4 MRM 1.2 Risk Control Process

Table A.11 — MRM1.2 BP1

MRM.1.2 BP1: Identify proposed risk control measures for each identified risk. Use risk control measures in the following order — inherent control by design, protective measures, and information for assurance. Consider key properties in the following order — safety, effectiveness, and data and systems security when considering risk control options.	
Question:	**Guidance:**
MRM.1.2 BP1 Q.1 Are proposed risk control measures identified for every risk? **MRM.1.2 BP1 Q.2** How are risk control measures considered in relation to the key properties and prioritised?	Risk control measures shall be used in the following order, inherent control by design, protective measures, and information for assurance. Risk Control measures can include for example, Instructions and constraints documented as a change permit, network components, organizational considerations, or changes to the incorporated medical devices. For each risk, the design should carefully consider where to best implement the control to ensure sustainability, for example, by changes to the medical IT-network or manufacturer-authorized changes to the medical device. Consider key properties in the following order, safety, effectiveness, and data and systems security when considering risk control options. If, during risk control option analysis, the responsible organization determines that required risk reduction is not practicable, the responsible organization shall conduct and document a risk/benefit analysis of the residual risk.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.11 *(continued)*

Technical Report:	Section:
IEC 80001–2-1	5.6 RISK CONTROL measures (mitigations)
IEC 80001–2-1	6.1 Overview of the steps — Step 6
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK — Steps 6-10 (Figure 3) — Step 6
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures
IEC 80001–2-1	7.4.6.3 Select RISK CONTROL measure
IEC 80001–2-1	7.4.6.4 Re-evaluate RISK
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, Clause 6 to 6.2)
IEC 80001–2-1	Practical examples of steps 6 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3
IEC 80001–2-1	Figure D.1 — Application of Steps 5 and 6 with 3 levels of RISK acceptability
IEC 8001–2-2	For guidance for the HDO in the communication of security needs, risks, and controls please refer to IEC/TR 80001–2-2:2012 All Sections.
IEC 80001–2-3	For guidance on the identification of risk control measures related to wireless networks, please refer to all section of this Technical Report (with particular reference to Clause 5 and 8 and Annexes A and B.)
IEC 80001–2-4	For guidance on the identification of proposed risk control measures, please refer to all sections of this Technical Report

Table A.12 — MRM1.2 BP2

MRM.1.2 BP2: Manage Risk Control measures under the Change/Release Management process. Manage risk control measures that require a change to the Medical IT-Network under the Change Release Management process. Notify the medical device manufacturer (if a change is undertaken without documented consent of the manufacturer) and follow all necessary regulatory steps for putting such a modified medical device into service.	
Question:	**Guidance:**
MRM.1.2 BP2 Q.1 Are risk control measures managed under the Change/Release Management Process?	Risk Control measures shall be managed and implemented as per the Change/Release Management Process and recorded in the Medical IT-Network risk management file. Risk control measures within the medical device should only be implemented by the medical device manufacturer or by the responsible organization following the instructions for use or with the documented permission of the medical device manufacturer. Notify the medical device manufacturer (if a change to a medical device is undertaken without documented consent of the manufacturer) and follow all necessary regulatory steps for putting such a modified medical device into service. Changes to a medical device without documented consent of the medical device manufacturer are NOT recommended.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.7 Step 7: Implement RISK CONTROL measures
IEC 80001–2-2	All sections

Table A.13 — MRM1.2 BP3

MRM.1.2 BP3: Record selected risk control measures in the Medical IT-Network Risk Management File.	
Question:	**Guidance:**
MRM.1.2 BP3 Q.1 Are the selected risk control measures documented in the risk Management file?	The selected risk control measures shall be documented in the Medical IT-Network Risk Management File.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.13 *(continued)*

Technical Report:	**Section:**
IEC 80001–2-1	5.6 RISK CONTROL measures (mitigations)
IEC 80001–2-1	6.1 Overview of the steps — Step 6
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK — Steps 6-10 (Figure 3) — Step 6
IEC 80001–2-1	Figure 4 — Sample summary RISK ASSESSMENT register format
IEC 80001–2-1	7.4.6 Step 6: Identify and document proposed RISK CONTROL measures and re-evaluate RISK (return to Step 3)
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures
IEC 80001–2-1	7.4.6.3 Select RISK CONTROL measure
IEC 80001–2-1	7.4.6.4 Re-evaluate RISK
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, Clause 6 to 6.2)
IEC 80001–2-1	Practical examples of steps 6 are given in 8.2.3, 8.3.3, 8.4.3, and 8.5.3
IEC 80001–2-1	Figure D.1 — Application of Steps 5 and 6 with 3 levels of RISK acceptability
IEC 80001–2-1	Annex H (informative) Template for examples
IEC 80001–2-2	All Sections
IEC 80001–2-3	All section of this Technical Report (with particular reference to Clauses 5 and 8 and Annexes A and B.)

Table A.14 — MRM1.2 BP4

MRM.1.2 BP4: Conduct risk/benefit analysis and document results including residual risk. Conduct risk/benefit analysis of residual risk when risk reduction measures have been determined not to be practical. Document the results of the risk benefit analysis including residual risk in the Medical IT-Network risk management file.	
Question:	**Guidance:**
MRM.1.2 BP4 Q.1 Is risk/benefit analysis of residual risk conducted (when risk reduction measures have been determined not to be practical) and are the results documented?	A risk/benefit analysis of residual risk shall be conducted (when risk reduction measures have been determined not to be practical) and the results documented in the Medical IT-Network Risk Management File.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.5 RISK/benefit analysis
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, 6.5)
IEC 80001–2-1	Figure D.1 — Application of Steps 5 and 6 with 3 levels of RISK acceptability

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.15 — MRM1.2 BP5

MRM.1.2 BP5: Implement Risk Control measures. Where the estimated risk(s) are not acceptable, selected risk control measures are implemented according to risk control option analysis	
Question:	**Guidance:**
MRM.1.2 BP5 Q.1 Are selected risk control measures implemented? **MRM.1.2 BP5 Q.2** How are risk control measures implemented?	Implement selected risk control measures. Any residual risk shall be documented in the Medical IT-Network risk management file. Implement Risk control measures according to the Risk Control Process, where estimated risk(s) are not acceptable.
Technical Report:	**Section:**
IEC 80001–2-1	5.6 RISK CONTROL measures (mitigations)
IEC 80001–2-1	6.1 Overview of the steps — Step 7
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK — Steps 6-10 (Figure 3) — Step 7
IEC 80001–2-1	7.4.7 Step 7: Implement RISK CONTROL measures
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, 6.3)
IEC 80001–2-1	Practical examples of steps 7 are given in 8.2.3, 8.3.3, 8.4.3, and 8.5.3
IEC 80001–2-1	Annex G (informative) Example of Change Window Form
IEC 80001–2-2	All Sections
IEC 80001–2-3	All Sections

Table A.16 — MRM1.2 BP6

MRM.1.2 BP6: Verify and document the implementation and effectiveness of risk control measures. Verify the implementation and effectiveness of all risk control measures in the operational system and document in the Medical IT-Network Risk Management File.	
Question:	**Guidance:**
MRM.1.2 BP6 Q.1 Is the implementation and effectiveness of risk control measures verified and documented?	Verify the implementation and effectiveness of all risk control measures in the operational system and document in the Medical IT-Network Risk Management File. It might be necessary to verify the effectiveness of risk control measures in a test environment prior to implementation in the operational system.
Technical Report:	**Section:**
IEC 80001–2-1	6.1 Overview of the steps — Step 8 7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (IEC 80001 subclause 4.4.4.4)
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK — Steps 6-10 (Figure 3) — Step 8
IEC 80001–2-1	7.4.8 Step 8: Verify RISK CONTROL measures
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (IEC 80001 subclause 4.4.4.4)
IEC 80001–2-1	Practical examples of steps 8 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3
IEC 80001–2-1	Annex E (informative) MONITORING RISK mitigation effectiveness — E.1 to E.5
IEC 80001–2-1	Annex G (informative) Example of Change Window Form
IEC 80001–2-2	All Sections
IEC 80001–2-3	All Sections (with particular reference to 6.6.)

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.17 — MRM1.2 BP7

MRM.1.2 BP7: Review and evaluate risk control measures and operational system and document results. Review implemented risk control measures and the operational system for new unacceptable risks. Document the results of the evaluation in the Medical IT-Network risk management file.	
Question:	**Guidance:**
MRM.1.2 BP7 Q.1 Are risk control measures and the operational system reviewed and evaluated and are the results documented?	Review implemented risk control measures and the operational system for new unacceptable risks. Document the results of the evaluation in the Medical IT-Network risk management file.
Technical Report:	**Section:**
IEC 80001–2-1	6.1 Overview of the steps — Step 9
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK — Steps 6-10 (Figure 3) — Step 9
IEC 80001–2-1	7.4.9 Step 9: Verify RISK CONTROL measures
IEC 80001–2-1	7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, 6.6)
IEC 80001–2-1	Practical examples of steps 9 are given in 8.2.3, 8.3.3, 8.4.3, and 8.5.3

A.1.5 MRM 1.3 Residual Risk Process

Table A.18 — MRM1.3 BP1

MRM.1.3 BP1: Review residual risk. Individual residual risks and overall residual risks are assessed for acceptability by persons responsible for reviewing and accepting residual risk in co-operation with the Medical IT-Network Risk Manager.	
Question:	**Guidance:**
MRM.1.3 BP1 Q.1 Is residual risk reviewed and assessed for acceptability?	During the review of residual risk, the persons responsible for reviewing and accepting individual residual risk and overall residual risk do so in co-operation with the Medical IT-Network Risk Manager. The results of these activities shall be documented in the Medical IT-Network Risk Management File
Technical Report:	**Section:**
IEC 80001–2-1	5.7 Degrees of RISK
IEC 80001–2-1	6.1 Overview of the steps — Step 10
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK Steps 6-10 (Figure 3) — Step 10
IEC 80001–2-1	7.4.10 Step 10: Evaluate and report overall RESIDUAL RISK
IEC 80001–2-1	7.5 The steps and their relationship to IEC 80001–1 and ISO 14971 (ISO 14971, Clause 7)
IEC 80001–2-1	Practical examples of steps 10 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3.

Table A.19 — MRM1.3 BP2

MRM.1.3 BP2: Evaluate residual risk. Evaluate residual risk based on a pre-release assessment of the effectiveness of the implemented risk control measures.	
Question:	**Guidance:**
MRM.1.3 BP2 Q.1 Is residual risk evaluated?	Residual risk shall be evaluated against the pre-release assessment of the effectiveness of the implemented risk control measures.
Technical Report:	**Section:**
IEC 80001–2-1	5.7 Degrees of RISK

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.19 *(continued)*

IEC 80001–2-1	6.1 Overview of the steps — Step 10
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK Steps 6-10 (Figure 3) — Step 10
IEC 80001–2-1	7.4.10 Step 10: Evaluate and report overall RESIDUAL RISK
IEC 80001–2-1	7.5 The steps and their relationship to IEC 80001–1 and ISO 14971 (ISO 14971, Clause 7)
IEC 80001–2-1	Practical examples of steps 10 are given in 8.2.3, 8.3.3, 8.4.3, and 8.5.3.

Table A.20 — MRM1.3 BP3

MRM.1.3 BP3: Apply additional risk control measures. Apply additional risk control measures where an individual or the overall risk is not determined to be acceptable.	
Question:	**Guidance:**
MRM.1.3 BP3 Q.1 Are additional risk control measures applied for unacceptable individual/overall unacceptable risks?	Apply additional risk control measures where an individual or the overall risk is not determined to be acceptable.

Table A.21 — MRM1.3 BP4

MRM.1.3 BP4: Define and document residual risk summary.	
Question:	**Guidance:**
MRM.1.3 BP4 Q.1 Is residual risk summary designed and documented?	Define and document residual risk summary.
Technical Report:	**Section:**
IEC 80001–2-1	Figure 4 — Sample summary RISK ASSESSMENT register format
IEC 80001–2-1	7.2 Application of 4.4.2: Document all RISK MANAGEMENT elements
IEC 80001–2-1	Annex H (informative) Template for examples

Table A.22 — MRM1.3 BP5

MRM.1.3 BP5: Document risk/benefit analysis. Document risk/benefit analysis of the individual or overall residual risk against the health benefits accrued (where reduction of the residual risk to an acceptable level is not practicable).	
Question:	**Guidance:**
MRM.1.3 BP5 Q.1 Is risk/benefit analysis of individual or overall residual risk documented?	Document risk/benefit analysis of the individual or overall residual risk against the health benefits accrued from the incorporation of the medical device into the IT network (where reduction of the residual risk to an acceptable level is not practicable). See ISO 14971 for risk benefit analysis.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.5 Risk/benefit analysis 7.5 Table 3 — Relationship between this technical report, IEC 80001–1:2010 and ISO 14971:2007 (ISO 14971:2007, 6.5 and Clause 7)

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.23 — MRM1.3 BP6

MRM.1.3 BP6: Make decision on residual risk. Make a decision on whether or not to approve the residual risk on the basis of the documented risk/benefit analysis.	
Question:	**Guidance:**
MRM.1.3 BP6 Q.1 Is the decision on whether or not to approve the residual risk based on the documented risk/benefit analysis?	Make a decision on whether or not to approve the residual risk on the basis of the documented risk/benefit analysis.
Technical Report:	**Section:**
IEC 80001–2-1	5.7 Degrees of RISK
IEC 80001–2-1	6.1 Overview of the steps — Step 10
IEC 80001–2-1	6.2.3 RISK CONTROL and final RISK Steps 6-10 (Figure 3) — Step 10
IEC 80001–2-1	7.4.10 Step 10: Evaluate and report overall RESIDUAL RISK
IEC 80001–2-1	7.5 The steps and their relationship to IEC 80001–1 and ISO 14971 (ISO 14971, Clause 7)
IEC 80001–2-1	Practical examples of steps 10 are given in 8.2.3, 8.3.3, 8.4.3, and 8.5.3

A.1.6 CRCM.1 Change Release and Configuration Management Process

Table A.24 — CRCM.1 BP1

CRCM.1 BP1. Document and Apply Configuration Management process. Document configuration management process and apply during the risk management of change release management.	
Question:	**Guidance:**
CRCM.1 BP1 Q.1 Is Configuration Management process documented and applied during the risk management of change release management?	Document configuration management process and apply during the risk management of change release management. Documentation related to these activities shall be maintained in the Medical IT-Network Risk Management File.

Table A.25 — CRCM.1 BP2

CRCM.1 BP2: Document Configuration Management information. Document current configuration management information in the Medical IT-Network Risk Management file.	
Question:	**Guidance:**
CRCM.1 BP2 Q.1 Is configuration management information documented in the Medical IT-Network Risk Management File?	Document current configuration management information in the Medical IT-Network Risk Management file. A configuration management process shall be documented and applied to control the versions of the medical IT-network across all risk management processes during medical IT-network change-release management. The configuration management information can be included in the medical IT-network risk management file either through explicit documentation or by reference, for example, to a live database. This file shall contain the current configuration management information for the medical IT-network.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.26 — CRCM.1 BP3

CRCM.1 BP3: Document Change/Release Management Process. Document and apply change-release management (including Risk Management).	
Question:	**Guidance:**
CRCM.1 BP3 Q.1 Is the Change/Release Management Process documented?	Document and apply change-release management (including Risk Management). The medical IT-network risk manager shall ensure that a change-release management process exists for the medical IT-network and that the process includes risk management. It should be noted that unintended consequences can occur when two or more projects running in parallel are insufficiently coordinated. There is a single set of risk management documents per medical IT-network, because risk control measures for any given project or change must not conflict with existing risk control measures for the medical IT-network or with risk control measures proposed by a concurrent project.

Table A.27 — CRCM.1 BP4

CRCM.1 BP4: Use risk management process to determine acceptability of changes. Determine the approval and acceptability of changes using the results of the risk management process during the change-release process.	
Question:	**Guidance:**
CRCM.1 BP4 Q.1 Are the acceptability of changes determined using the risk management process.	Using the risk management process, determine the approval and acceptability of changes using the results of the risk management process during the change-release process.

Table A.28 — CRCM.1 BP5

CRCM.1 BP5: Implement action plans following the Change-Release management process.	
Question:	**Guidance:**
CRCM.1 BP5 Q.1 Are action plans implemented following the Change/Release Management Process?	Implement action plans following the Change-Release management process. For each change to the Medical IT-Network, the change Release Process is implemented. Action plans arising from risk assessment activities of risk analysis, risk evaluation, risk control, residual risk evaluation shall follow the change-release management process.

A.1.7 CRCM.2 Decision on how to apply Risk Management Process

Table A.29 — CRCM.2 BP1

CRCM.2 BP1: Implement Change-Release Management process. Implement the Change-release management process for any new medical IT-Network or a change to an existing medical IT-Network.	
Question:	**Guidance:**
CRCM.2 BP1 Q.1 Is the Change-Release Management Process implemented?	Implement the Change-release management process for any new medical IT-Network or a change to an existing medical IT-Network.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.30 — CRCM.2 BP2

CRCM.2 BP2: Consider the nature of the change. 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.	
Question:	**Guidance:**
CRCM.2 BP2 Q.1 Has the nature of the change been identified?	Consider the nature of the change to decide whether the requirements are met by an applicable change permit. Where no applicable change permit exists, a medical IT-network project shall be initiated.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures Annex F (informative) RISK ANALYSING small changes in a MEDICAL IT-NETWORK
IEC 80001–2-1	All sections — Guidance for Large and Small Organizations

Table A.31 — CRCM.2 BP3

CRCM.2 BP3: Define change permit. Define change permit and specify what records are to be kept for each permitted change.	
Question:	**Guidance:**
CRCM.2 BP3 Q.1 Has a change permit been defined and have records of what is to be kept for each permitted change been specified?	Define change permit and specify what records are to be kept for each permitted change. If the responsible organization decides, as a result of risk management activities, that a specified type of routine change may be performed with acceptable risk, subject to specified constraints, then the responsible organization may define a change permit which allows such routine changes and specifies the constraints.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures Annex F (informative) RISK ANALYSING small changes in a MEDICAL IT-NETWORK

Table A.32 — CRCM.2 BP4

CRCM.2 BP4: Specify the constraints of the change permit.	
Question:	**Guidance:**
CRCM.2 BP4 Q.1 Have the constraints of the change permit been specified?	Specify the constraints of the change permit. For example, a change permit might allow varying the number of medical devices of a specified type in a medical IT-network within a specified range. Provided that the changes performed always conform to the change permit and its limitations, no change-release management or risk management is needed each time the change permit is used. Change permits can only be established as an outcome of the risk management process.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures Annex F (informative) RISK ANALYSING small changes in a MEDICAL IT-NETWORK

Table A.33 — CRCM.2 BP5

CRCM.2 BP5: Implement routine change. Implement routine change once change permit has been defined and the constraints have been specified.	
Question:	**Guidance:**
CRCM.2 BP5 Q.1 Have routine changes been implemented according to the change permit?	Implement routine change once change permit has been defined and the constraints have been specified.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.34 — CRCM.2 BP6

CRCM.2 BP6: Document Change permits. Document change permits and maintain in the Medical IT- Network Risk Management File.	
Question:	**Guidance:**
CRCM.2 BP6 Q.1 Are change permits documented and maintained in Medical IT-Network Risk Management File?	Document change permits and maintain in the Medical IT-Network Risk Management File.
Technical Report:	**Section:**
IEC 80001–2-1	7.4.6.2 Identify RISK CONTROL measures Annex F (informative) RISK ANALYSING small changes in a MEDICAL IT-NETWORK

Table A.35 — CRCM.2 BP7

CRCM.2 BP7: Establish project plan. Establish project plan for specific circumstances that have the potential to introduce new risk (not covered by change permit).	
Question:	**Guidance:**
CRCM.2 BP7 Q.1 Has a project plan been established?	Establish and maintain a project plan for the incorporation of a new type of medical device into an IT-network, for change to the medical IT-network, for change to the medical devices incorporated in the medical IT-network, for decommissioning of a medical device or medical IT-network, or any other activity that has the potential to introduce new risk. The project plan shall provide: *requirements for risk management activities including the following:* — activities to establish or update any risk management file documents needed as a result of this project, such as the risk management plan or other risk Management documents; — a plan to meet the requirements stated in the risk management plan for the affected medical IT-network(s); — activities for verification of risk control measures. *a description of the project including the following:* — identification of medical IT-network(s) developed or affected by the project; — requirements specification for the project; — specification of minimum set of documents required for the medical IT-network project. *the scope of the planned changes to the medical IT-network, including but not limited to the following:* — physical and logical configuration of the medical IT-network before and after the planned changes; — information flow before and after the planned changes; — components to be acquired or removed; — specifications of non-medical network components where relevant; — constraints on the extendability of the existing medical IT-network.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.36 — CRCM.2 BP8

CRCM.2 BP8: Maintain and revise Project Plan. Maintain project plan and revise to reflect changes to the project.	
Question:	**Guidance:**
CRCM.2 BP8 Q.1 Has the project plan been maintained and revised to reflect changes to the project?	Maintain project plan and revise to reflect changes to the project. Where changes to the IT-Network occur frequently, the project plan may be established as a reusable protocol document containing all these essential elements.

Table A.37 — CRCM.2 BP9

CRCM.2 BP9: Document Project plan. Document the project plan in the Medical IT-Network Risk management file.	
Question:	**Guidance:**
CRCM.2 BP9 Q.1 Has the project Plan been documented?	Document the project plan in the Medical IT-Network Risk management file.

A.1.8 CRCM.3 Go-Live Process

Table A.38 — CRCM.3 BP1

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.	
Question:	**Guidance:**
CRCM.3 BP1 Q.1 Is residual risk reviewed in the context of recent or pending changes prior to go-live?	Prior to going live, review all residual risk summaries (from changes or projects) for acceptability of risk associated with interactions of recent or pending projects or changes

Table A.39 — CRCM.3 BP2

CRCM.3 BP2: Approve specified change. Approval is given for the specified change by the Medical IT-Network Risk Manager prior to go-live.	
Question:	**Guidance:**
CRCM.3 BP2 Q.1 Have the specified changes been approved prior to go-live?	Approval is given for the specified change by the Medical IT-Network Risk Manager prior to go-live.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.40 — CRCM.3 BP3

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.	
Question:	**Guidance:**
CRCM.3 BP3 Q.1 Is approval of residual risk documented?	Document the approval of the Medical IT-Network residual risk in the Medical IT-Network risk management file.

A.1.9 LNRM.1 Monitoring Process

Table A.41 — LNRM.1 BP1

LNRM.1 BP1: Establish process outlining monitoring requirements. Establish a process which outlines the monitoring requirements as part of the risk management plan to monitor each installed Medical IT-Network.	
Question:	**Guidance:**
LNRM.1 BP1 Q.1 Has a process for monitoring of the live network been established?	Establish a process which outlines the monitoring requirements as part of the risk management plan to monitor each installed Medical IT-Network for emerging risks, effectiveness of risk control measures, and accuracy of original estimations of risk.
Technical Report:	**Section:**
IEC 80001–2-3	7.2 Network and application management

Table A.42 — LNRM.1 BP2

LNRM.1 BP2: Include monitoring requirements as part of the risk management plan.	
Question:	**Guidance:**
LNRM.1 BP2 Q.1 Are requirements for monitoring included in the risk management plan?	Include monitoring requirements as part of the risk management plan. Examples of what to monitor are the following: — environment changes (including local/connected environment as well as relevant network or component DATA AND SYSTEMS SECURITY vulnerabilities); — operational/performance feedback, e.g. user feedback, speed problems, high error rates, failure, malicious software attacks; — information about the incorporated components; — information about similar medical IT-networks; — reported events; — auditing of non-technical risk control measures such as organizational policies and procedures.

Table A.43 — LNRM.1 BP3

LNRM.1 BP3: Initiate Event Management process. Initiate the Event Management process where monitoring indicates actual or potential increase in risk.	
Question:	**Guidance:**
LNRM.1 BP3 Q.1 Has event management process been initiated where monitoring indicates actual or potential increase in risk?	Initiate the Event Management process where monitoring indicates actual or potential increase in risk associated with the medical IT-network or its components (potential or actual negative impact). Significant findings shall be reported to the appropriate party in the responsible organization. In some cases, the responsible organization might be required to report observations to regulatory bodies.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

A.1.10 LNRM.2 Event Management Process

Table A.44 — LNRM.2 BP.1

LNRM.2 BP1: Establish Event Management Process. Establish Event Management process to ensure that negative events are captured and documented.	
Question:	**Guidance:**
LNRM.2 BP1 Q.1 Has an event management process been established? **LNRM.2 BP1 Q.2** Are negative events captured and documented?	Establish Event Management process to ensure that negative events are captured and documented.

Table A.45 — LNRM.2 BP.2

LNRM.2 BP2: Evaluate events and proposed changes arising from events. Evaluate events and proposed changes arising from events.	
Question:	**Guidance:**
LNRM.2 BP2 Q.1 Are events and proposed changes arising from events evaluated?	Evaluate events and proposed changes arising from events as appropriate through the Change Release Management Process.

Table A.46 — LNRM.2 BP.3

LNRM.2 BP3: Manage proposed changes. Manage proposed changes through the change-release management process.	
Question:	**Guidance:**
LNRM.2 BP3 Q.1 Are post event proposed changes managed through the change-release management process?	Manage proposed changes through the change-release management process.

Table A.47 — LNRM.2 BP.4

LNRM.2 BP4: Track corrective and preventive actions. Track all corrective and preventive actions leading to closure.	
Question:	**Guidance:**
LNRM.2 BP4 Q.1 Are corrective and preventive actions tracked to closure?	Track all corrective and preventive actions leading to closure.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.48 — LNRM.2 BP.5

LNRM.2 BP5: Report significant finds. Report significant finds to the medical IT-network risk manager and/or others in the responsible organization.	
Question:	**Guidance:**
LNRM.2 BP5 Q.1 Are significant finds reported?	Report significant finds to the medical IT-network risk manager and/or others in the responsible organization.

A.1.11 MDP.1 Medical IT-Network Planning Process

Table A.49 — MDP.1 BP.1

MDP.1 BP1: Establish Risk Management plan. Establish risk management plan for each Medical IT-Network for risk management activities.	
Question:	**Guidance:**
MDP.1 BP1 Q.1 Has a risk management plan been established for each Medical IT-Network?	Establish risk management plan for each Medical IT-Network for risk management activities. The risk management plan shall include the following: — a description of the medical IT-network, including: — identified stakeholders within the responsible organization that shall be informed about hazards to ensure their risk awareness; — the defined use and expected benefits of the medical IT-network; — the reason for each medical device incorporation; — the use of each medical device, due to its incorporation into the medical IT-network that is not included in the manufacturer's intended use; — a description of activities, roles, and responsibilities for all parties involved in operating/maintaining the medical IT-network, with respect to risk management.; — requirements for monitoring the medical IT-network, criteria for risk acceptability, based on the responsible organization's policy for determining acceptable risk, including criteria for accepting risks when the probability of occurrence of harm cannot be estimated.
Technical Report:	**Section:**
IEC 80001–2-3	5 Wireless MEDICAL IT-NETWORKS: planning and design

Table A.50 — MDP.1 BP.2

MDP.1 BP2: Plan risk management. Plan risk management activities considering the current state of the IT network and planned changes.	
Question:	**Guidance:**
MDP.1 BP2 Q.1 Has risk management been planned considering the current state of the IT network and planned changes?	Plan risk management activities considering the current state of the IT network and planned changes. The responsible organization shall plan risk management of the medical IT-network by providing — risk-relevant asset description, — IT-network documentation, and — a risk management plan for the medical IT-network. Assessment and documentation of the structure of the network is essential to provide the necessary information for risk analysis and risk evaluation. Because of the nature of IT-networks, both the current state of the IT-network and planned changes shall be considered.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.50 *(continued)*

Technical Report:	**Section:**
IEC 80001–2-3	All Sections
IEC 80001–2-4	5.4.3 Development status 5.4.3 of MEDICAL IT-NETWORK

Table A.51 — MDP.1 BP.3

MDP.1 BP3: Initiate project. Initiate a project for the development of a new Medical IT-Network or for changes which are not covered by documented change permits.	
Question:	**Guidance:**
MDP.1 BP3 Q.1 Has a project been initiated for the development of a new Medical IT-Network or for changes which are not covered by documented change permits?	Initiate a project for the development of a new Medical IT-Network or for changes which are not covered by documented change permits. Initial development of new medical IT-networks as well as changes to existing medical IT-networks not covered by documented change permits shall be managed by projects. A medical IT-network can have multiple concurrent or sequential projects.
Technical Report:	**Section:**
IEC 80001–2-3	All Sections
IEC 80001–2-4	4.3 Large RESPONSIBLE ORGANIZATION — points to consider
IEC 80001–2-4	5.4.1 Performing a RISK ASSESSMENT

Table A.52 — MDP.1 BP.4

MDP.1 BP4: Maintain and update risk management plan. Risk Management plan is maintained and updated when a project introduces changes to an existing Medical IT-Network.	
Question:	**Guidance:**
MDP.1 BP4 Q.1 Has the risk management plan been maintained and updated when a project changes an existing Medical IT-Network?	Risk Management plan is maintained and updated when a project introduces changes to an existing Medical IT-Network.

Table A.53 — MDP.1 BP.5

MDP.1 BP5: Establish document control procedure.	
Question:	**Guidance:**
MDP.1 BP5 Q.1 Has a document control procedure been established?	Establish document control procedure.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015

Table A.54 — MDP.1 BP.6

MDP.1 BP6: Maintain documents as per the document control procedure. Revise, amend, review, and approve all relevant documents in the medical IT-network life cycle in accordance with the document control procedure.	
Question:	**Guidance:**
MDP.1 BP6 Q.1 Are documents maintained and approved as per the document control procedure?	Revise, amend, review, and approve all relevant documents in the medical IT-network life cycle in accordance with the document control procedure.

Table A.55 — MDP.1 BP.7

MDP.1 BP7: Provide traceability for each identified hazard. Provide traceability for each identified hazard within the Medical IT-Network risk management file.	
Question:	**Guidance:**
MDP.1 BP7 Q.1 Has traceability been provided for each identified hazard?	Provide traceability for each identified hazard within the Medical IT-Network risk management file. The medical IT-network risk management file shall provide traceability for each identified hazard to the following: — the risk analysis; — the risk evaluation; — the implementation and verification of the risk control measures; — the assessment of the acceptability of any residual risk(s) with approval. The records and other documents that make up the medical IT-network risk management file can form part of other documents and files. The medical IT-network risk management file need not physically contain all the records and other documents; however, it should contain at least references or pointers to all required documentation. The responsible organization should be able to assemble the information referenced in the medical IT-network risk management file in a timely fashion. The medical IT-network risk management file can be in any form or type of medium. In those organizations where an “assurance case” is the means of organizing the medical IT-network risk management file, refer to ISO/IEC 15026-2 (under development) for more information.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 80001-2-7:2015