Technical Information Report

AAMI/ISO TIR80001-2-7:2014

Application of risk management for IT-networks incorporating medical — Application guidance — Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

AAMI
Advancing Safety in Healthcare Technology

Application of risk management for IT-networks incorporating medical — Application guidance — Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

Approved 24 October 2014 by
Association for the Advancement of Medical Instrumentation

Registered 24 December 2014 by
American National Standards Institute

Abstract: The purpose of this technical report is to provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1. The purpose of this Technical Report is to:

1) provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1
2) provide an exemplar assessment method which can be used by HDOs in varying contexts to assess themselves against IEC 80001-1
3) 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
4) 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 technical report does not introduce any requirements in addition to those expressed in IEC 80001-1.

Keywords: risk management, IT-network, HDO, self-assessment

Published by

Association for the Advancement of Medical Instrumentation
4301 N Fairfax Drive, Suite 301
Arlington, VA 22203-1633

Printed in the United States of America

ISBN 1-57020-579-5

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. For a TIR, AAMI consults with a technical committee about five years after the publication date (and periodically thereafter) for guidance on whether the document is still useful—that is, to check that the information is relevant or of historical value. If the information is not useful, the TIR is removed from circulation.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

ANSI Registration

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

Contents

Page

Glossary of equivalent standards

International Standards adopted in the United States may include normative references to other International Standards. AAMI maintains a current list of each International Standard that has been adopted by AAMI (and ANSI). Available on the AAMI website at the address below, this list gives the corresponding U.S. designation and level of equivalency to the International Standard.

www.aami.org/standards/glossary.pdf

Committee representation

Association for the Advancement of Medical Instrumentation

AAMI/SM/WG 02, Information Technology Networks Working Group

The adoption of the ISO 80001-2-7 as a new AAMI/ISO Technical Information Report was initiated by the AAMI Information Technology Working Group.

Committee approval of the standard does not necessarily imply that all committee members voted for its approval.

At the time this document was published, the **AAMI Information Technology Networks Working Group** had the following members:

Chair: Bill Hintz, Medtronic Inc

Members:
John Collins, American Hospital Association
Todd Cooper
Becky Crossley, Susquehanna Health
Conor Curtin, Fresenius Medical Care
Yadin David, Biomedical Engineering Consultants LLC
Richard De La Cruz, Hospira Worldwide Inc
Christina DeMur, Draeger Medical Systems Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Kurt Elliason, Smiths Medical
Jim Gabalski, Getinge USA
George Gray, Ivenix Inc
Thomas Grobaski, Belimed Inc
Catherine Li, FDA/CDRH
Yimin Li, St Jude Medical Inc
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, Mary Beth McDonald Consulting
Dave Osborn, Philips Electronics North America
Geoff Pascoe
Steven Rakitin, Software Quality Consulting
Rick Schrenker, Massachusetts General Hospital
Neal Seidl, GE Healthcare
Xianyu Shea, Stryker Medical Division
Ray Silkaitis, Amgen Inc
Bob Steurer, Spacelabs Medical Inc
Donna-Bea Tillman, Biologics Consulting Group
Daidi Zhong, Chongqing University

Alternates:
Denise Adams, B Braun of America Inc
James Dundon, Spacelabs Medical Inc
Brian Fitzgerald, FDA/CDRH
Rich Gardner, GE Healthcare
Andrew Northup, Medical Imaging & Technology Alliance a Division of NEMA
Phil Raymond, Philips Electronics North America
Thomas Schultz, Medtronic Inc WHQ Campus
Chandresh Thakur, CareFusion
Fei Wang, Fresenius Medical Care

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Background of AAMI adoption of ISO TR 80001-2-7 Ed.1

As indicated in the foreword to the main body of this document, the International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. The United States is one of the ISO members that took an active role in the development of this technical report.

International Technical Report ISO TR 80001-2-7 Ed.1 was developed jointly by Sub-Committee IEC/SC 62A, Common aspects of electrical equipment used in medical practice and ISO/TC 215, Health informatics, to define the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security.

U.S. participation in this IEC SC is organized through the U.S. Technical Advisory Group for IEC/SC 62A, administered by AAMI on behalf of the American National Standards Institute (ANSI).

AAMI encourages its committees to harmonize their work with international documents as much as possible. The AAMI Information Technology Working Group, together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed ISO TR 80001-2-7 Ed.1 to formulate the U.S. position while the document was being developed. This close collaboration helped gain widespread U.S. consensus on the document. As the U.S. Technical Advisory Group for IEC/SC 62A, the AAMI Information Technology Networks Working Group voted to adopt the IEC Technical Report as written.

AAMI has adopted other ISO documents. See the Glossary of Equivalent Standards for a list of ISO standards adopted by AAMI, which gives the corresponding U.S. designation and the level of equivalency with the ISO standard.

The concepts incorporated into this technical report should not be considered inflexible or static. This technical information report, like any other, must be reviewed and updated periodically to assimilate progressive technological developments. To remain relevant, it must be modified as technological advances are made and as new date comes to light.

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Suggestions for improving this TIR are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N Fairfax Drive, Suite 301, Arlington VA 22203-1633

NOTE—Beginning with the ISO foreword on page viii, AAMI/ISO TIR 80001-2-7 Ed.1, *Application of risk management for IT-networks incorporating medical — Application guidance — Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-* is identical to ISO/TR 80001-2-7 Ed.1.

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/IEC TR 80001-2-7 was prepared by Technical Committee ISO/TC 215, *Heath informatics*, Subcommittee SC , .

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 disclosure and communication of medical device security needs, risks and controls*

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

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

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

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

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

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

Introduction

This technical report provides guidance for a Healthcare Delivery Organization (HDO) that wishes to self-assess its implementation of the processes of IEC 80001-1. This technical report can be used to assess Medical IT-Network projects where IEC 80001-1 has been determined to be applicable. This technical report 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 technical report The PRM and PAM can be used to provide a standardized basis for tailoring the exemplar assessment method where required.

This Technical Report can be used in a number of ways including:

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

2) 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.

3) 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 Technical Report. 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 technical report provides:

- 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
- can be tailored on a standardized 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

Application of risk management for IT-networks incorporating medical — 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 technical report is to provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1. The purpose of this Technical Report is to:

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

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

3) 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

4) 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 technical report does not introduce any requirements in addition to those expressed in IEC 80001-1.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this document. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to 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 15504-1:2004, *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 technical report, 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 technical report is based on the processes and practices as defined in the PRM and PAM which are presented in the appendices of this technical report. 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 of this technical report, 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 perform 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

NOTE In order to produce a repeatable and consistent approach to assessment, the assessment is carried out in a number of stages. A 7 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 stages1 and 2 of the assessment process is provided in Annex 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 Annex A Clause 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 Annex 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 subclause 4.4 of this technical report. 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 Annex 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 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 Annex C, subclause C.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 subclause 4.42.

4.4.2 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 technical report 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 perfomed 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 technical report 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 Introduction

This clause contains a set of exemplar assessment questions for each of the 14 processes which are defined in the PRM and PAM contained in the appendices B and C of this technical report. 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 another technical report in the IEC 80001-1 series, 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 technical report. 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 technical report 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 of this technical report.

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:**
80001-2-1	7.4.6.2 Identify RISK CONTROL measures
80001-2-1	7.4.6.4 Re-evaluate RISK
80001-2-1	7.4.6.5 RISK/benefit analysis
80001-2-1	7.4.7 Step 7 Implement RISK CONTROL measures
80001-2-1	7.4.8.2 VERIFICATION of effectiveness
80001-2-1	7.4.9 STEP 9: Evaluate any new RISKS arising from RISK CONTROL
80001-2-1	7.4.10 STEP 10: Evaluate and report overall RESIDUAL RISK (in ref to documenting individual residual risks and overall residual risk
80001-2-1	Figure 8 – Sample summary RISK ASSESSMENT register for the PACU example
80001-2-1	E.6 VERIFICATION of the design and execution of the RISK MANAGEMENT PROCESS
80001-2-1	Annex F RISK ANALYZING small changes in a MEDICAL IT-NETWORK (Figure F.1)
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.
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:**
80001-2-1	7.4.6.2 Identify RISK CONTROL measures
80001-2-1	7.4.6.4 Re-evaluate RISK
80001-2-1	7.4.6.5 RISK/benefit analysis
80001-2-1	7.4.7 Step 7 Implement RISK CONTROL measures
80001-2-1	7.4.8.2 VERIFICATION of effectiveness
80001-2-1	7.4.9 STEP 9: Evaluate any new RISKS arising from RISK CONTROL
80001-2-1	7.4.10 STEP 10: Evaluate and report overall RESIDUAL RISK (in ref to documenting individual residual risks and overall residual risk
80001-2-1	Figure 8 – Sample summary RISK ASSESSMENT register for the PACU example
80001-2-1	E.6 VERIFICATION of the design and execution of the RISK MANAGEMENT PROCESS
80001-2-1	Annex F RISK ANALYZING small changes in a MEDICAL IT-NETWORK (Figure F.1)
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 & 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
IEC 80001-2-1	7.5 - Table 3 – Relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007(14971 Clause/subclause 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, Analyze 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, analyze and evaluate associated risk for each identified hazard throughout the life cycle?	Consider how to estimate, analyze 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 (14971 Clause/subclause 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

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 prioritized?	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, organisational 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.
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(14971 Clause/subclause 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 TR (with particular reference to sections 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.
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(14971 Clause/subclause 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 TR (with particular reference to sections 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(14971 Clause/subclause 6.5)
IEC 80001-2-1	Figure D.1 – Application of STEPs 5 and 6 with 3 levels of RISK acceptability

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(14971 Clause/subclause 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:**
IEC80001-2-1	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(80001 subclause 4.4.4.4)
IEC80001-2-1	6.2.3 RISK CONTROL and final RISK – Steps 6 – 10 (Figure 3) – Step 8
IEC80001-2-1	7.4.8 STEP 8: Verify RISK CONTROL measures
IEC80001-2-1	7.5 Table 3 – Relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007(80001 subclause 4.4.4.4)
IEC80001-2-1	Practical examples of steps 8 are given in 8.2.3, 8.3.3, 8.4.3 and 8.5.3
IEC80001-2-1	Annex E (informative) MONITORING RISK mitigation effectiveness – E.1 to E.5
IEC80001-2-1	Annex G (informative) Example of Change Window Form
IEC 80001-2-2	All Sections
IEC80001-2-3	All Sections (with particular reference to sections 6.6.)

Table A.17 — MRM1.2 BP7

MRM.1.2 BP7: Review and evaluate risk control measures & 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(14971 Clause/subclause 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 (14971 Clause/subclause 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
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 (14971 Clause/subclause 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 Subclause 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(14971 Clause/subclause 6.5 and 7)

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 (14971 Clause/subclause 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 & Configuration Management Process

Table A.24 — CRCM.1 BP1

CRCM.1 BP1. Document & 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.

Table A.26 — CRCM.1 BP3

CRCM.1 BP3: Document Change/Release Process. Document and apply change-release management (including Risk Management).	
Question:	**Guidance:**
CRCM.1 BP3 Q.1 Is the Change/Release 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.

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.

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:**
IEC80001-2-1	7.4.6.2 Identify RISK CONTROL measures, Annex F (informative) RISK ANALYZING small changes in a MEDICAL IT-NETWORK
IEC 80001-2-1	All sections – Guidance for Large and Small Organisations

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 organisation 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 organisation 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 ANALYZING 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 ANALYZING 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.

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 ANALYZING 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:* • 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); and • activities for verification of risk control measures. *a description of the project including:* • identification of medical IT-network(s) developed or affected by the project; • requirements specification for the project; and • 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:* • 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; and • constraints on the extendibility of the existing medical IT-network.

Table A.36 — CRCM.2 BP8

CRCM.2 BP8: Maintain & 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.1.6 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.

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.1.7 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: • 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; and • 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.

A.1.8 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.

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.1.9 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: • 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; and • 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.
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 project 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.

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 risk analysis; • the risk evaluation; • the implementation and verification of the risk control measures; and • 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.

A.1.10 MDP.2 Medical IT-Network Documentation Process

Table A.56 (1 of 2) — MDP.2 BP.1

MDP.2 BP1: Obtain/Provide additional documentation for the connection of a medical device to an IT network. Obtain (Responsible organisation) /Provide (medical device manufacturer) instructions for implementing the connection of a medical device to an IT network.	
Question:	**Guidance:**
MDP.2 BP1 Q.1 Has additional documentation for the connection of a medical device to an IT network been provided?	Obtain instructions for implementing the connection of a medical device to an IT network. The Responsible organisation shall ensure that the medical device manufacturer shall make available, instructions for implementing such connection, including but not limited to the following: • the purpose of the medical device’s connection to an IT-network; • the required characteristics for the IT-network incorporating the medical device; • the required configuration of the IT-network incorporating the medical device; • the technical specifications of the network connection of the medical device including security specifications; • the intended information flow between the medical device, the medical IT-network and other devices on the medical IT-network and, if relevant to the key properties, the intended routing through the medical it-network; and • a list of the hazardous situations resulting from a failure of the IT-network to provide the characteristics required to meet the purpose of the medical device connection to the IT-network.

Table A.56 (2 of 2) – MDP.2 BP.1

Question:	Guidance:
	Compliance is checked by availability of the medical device manufacturer's accompanying documents and other available instructions for implementing such connection. Where the content made available does not meet the responsible organization's risk management need, additional content can be made available under a responsibility agreement. Pursuant to applicable regulations and relevant standards, the responsible organisation shall ensure that each provider of other information technology (equipment and/or software) shall make available documentary information applicable to the technology being supplied as follows: • technical descriptions and technical manuals; • required IT-network characteristics; • recommended product configurations; • known incompatibilities and restrictions; • operating requirements; • product corrective actions and recalls; and • cyber security notices (warnings of known security vulnerabilities). Compliance is checked by confirming the availability of the documentary information from each provider of other information technology. Where the content made available does not meet the responsible organization's risk management need, additional content can be made available under a responsibility agreement. The responsible organization shall obtain supplementary documentary information for other information technology as necessary to further support the risk management activities of the medical IT-network. Examples of supplementary information are: • test strategies and test acceptance criteria; • disclosure of failure modes; • system reliability statistics; • safety assurance cases; and • performance

Table A.57 — MDP.2 BP.2

MDP.2 BP2: Maintain accompanying documents in the Medical IT-Network risk management file. Maintain documents and additional documentation (obtained for a medical device incorporated into an IT network) as required for risk management purposes in the Medical IT-Network Risk Management file.	
Question:	**Guidance:**
MDP.2 BP2 Q.1 Are accompanying documents maintained in the Medical IT-Network Risk Management File?	Maintain documents and additional documentation (obtained for a medical device incorporated into an IT network) as required for risk management purposes in the Medical IT-Network Risk Management file.

Table A.58 — MDP.2 BP.3

MDP.2 BP3: Maintain risk relevant asset description. Maintain risk relevant asset description, including a list of assets of IT networks interfacing with medical devices, as part of the risk management process.	
Question:	**Guidance:**
MDP.2 BP3 Q.1 Has a risk relevant asset description been maintained?	Maintain risk relevant asset description, including a list of assets of IT networks interfacing with medical devices, as part of the risk management process. The responsible organization shall plan risk management of the medical IT-network by providing a risk-relevant asset description. Typical assets include, but are not limited to hardware, software, and data essential to the intended use of the medical device and the defined use of the medical IT-network. The asset list may include for example: • specific components of the medical IT-network and all incorporated medical devices and other equipment (e.g. image creating modalities, network components) of the IT infrastructure; • operational characteristics of the IT infrastructure of the medical IT-network (e.g. performance properties such as bandwidth); • configuration management information; • medical application software; • data about configuration of hardware and software; • characterization of identifiable patient data on the medical IT-network or used by the incorporated medical device including its nature, volume, and sensitivity; • healthcare procedure support information, including history of use and operator/user details; and • a security description and other materials relevant to total system safety considerations (in case security is an aspect of safety). The responsible organization shall establish and maintain network documentation necessary to support the risk management of the medical IT-network for the interfaces between the medical device(s) and all network components (both software and hardware). This documentation shall include but not be limited to: • physical and logical network configuration; The network configuration includes defining the boundaries of the network. Documentation can contain IT-Network electrical properties that might impact the performance of the Medical IT-network and incorporated devices. Examples include, but are not limited to, grounding, galvanic (de)coupling, stray currents, and power over Ethernet. • applied standards and conformance statements; • physical and logical client/server structure; • network security, reliability and data integrity; • network communication requirements for each medical device as specified by the manufacturer; and • future (planned/reasonably foreseeable) changes/upgrades/enhancements.
Technical Report:	**Section:**
IEC 80001-2-4	5.4.2.1 Understanding of the components of the MEDICAL IT-NETWORK
IEC 80001-2-4	5.4.2.2 Small RESPONSIBLE ORGANIZATION – points to consider.

A.1.11 MDP.3 Responsibility Agreements Process

Table A.59 — MDP.3 BP.1

MDP.3 BP1: Determine the need for a responsibility agreement. Determine the need for one or more documented responsibility agreements whenever a medical device is incorporated into an IT network or the configuration of such a connection is changed.	
Question:	**Guidance:**
MDP.3 BP1 Q.1 Has the need for a responsibility agreement(s) been determined?	Determine the need for one or more documented responsibility agreements whenever a medical device is incorporated into an IT network or the configuration of such a connection is changed.
Technical Report:	**Section:**
IEC 80001-2-3	8.12 External partnering with both MEDICAL DEVICE and networking manufacturer
IEC 80001-2-4	5.4.5 External IT and bio-medical engineering support
IEC 80001-2-4	6 RESPONSIBILITY AGREEMENTS

Table A.60 — MDP.3 BP.2

MDP.3 BP2: Define the responsibilities of stakeholders within the responsibility agreement.	
Question:	**Guidance:**
MDP.3 BP2 Q.1 Do the responsibility agreement(s) define the responsibilities of stakeholders?	Define the responsibilities of stakeholders within the responsibility agreement. A responsibility agreement may cover one or more projects or the maintenance of one or more medical IT-networks, and shall identify responsibility for all aspects of the medical IT-network life cycle and all activities that form part of that life cycle. The responsibility agreements shall contain (or refer to documents which contain) at a minimum: • the name of the person responsible for risk management for the activities covered by the responsibility agreement; • the scope of the activities covered by the responsibility agreement, including a summary of and/or reference to the requirements; • a list of the medical devices and other equipment which are to be incorporated into the IT-network or changed, together with the names of medical device manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project; • a list of documents to be supplied by the medical device manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT-network; • technical information to be supplied by the medical device or IT manufacturers and other equipment suppliers that is necessary to perform risk analysis for the IT-network; and • definition of roles and responsibilities in managing potentially adverse events. The responsible organization shall provide a summary of responsibilities as appropriate. If the co-operation of manufacturers of medical devices, suppliers of other equipment or other organizations is necessary in addition to the listed documents supplied by the manufacturers or organizations, a responsibility agreement shall: • identify the nature of the co-operation required; and
	h) state: • Who is responsible for requesting such co-operation? • Who is responsible for responding to such requests? • What criteria will be used to judge the adequacy of such response? Since this information can change through the lifecycle of a medical IT-network, it is recommended that it be updated periodically in the responsibility agreement.
Technical Report:	**Section:**
IEC 80001-2-3	8.12 External partnering with both MEDICAL DEVICE and networking manufacturer
IEC 80001-2-4	5.4.5 External IT and bio-medical engineering support
IEC 80001-2-4	6 RESPONSIBILITY AGREEMENTS

Table A.61 — MDP.3 BP.3

MDP.3 BP3: Define the scope of the responsibility agreement. Define the scope of the responsibility agreement including whether the agreement applies to one or more project or the maintenance of one or more Medical IT-Networks. Compliance is checked by inspection of the Medical IT-Network risk management file.	
Question:	**Guidance:**
MDP.3 BP3 Q.1 Has the scope of the responsibility agreement(s) been defined and documented?	Define the scope of the responsibility agreement including whether the agreement applies to one or more project or the maintenance of one or more Medical IT-Networks. Compliance is checked by inspection of the Medical IT-Network risk management file.
Technical Report:	**Section:**
IEC 80001-2-3	8.12 External partnering with both MEDICAL DEVICE and networking manufacturer
IEC 80001-2-4	5.4.5 External IT and bio-medical engineering support
IEC 80001-2-4	6 RESPONSIBILITY AGREEMENTS

A.1.12 MDP.4 Risk Management Policy Process

Table A.62 — MDP.4 BP.1

MDP.4 BP1: Establish Risk Management Policy. Risk Management policy outlines criteria for determining acceptable risk, taking into account relevant international standards and national or regional regulations.	
Question:	**Guidance:**
MDP.4 BP1 Q.1 Has a risk management policy been established?	Top Management ensure that a risk Management policy is established and that it outlines criteria for determining acceptable risk, taking into account relevant international standards and national or regional regulations.
Technical Report:	**Section:**
IEC 80001-2-4	1.4 Prerequisites
IEC 80001-2-4	4.1 TOP MANAGEMENT responsibilities
IEC 80001-2-4	4.3 Large RESPONSIBLE ORGANIZATION – points to consider

Table A.63 — MDP.4 BP.2

MDP.4 BP2: Document Risk Management Policy with the Medical IT-Network Risk Management file.	
Question:	**Guidance:**
MDP.4 BP2 Q.1 Has the risk management policy been documented with the Medical IT-Network Risk Management File?	Document Risk Management Policy within the Medical IT-Network Risk Management file.
Technical Report:	**Section:**
IEC 80001-2-4	1.4 Prerequisites
IEC 80001-2-4	4.1 TOP MANAGEMENT responsibilities
IEC 80001-2-4	4.3 Large RESPONSIBLE ORGANIZATION – points to consider

Table A.64 — MDP.4 BP.2

MDP.4 BP3: Design the risk management policy to balance the three key properties with the mission of the responsible organisation.	
Question:	**Guidance:**
MDP.4 BP3 Q.1 Has the risk management policy been designed to balance the 3 key properties with the mission of the responsible organisation?	Design the risk management policy to balance the three key properties with the mission of the responsible organisation.
Technical Report:	**Section:**
IEC 80001-2-4	1.4 Prerequisites
IEC 80001-2-4	4.1 TOP MANAGEMENT responsibilities
IEC 80001-2-4	4.3 Large RESPONSIBLE ORGANIZATION – points to consider

Table A.65 — MDP.4 BP.4

MDP.4 BP4: Include description of or reference to processes applying to Medical IT-Networks. Include description of or reference to processes applying to Medical IT-Networks. (Including at least Event Management, Change - Release Management, Configuration Management & Monitoring).	
Question:	**Guidance:**
MDP.4 BP4 Q.1 Does the risk management policy Include description of or reference to processes applying to Medical IT-Networks?	Description of or reference to processes applying to Medical IT-Networks to include: Event Management, Change - Release Management, Configuration Management & Monitoring. Medical IT-network life cycle activities can be captured in an IT service management policy (e.g. per ISO 20000) provided there is a clear relationship to the risk management policy. The policy shall be expressed in terms that can be interpreted throughout all risk management activities.
Technical Report:	**Section:**
IEC 8001-2-4	5.3 Establish underlying RISK framework

A.1.13 MDP.5 Organisational Risk Management Process

Table A.66 — MDP.5 BP.1

MDP.5 BP1: Establish & maintain Risk Management Process. Establish and maintain a risk management process which takes into account the defined use of the medical IT-network.	
Question:	**Guidance:**
MDP.5 BP1 Q.1 Has a risk management process been established and maintained which takes into account the defined use of the medical IT-network?	Establish and maintain a risk management process for identifying hazards, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the risk controls, which takes into account the defined use of the medical IT-network. Subsequent changes to the medical IT-network could introduce new risks and require additional analyses
Technical Report:	**Section:**
IEC 80001-2-4	5.2 Determine the clinical context within which the healthcare provision is made
IEC 80001-2-4	5.4 Determining and understanding a MEDICAL IT-NETWORK

Table A.67 — MDP.5 BP.2

MDP.5 BP2: Execute Risk Management Process in line with Risk Management Policy. Medical IT-Network risk Manager executes the risk management process in line with the risk management policy.	
Question:	**Guidance:**
MDP.5 BP2 Q.1 Is the risk management process executed in line with the risk management policy?	Medical IT-Network risk Manager shall supervise the execution of the risk management process in line with the risk management policy to maintain the key properties of the medical IT-network. The medical IT-network risk manager shall be responsible for the performance of the risk management process. This includes but is not limited to responsibility for: • collection of all risk-relevant information on the medical devices; • planning the incorporation of the medical devices in accordance with the instructions provided by the various medical device manufacturers and the policies of the responsible organization; • the performance of the risk management process whenever a medical device is added to an IT-network; • the performance of the risk management process whenever an incorporated medical device or the medical IT-network is changed; • authorization to proceed with go-live following a change to the medical IT-network; • informing the responsible organization about unacceptable risk related to the medical IT-network and the associated hazards arising from any changes in configuration; and • monitoring all medical IT-network projects or changes to the medical IT-network for which the medical IT-network risk manager is responsible. These tasks may be delegated, but the medical IT-network risk manager remains responsible for ensuring their adequate performance.

Table A.68 — MDP.5 BP.3

MDP.5 BP3: Report on performance of Risk Management Process. Report (made by Medical IT-Network Risk Manager) on the performance of the risk management process to Top Management.	
Question:	**Guidance:**
MDP.5 BP3 Q.1 Is the performance of the risk management process reported to Top Management?	Report (made by Medical IT-Network Risk Manager) on the performance of the risk management process to Top Management.

Table A.69 — MDP.5 BP.4

MDP.5 BP4: Manage communications. Manage communications (made by Medical IT-Network Risk Manager) between internal and external participants in risk management.	
Question:	**Guidance:**
MDP.5 BP4 Q.1 Are communications managed?	Manage communications (made by Medical IT-Network Risk Manager) between internal and external participants in risk management. Such participants may include, as appropriate: • medical device manufacturers; • other suppliers of IT equipment, software and services; • internal IT function and other facilities management functions; • clinical users; and • technical support function responsible for medical devices (for example biomedical engineering).

A.2 Exemplar Assessment Documentation:

A.2.1 Introduction

This annex provides sample templates which can be used during the assessment process. The text in italics shows sample text or gives further details of the information that should be recorded in the relevant fields. The templates serve as an example of the format that the documentation may take and can be tailored for use as required by the specific context of the HDO. The templates in this annex can be used for either an assessment of conformance or an assessment of the capability level of the risk management processes.

A.2.2 Assessment Details

This template can be used during Stages 1 and 2 of the assessment process as described in subclause 4.3.2 and 4.3.2 of the technical report to define the assessment scope and to record the risk management stakeholders and their responsibilities during the assessment.

Table A.70 — Assessment Details Template

Document ID:	*(as per the document management policy)*		
Department:	*Name*	**Project**	(as per the assessment scope)
Top Manager:	*Name*	**Status:**	*e.g. Initial Draft*
Medical IT Network Risk Manager	*Name*	**Version:**	*e.g. v0.1*
Assessor(s)	*(defining lead assessor if required)*	**Date:**	*Date*
Assessment Scope:			
Details of the assessment scope such as the project or medical IT network which is to be in scope for the assessment, the processes which are being assessed, whether the focus of the assessment is to assess conformance or is to assess the capability levels of the processes, whether this is an assessment or reassessment.			
Risk Management Stakeholder(s):	**Role:**	**Responsibilities:**	
Name	*Description of risk management role within the HDO*	*Description of responsibilities during the assessment process*	

A.2.3 Assessment Interview Template

The template provided in this subclause can be used for group or individual interviews which are performed during stage 3 of the assessment process. The template can be used for group or individual interviews to record participant responses to the assessment questions provided in annex A.1 and should include or make reference to the information collected in relation to assessment details in Annex A.2.2.

Table A.71 — Assessment Interview Template

Participant(s):	*Name*	**Date:**	*Date*
Question:	**Response Summary:**	**Work Product Inspection:**	**Rating:**
e.g.MRM.1 BP1 Q.1	*Summary of information collected during the interview to identify strengths and weaknesses in the current risk management processes.*	*Summary of work products which have been reviewed as part of the assessment process including a summary of any strengths and weaknesses which have been identified*	*Rating of the relevant base practice by the assessor based on the information collected during interviews and through inspection of work products. The rating should use the process attribute rating scale which is defined in subclause 4.4.2*

A.2.4 Findings Report

This template can be used to draft the findings report which is prepared during stage 5 of the assessment process and presented during stage 6 of the assessment process. The findings report can be used as a basis for the development of an improvement plan if required (stage 6 of the assessment process). The findings report can be used to determine the need for and to inform the scope of a reassessment (if required as part of assessment stage 7).The findings report contains two sections. The first section provides a summary of assessment results (based on either conformance or capability level) for each of the 14 processes. Each of the processes are described both in terms of conformance capability and a summary of the assessment findings highlighting strengths and weaknesses in the current risk management processes. The overall summary is a synopsis of the weaknesses highlighted during the assessment. The second section provides details assessment findings and highlights the recommended steps to be taken to improve risk management processes based on the weaknesses identified for each of the processes assessed.

The findings report should include or make reference to the information collected in relation to assessment details in Annex A.2.2.

Table A.72 — Findings Report Template

Overall Assessment Summary:			
Process ID:	**Conformant:**	**Capability Level:**	
MRM.1	*Yes/No (Capability Level 1)* *Summary:*	*Capability Level Upper than 1(if applicable)*	
Assessment Findings:			
Process ID:	**Recommendations:**	**Owner:**	**Target Date:**
MRM.1	*Description of steps which are to be taken to improve risk management processes to achieve conformance or to achieve a higher capability level. Recommendations are based on the information collected during stage 3 of the assessment and may be presented based on individual base practices or may summarize recommendations related to a specific process based on a review of all base practices (and a review of the relevant work products).*	*Risk Management stakeholder tasked with ensuring that identified recommendations are implemented (if required as part of stage 6 of the assessment process).*	*Date by which recommendations are scheduled to be implemented (if required as part of stage 6 of the assessment process).*

Annex B
(informative)

Process Reference Model

B.1 Introduction

The purpose of this annex is to describe a PRM that facilitates the development of a PAM to assess against IEC 80001-1. The PAM is described in Annex C.

ISO/IEC 15504-2 describes the requirements for the conduct of an assessment and a measurement scale for assessing process capability. ISO/IEC 15504-1 describes the concepts and terminology used for process assessment. ISO/IEC TR 24774 provides guidelines for process description. These standards have been used to inform the development of both the PRM and PAM.

This PRM is a logical representation of the elements of the processes within the risk management process for the incorporation of medical devices into IT-Networks. Using the PRM in a practical application might require additional elements suited to the environment and circumstances. The PRM specified in this technical report describes at an abstract level the processes including the general risk management (RM) processes implied by IEC 80001-1. Each process of this PRM is described in terms of a purpose and outcomes. The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability required to fulfil the IEC 80001-1 requirements. The PRM is not intended to be used for a conformity assessment audit or process implementation reference guide.

Any organization can define processes for its specific environment and circumstances for a PRM. The purposes and outcomes of each process described in this technical report are, however, considered to be the minimum necessary to meet IEC 80001-1 requirements in relation to each process. The 14 processes in the PRM have been identified in order to give coverage to all the requirements of IEC 80001-1.

The PRM does not provide the evidence required by ISO/IEC 80001-1. The PRM does not specify the interfaces between the processes.

Clause B.2 of this Annex provides an overview of the PRM. Clause B.3 provides a description of the risk management processes for IT networks incorporating medical devices. Clause B.4 provides a statement of conformity for this PRM in accordance with ISO/IEC 15504-2.

B.2 Overview of the Process Reference Model

B.2.1 General

This clause describes the structure of the PRM in the context of risk management of IT-Networks incorporating Medical Devices to address Safety, Effectiveness and Data & System Security.

Figure B.1 identifies the processes derived from IEC 80001-1 requirements, which are included in this PRM for Application of Risk Management for IT-Networks Incorporating Medical Devices.

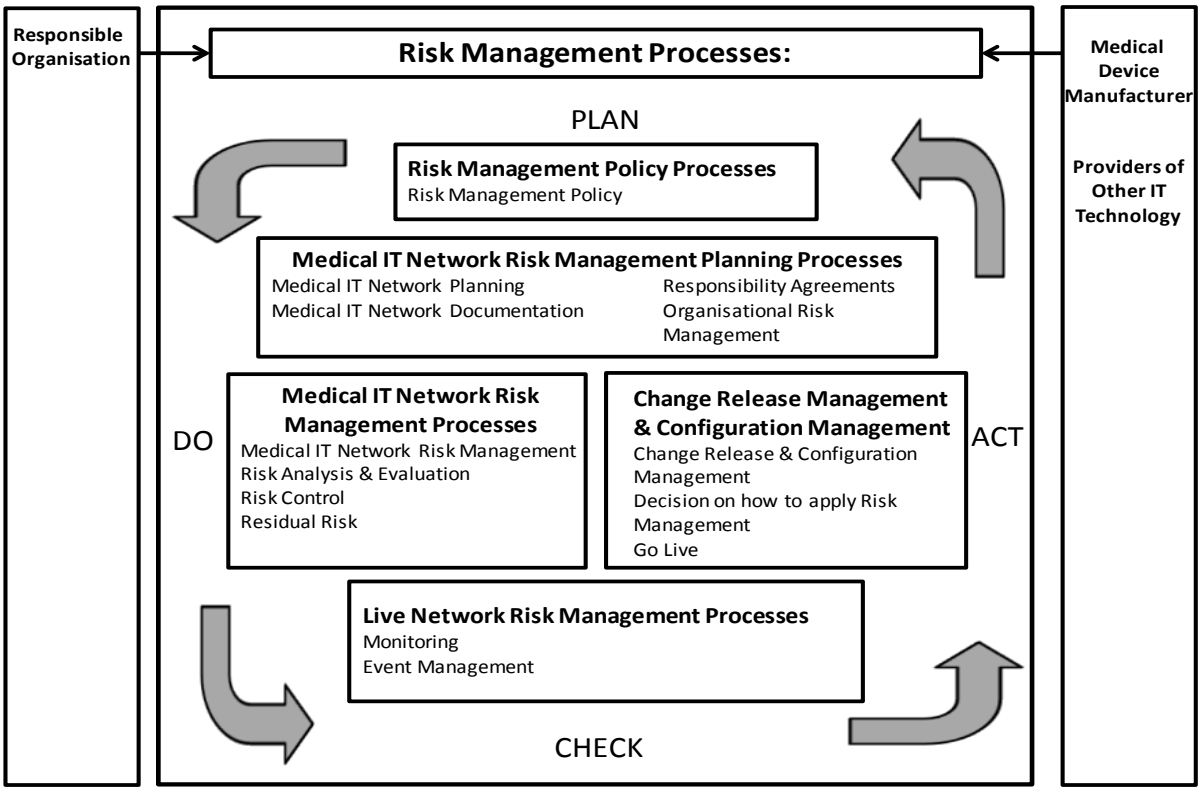

Figure B.1 — Processes in the Process Reference Model

B.2.2 Process Descriptions

Each process in the PRM has the following descriptive elements:

Name: the name of a process is a short noun phrase that summarizes the scope of the process, identifying the principal concern of the process, and distinguishes it from other processes within the scope of the PRM.

Context: for each process a brief overview describes the intended context of the application of the process.

Purpose: the purpose of the process is a high level, overall goal for performing the process.

Outcomes: an outcome is an observable result of the successful achievement of the process purpose. Outcomes are measurable, tangible, technical or business results that are achieved by a process. Outcomes are observable and assessable.

Requirements traceability: the outcomes are based on the requirements of IEC 80001-1. The references identify the applicable subclauses of IEC 80001-1, the subclause heading, and the outcomes that are supported.

In clause B.3 (subclauses B.3.1 to B.3.14) all entries in the requirements traceability row end with a reference to a numbered outcome in square brackets, (i.e. [Outcome: n]) which are directly linked to the requirements of IEC 80001-1. The referencing is illustrated by example 1, given below.

EXAMPLE 1 The first requirements traceability entry in subclause B.3.1 – MRM.1 Medical-IT Network Risk Management:

IEC 80001-1, 3.1 - Roles & Responsibilities - General [1]

The [1] is a reference to outcome 1 in the previous row of subclause B.3.1 – MRM.1 Medical-IT Network Risk Management.

Outcome 1 is: A Medical IT-Network Risk Management file is established and maintained containing all required documentation.

B.3 Process Descriptions

B.3.1 MRM.1 Medical IT-Network Risk Management Process

Name:	**Medical IT-Network Risk Management Process**
Process ID:	**MRM.1**
Context:	The responsible organization is the owner of the risk management process for the medical IT-network and ensures the provision of adequate resources and ensuring the assignment of qualified personnel for management, performance of work and assessment activities; reviewing the results of risk management activities, including event management, at defined intervals to ensure the continuing suitability and the effectiveness of the risk management process. Top management appoint a medical IT-network risk manager, who has the necessary qualifications, knowledge and competence for risk management applied to medical IT-networks. Top management identify the people responsible for the risk management tasks and ensure that they co-operate with the medical IT-network risk manager:
Purpose:	The purpose of the Medical IT-Network process is to gather, analyze, assess and store information spanning planning, design, installation, device connection, configuration, use/operation, maintenance, and device decommissioning for lifecycle management of Medical Devices incorporated in IT-Networks.
Outcomes:	As a result of the successful implementation of the Medical IT-Network Risk Management Process : 1. A Medical IT-Network Risk Management file is established and maintained containing all required documentation. 2. Adequate appropriately qualified resources for management, performance of work and assessment activities are assigned. 3. The results of risk management activities, including event management, are reviewed at defined intervals. 4. A qualified medical IT-network risk manager is appointed. 5. People responsible for Risk Management activities and lifecycle management (including procurement and maintenance) of medical devices incorporated into IT networks, co-operate with the medical IT-network risk manager. 6. Risk management process for medical IT-networks includes the participation of management responsible for life cycle management of Medical IT-Networks, general IT activities and the use of Medical Devices. 7. All supervision, operation, installation and maintenance of Medical IT-Network(s) throughout the life cycle are made according to the Risk Management plan and follow the results of the IT-Network Risk Management Process. 8. All parties performing supervision, operation, installation, service, troubleshooting and maintenance of Medical IT-Network(s) are adequately informed about their responsibility according to this standard, including their responsibility for maintaining the effectiveness of Risk Controls. 9. The key properties of the medical IT-network are maintained throughout the life cycle. 10. The risk management activities of risk analysis, risk evaluation, risk control, residual risk evaluation and reporting and approval are documented.
Requirements traceability:	IEC 80001-1, 3.1. Roles & Responsibilities - General [1] IEC 80001-1, 3.3, (c) Top Management Responsibilities [2] IEC 80001-1, 3.3, (d) Top Management Responsibilities [2] IEC 80001-1, 3.3, (e. Top Management Responsibilities [3] IEC 80001-1, 3.3. Top Management Responsibilities [4] IEC 80001-1, 3.3, (f, g, i, j. Top Management Responsibilities [5] IEC 80001-1, 3.3, (k, m, n, o) Top Management Responsibilities [6] IEC 80001-1, 3.3, (p) Top Management Responsibilities [7] IEC 80001-1, 3.3, (q) Top Management Responsibilities [8] IEC 80001-1, 4 Life Cycle Risk Management in Medical IT-Networks Overview [9] IEC 80001-1, 4.4.1 Medical IT-Network Risk Management - Overview [10]

B.3.2 MRM.1.1 Risk Analysis & Evaluation Process

Name:	**Risk Analysis & Evaluation**
Process ID:	**MRM.1.1**
Context:	This process allows the Responsible Organisation to identify risks related to the incorporation of medical devices into an IT network. Once these risks have been identified, the process allows the Responsible Organisation to analyze & evaluate the risks throughout the life cycle. The risk evaluation process is based on the risks identified during the risk analysis phase.
Purpose:	The purpose of the Risk Analysis process is to identify, analyze & evaluate risk related to the incorporation of Medical Device into IT Networks.
Outcomes:	As a result of the successful implementation of the Risk Analysis process : 1. Hazards that are likely to arise from the medical IT–network are identified. 2. For each identified hazard, the associated risks are estimated, analyzed and evaluated using available information or data throughout the lifecycle. 3. Possible consequences of harm (where probability of occurrence cannot be estimated) are listed for use in risk control. 4. The results of these activities are recorded in the medical IT-network risk management file. 5. Where the estimated risk(s) is so low that risk reduction need not to be pursued, the rationale for this decision is documented in the medical IT-network risk management file.
Requirements traceability:	IEC 80001-1, 4.4.2. Risk Analysis [1, 2 ,3, 4] IEC 80001-1, 4.4.3, (a). Risk Evaluation [2, 5] IEC 80001-1, 4.4.3, (b). Risk Evaluation [2]

B.3.3 MRM.1.2 Risk Control Process

Name:	**Risk Control Process**
Process ID:	**MRM.1.2**
Context:	Having completed the risk analysis and risk evaluation, the risk control process implements risk control measures until the residual risk is judged to be of an acceptable level.
Purpose:	The purpose of the Risk Control Process is to implement risk control measures until the residual risk is judged to be of an acceptable level.
Outcomes:	1. As a result of the successful implementation of the Risk Control process: Proposed risk control measures are identified and documented for each unacceptable risk. 2. Risk control options are used in the following order: inherent control by design; protective measures; information for assurance. 3. Key properties are considered in the following order of priority - safety, effectiveness, and data & systems security, when considering risk control options. 4. A risk/benefit analysis of the residual risk is conducted and documented when the required risk reduction has been determined not to be practical. 5. Risk control measures that require a change to the medical IT-network are managed under the change-release management process. 6. Selected Risk control measures are recorded in the medical IT-network risk management file. 7. Where the estimated risk(s) are not acceptable, selected risk control measures are implemented according to risk control option analysis. 8. If a change is undertaken without documented consent of the medical device manufacturer, the manufacturer is notified and all necessary regulatory steps for putting such a modified medical device into service are followed. (Changes to a medical device without documented consent of the medical device manufacturer are NOT recommended). 9. Any residual risk is documented in the medical IT-network risk management file. 10. Implementation & effectiveness of all risk control measures in the operational system are verified and documented in the medical IT-network risk management file. 11. The implemented risk control measures and the installed operational system are reviewed for new, unacceptable RISKS and the evaluation is documented in the Medical IT-Network risk management file.
Requirements traceability:	IEC 80001-1, 4.4.4.1, (a, b, c). Risk Control Option Analysis [1, 2] IEC 80001-1, 4.4.4.1. Risk Control Option Analysis [3, 4] IEC 80001-1, 4.4.4.2. Risk Control Measures [5, 6] IEC 80001-1, 4.4.4.3. Implementation of Risk Control Measures [7, 8, 9] IEC 80001-1, 4.4.4.4. Verification of Risk Control Measures [10] IEC 80001-1, 4.4.4.5. New Risks arising from Risk Control [11]

B.3.4 MRM.1.3 Residual Risk Process

Name:	**Residual Risk Process**
Process ID:	**MRM.1.3**
Context:	Once risk control measures have been implemented, residual risk is reviewed and additional risk control measures applied if necessary. Residual risks are documented and where additional risk control measures are not practical, a risk benefit analysis is carried out and documented.
Purpose:	The purpose of the Residual Risk Process is to ensure that residual risk is documented and a risk benefit analysis is conducted to decide whether to accept the residual risk.
Outcomes:	As a result of the successful implementation of the Residual Risk Process: 1. Persons responsible for reviewing and accepting residual risk have co-operated with Medical IT-Network Risk Manager. 2. Residual risk is evaluated based on a pre-release assessment of the effectiveness of the implemented risk control measures. 3. Individual residual risks and the overall residual risk are assessed for acceptability. 4. Additional risk control measures are applied where an individual residual risk or the overall residual risk is not determined to be acceptable. 5. A residual risk summary is defined and documented. 6. The decision to approve the residual risk is made on the basis of a documented risk/benefit analysis of the individual or overall residual risk against the health benefit accrued (where the reduction of residual risk to an acceptable level is not practicable).
Requirements traceability:	IEC 80001-1, 3.3. Top Management Responsibilities [1] IEC 80001-1, 4.4.5. Residual Risk Evaluating & Reporting [2, 3, 4, 5, 6]

B.3.5 CRCM.1 Change Release & Configuration Management Process

Name:	Change Release & Configuration Management Process
Process ID:	CRCM.1
Context:	The Change Release process ensures that a documented change release process is in place and that the process includes risk management activities. In addition to this a configuration management process shall also be in place.
Purpose:	The purpose of the Change Release process is to ensure that a documented Change Release Process is in place and that risk management activities take place during the Change Release. Acceptability of the change is based on the results of the Risk Management activities as part of the Change Release process. All changes to the system shall be reflected in the Configuration Management process.
Outcomes:	As a result of the successful implementation of the Change Release Process : 1. Current Configuration Management information for the medical IT-Network is contained in the Risk Management file. 2. Action plans arising from risk assessment follow the change-release management process. 3. A Change Release policy (including Risk Management) is documented and applied. 4. The results of the risk management process are used to determine approval and acceptability of changes during the change-release management process. 5. A configuration management policy is documented and applied during risk management of the change release management.
Requirements traceability:	IEC 80001-1, 3.1. Roles & Responsibilities - General [1] IEC 80001-1, 4.4.1. Medical IT-Network Risk Management - Overview [2] IEC 80001-1, 4.5.1. Change Release Management Process [3, 4, 5]

B.3.6 CRCM.2 Decision on how to apply Risk Management Process

Name:	Decision on how to apply Risk Management
Process ID:	CRCM.2
Context:	This process allows the responsible organisation to consider the nature of the change and decide whether the change should be implemented as a change permit or whether the change should be implemented through the initiation of a Medical IT-Network project.
Purpose:	The purpose of the Decision on how to apply Risk Management process is to ensure that a policy is in place to allow organisations to consider the nature of the change that is required to the Medical IT-Network and assess if the change should be carried out under a change permit or by initiating a Medical IT-Network project.
Outcomes:	As a result of the successful implementation of the Decision on the Application of Risk Management Process : 1. The change-release management process is initiated for any new medical IT-network or a change to an existing medical IT-Network. 2. The nature of the change is considered to decide whether the requirements are met by an applicable change permit and if not, a medical IT-network project is initiated. 3. A routine change is performed once a change permit is defined and constraints are specified. 4. Change permits specify what records are to be kept for each permitted change. 5. Change permits are maintained in the medical IT-network risk management file. 6. A project plan is established and maintained for specific circumstances that have the potential to introduce new risk. 7. The project plan is revised whenever necessary to reflect changes to the project. 8. The project plan is kept in the medical IT-network Risk Management File.
Requirements traceability:	IEC 80001-1, 4.5.2.1. Decision on how to apply Risk Management - Overview [1, 2] IEC 80001-1, 4.5.2.2. Decision on how to apply Risk Management - Change Permits [3, 4, 5] IEC 80001-1, 4.5.2.3. Decision on how to apply Risk Management - Medical IT-Network Projects [6, 7, 8]

B.3.7 CRCM.3 Go Live Process

Name:	**Go-Live**
Process ID:	**CRCM.3**
Context:	This process allows the responsible organisation to manage the Go-Live Phase of the project and to consider the decision to go live in terms of the residual risk.
Purpose:	The purpose of the Go-Live Process is to allow the responsible organisation to manage the transition of the IT network to the live environment and to allow the responsible organisation to manage the risk management activities associated with the Go-Live phase of the project.
Outcomes:	As a result of the successful implementation of Go-Live Process : 1. Medical IT-network residual risk is reviewed prior to going live. 2. Residual risk summaries are reviewed for acceptability of risks associated with interactions of recent or pending projects or changes. 3. The specified change to the medical IT-network is approved prior to go-live by the medical IT-network risk manager. 4. The approval of the medical-IT network residual risk is documented in the medical IT-network risk management file.
Requirements traceability:	IEC 80001-1, 4.5.3. Go Live [1, 2, 3, 4]

B.3.8 LNRM.1 Monitoring Process

Name:	**Monitoring Process**
Process ID:	**LNRM.1**
Context:	Once the medical IT-network has been deployed to the live environment, this process allows for the network to be monitored during the operational phase.
Purpose:	The purpose of the process is to allow the successful monitoring of the medical IT-network during the operational phase and to establish requirements for monitoring to be established as part of the risk management plan of the medical IT-network. This allows the network to be monitored for emerging risks, effectiveness of risk control measures, and accuracy of original estimations of risk.
Outcomes:	As a result of the successful implementation of Monitoring Process : 1. A process outlining monitoring requirements is established as part of the risk management plan to monitor each installed medical IT-network. 2. Requirements for monitoring are established as part of the risk management plan of the medical IT-network. 3. Event Management process is initiated where monitoring indicates actual or potential increase in risk.
Requirements traceability:	IEC 80001-1, 4.6.1. Monitoring [1, 2, 3]

B.3.9 LNRM.2 Event Management Process

Name:	**Event Management Process**
Process ID:	**LNRM.2**
Context:	During the operational phase of the Medical IT-Network, if a negative event occurs, this is dealt with under the event management process.
Purpose:	The purpose of the Event Management process is to allow the responsible organisation to manage events which have a negative impact on the medical IT-network. Required changes are managed through the Change Release Process and events are tracked to closure.
Outcomes:	As a result of the successful implementation of the Event Management Process: 1. Event management policy is established to ensure negative events are captured and documented. 2. Events are evaluated and proposed changes as appropriate are managed through change-release management process. 3. All corrective and preventive actions leading to closure are tracked. 4. Significant finds are reported to the medical IT-network risk manager and/or others in the responsible organization.
Requirements traceability:	IEC 80001-1, 4.6.2, (a). Event Management [1] IEC 80001-1, 4.6.2, (b). Event Management [2] IEC 80001-1, 4.6.2, (c). Event Management [3] IEC 80001-1, 4.6.2, (d). Event Management [4]

B.3.10 MDP.1 Medical IT-Network Planning Process

Name:	**Medical IT-Network Planning Process**
Process ID:	**MDP.1**
Context:	During the Planning phase of the Medical IT-Network, risk management shall be considered. This process deals with the approach to the planning of risk management activities.
Purpose:	The purpose of the Medical IT-Network Planning Process is to ensure that Risk Management activities are planned in accordance with the Risk Management Policy.
Outcomes:	As a result of the successful implementation of the Medical IT-Network planning process: 1. The current state of the IT network and planned changes have been considered in the planning of risk management. 2. Initial development of new medical IT-networks and changes to existing networks not covered by documented change permits are managed by projects. 3. A risk management plan for each medical IT-network is established and maintained. 4. Risk Management Plan is updated when a project introduces changes to an existing medical IT-network.
Requirements traceability:	IEC 80001-1, 4.3.1, (c). Overview [1] IEC 80001-1, 4.3.1. Overview [2, 3] IEC 80001-1, 4.3.5, (a, b, c, d). Risk Management plan for the Medical IT-Network [4] IEC 80001-1, 4.3.5. Risk Management plan for the Medical IT-Network [5]

B.3.11 MDP.2 Medical IT-Network Documentation Process

Name:	**Medical IT-Network Documentation Process**
Process ID:	**MDP.2**
Context:	In order to successfully perform risk management activities, medical device manufacturers shall provide certain documents to allow for the successful connection of the device to the IT network. This process details what documents are required.
Purpose:	The purpose of the Medical IT-Network Documentation Process is to ensure additional documents are made available by the medical device manufacturer to the Responsible organisation that describe the intended use of the device and give instructions necessary for the safe and effective use of the medical device. This should be a fluent process throughout the lifecycle and allow the Responsible Organisation to protect the 3 key properties of the network.
Outcomes:	As a result of the successful implementation of the Medical IT-Network Documentation process: 1. For a medical device that can be connected to an IT-network, the medical device manufacturer makes available, instructions for implementing such connection. 2. Accompanying documents obtained for a medical device incorporated in a medical IT-network are maintained in the medical IT-network risk management file. 3. Additional documentary information provided as necessary to perform risk management for the medical IT-network and is maintained in the medical IT-network risk management file. 4. Network documentation necessary to support the risk management of the Medical IT-Network for the interfaces between the medical devices and all network components is maintained. 5. As part of risk management planning of the medical IT-network a risk-relevant asset description is maintained. 6. A list of assets of IT-networks interfacing with medical devices is maintained. 7. All relevant documents in the medical IT-network life cycle are revised, amended, reviewed, and approved in accordance with a document control procedure. 8. The risk management file provides full traceability for each identified hazard.
Requirements traceability:	IEC 80001-1, 3.5. Medical Device Manufacturers [2] IEC 80001-1, 3.5, (a) to (f) Medical Device Manufacturers [1, 3] IEC 80001-1, 3.6, (g) to (m). Providers of other Information Technology [3] IEC 80001-1, 4.3.1 (a). Overview [5] IEC 80001-1, 4.3.1, (a) to (h). Overview [3, 6] IEC 80001-1, 4.3.3, (a) to (f). Medical IT-Network Documentation [4] IEC 80001-1, 5.1. Document Control Procedure [7] IEC 80001-1, 5.2, (a, b, c, d). Medical IT-Network Risk Management File [8]

B.3.12 MDP.3 Responsibility Agreements Process

Name:	**Responsibility Agreements Process**
Process ID:	**MDP.3**
Context:	In order to establish the responsibilities of Medical Device Manufacturers and Other IT providers, Responsibility Agreements are drafted.
Purpose:	The purpose of the process is to establish the responsibilities of Medical Device Manufacturers and Other IT providers in regard to risk management responsibilities.
Outcomes:	As a result of the successful implementation of the Responsibility Agreements Process: 1. The need for one or more documented responsibility agreements is determined whenever a medical device is incorporated into an IT network or the configuration of such a connection is changed. 2. Where necessary, a responsibility agreement is established. 3. A responsibility agreement defines the responsibilities of all relevant stakeholders throughout the lifecycle. 4. A responsibility agreement covers one or more projects or the maintenance of one or more medical IT-networks.
Requirements traceability:	IEC 80001-1, 4.3.4. Responsibility Agreements [1, 2, 4] IEC 80001-1, 4.3.4 (a) to (h). Responsibility Agreements [3]

B.3.13 MDP.4 Risk Management Policy Process

Name:	**Risk Management Policy Process**
Process ID:	**MDP.4**
Context:	The process ensures that a Risk Management policy is put in place which determines acceptable risks and will ensure that the policy balances the 3 key properties of the network with the mission of the responsible organisation. The policy is defined in terms that can be interpreted throughout all risk management activities. Risk management activities are to be carried out in line with the risk management policy.
Purpose:	The purpose of the Risk Management Policy Process is to define and document a risk management policy for incorporating medical devices into an IT-network.
Outcomes:	As a result of successful implementation of the Risk Management Policy: 1. A policy for risk management for incorporating medical devices is established, designed and documented. 2. Criteria for determining acceptable risk are outlined in the Risk Management Policy, taking into account relevant international standards and national or regional regulations. 3. The three key properties are balanced with the mission of the responsible organisation in the Risk Management Policy. 4. The Risk Management policy includes description of or reference to processes applying to Medical IT-Networks (including at least Event Management, Change - Release Management, Configuration Management & Monitoring.
Requirements traceability:	IEC 80001-1, 3.3, (a). Top Management Responsibilities [1] IEC 80001-1, 3.3, (b). Top Management Responsibilities [2] IEC 80001-1, 4.2.1, (a). Policy for Risk Management for Incorporating Medical Devices [3] IEC 80001-1, 4.2.1, (b). Policy for Risk Management for Incorporating Medical Devices [2] IEC 80001-1, 4.2.1, (c). Policy for Risk Management for Incorporating Medical Devices[4]

B.3.14 MDP.5 Organisational Risk Management Process

Name:	**Organisational Risk Management Process**
Process ID:	**MDP.5**
Context:	This is an umbrella process to outline the responsibilities of the Medical IT-Network Risk Manager is relation to the establishment of the Risk Management process.
Purpose:	The purpose of the Organisational Risk Management Process is to outline the responsibilities of the Medical IT-Network Risk Manager in relation to the performance of Risk Management activities for an IT Network incorporating Medical Devices.
Outcomes:	As a result of the successful implementation of the Organisational Risk Management process: 1. Execution of the risk management process in line with the established Risk Management policy is supervised by the Medical IT-Network risk manager. 2. Performance of Risk Management Process is reported to Top Management by medical IT-network Risk Manager. 3. Communication between internal and external participants in Risk Management is managed by the medical IT-network Risk Manager. 4. A Risk Management Process which takes into account the defined use of the medical IT-network into account is established and maintained by the medical IT-network Risk Manager.
Requirements traceability:	IEC 80001-1, 3.4. Medical IT-Network Risk Manager [1] IEC 80001-1, 3.4, (a). Medical IT-Network Risk Manager [1] IEC 80001-1, 3.4, (b). Medical IT-Network Risk Manager [2, 3] IEC 80001-1, 4.2.2. Risk Management Process [4]

B.4 PRM Conformity to ISO/IEC 15504-2

B.4.1 General

The PRM in this technical report is suitable for use in process assessment performed in accordance with ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing an assessment*.
ISO/IEC 15504-2:2003, clause 6.2 places requirements on PRMs suitable for assessment against ISO/IEC 15504-2. The following subclauses quote the requirements for a PRM and describe how the PRM contained in this technical report meets these. In each of the following clauses the text in a box quotes the requirements from the text of ISO/IEC 15504-2 and the text below each box describes the manner in which the requirements are satisfied in this PRM.

B.4.2 Requirements for Process Reference Models

ISO/IEC 15504-2:2003, Information technology – Process assessment – Performing an assessment

6.2.3.1 A PRM shall contain:

a) A declaration of the domain of the PRM.

b) A description, meeting the requirements of Clause 6.2.4 of this International Standard, of the processes within the scope of the PRM.

c) A description of the relationship between the PRM and its intended context of use.

d) A description of the relationship between the processes defined within the PRM.

— The declaration of the domain is risk management process for the incorporation of medical devices into IT-Networks.

— The description of the processes is provided in clause B.2 of this Annex.

— This PRM is intended to be used as described in the introduction.

— A description of the relationship between the processes defined within this PRM is supported by Figure B.1

— The relevant communities of interest and their mode of use are described in the Introduction of this technical report.

ISO/IEC 15504-2: 2003, Information technology – Process assessment – Performing an assessment

6.2.3.3 The processes defined within a Process Reference Model shall have unique process descriptions and identification.

— The process descriptions are unique. The identification is provided by unique names and by the identifier of each process of this technical report.

B.4.3 Process descriptions

ISO/IEC 15504-2: 2003, Information technology – Process assessment – Performing an assessment

6.2.4 The fundamental elements of a Process Reference Model are the descriptions of the processes within the scope of the model. The process descriptions in the Process Reference Model incorporate a statement of the purpose of the process which describes at a high level the overall objectives of performing the process, together with the set of outcomes which demonstrate successful achievement of the process purpose. These process descriptions shall meet the following requirements:

a) a process shall be described in terms of its purpose and outcomes;

b) in any process description the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process;

c) process descriptions shall be such that no aspects of the Measurement Framework as described in Clause 5 of this International Standard beyond level 1 are contained or implied.

An outcome statement describes one of the following:

– Production of an artefact;

– A significant change of state;

– Meeting of specified constraints, e.g. requirements, goals etc.

— These requirements are met by the process descriptions in clause B.2 of this Annex

Annex C
(informative)

Process Assessment Model

C.1 Introduction

This Annex provides an exemplar PAM to assess risk management processes for the incorporation of medical devices into IT-Networks for use in performing a conformant assessment in accordance with the requirements of ISO/IEC 15504-2. It enables implemented processes of IEC 80001-1 to be assessed according to the requirements of ISO/IEC 15504-2.

The PRM defined in Annex B of this technical report, associated with the process attributes defined in ISO/IEC 15504-2, establish a PAM used as a common basis for performing assessments of process capability, allowing for the reporting of results using a common rating scale.

An integral part of conducting an assessment is to use a PAM that is constructed for that purpose, is related to a PRM and is conformant with ISO/IEC 15504-2. ISO/IEC 15504-2 sets out the minimum requirements for performing an assessment in order to ensure consistency and repeatability of the ratings. ISO/IEC 15504-2 addresses the assessment of process and the application of process assessment for improvement and capability determination. Results of conformant process assessments may be compared when the scope of the assessments are considered to be similar.

The IEC 80001-1 PRM in Annex B of this technical report has been used as the basis for the PAM. The relationship between IEC 80001-1, IEC 80001-1 (PRM), IEC 80001-1 (PAM) and ISO/IEC 15504-2 is shown in Figure C.1.

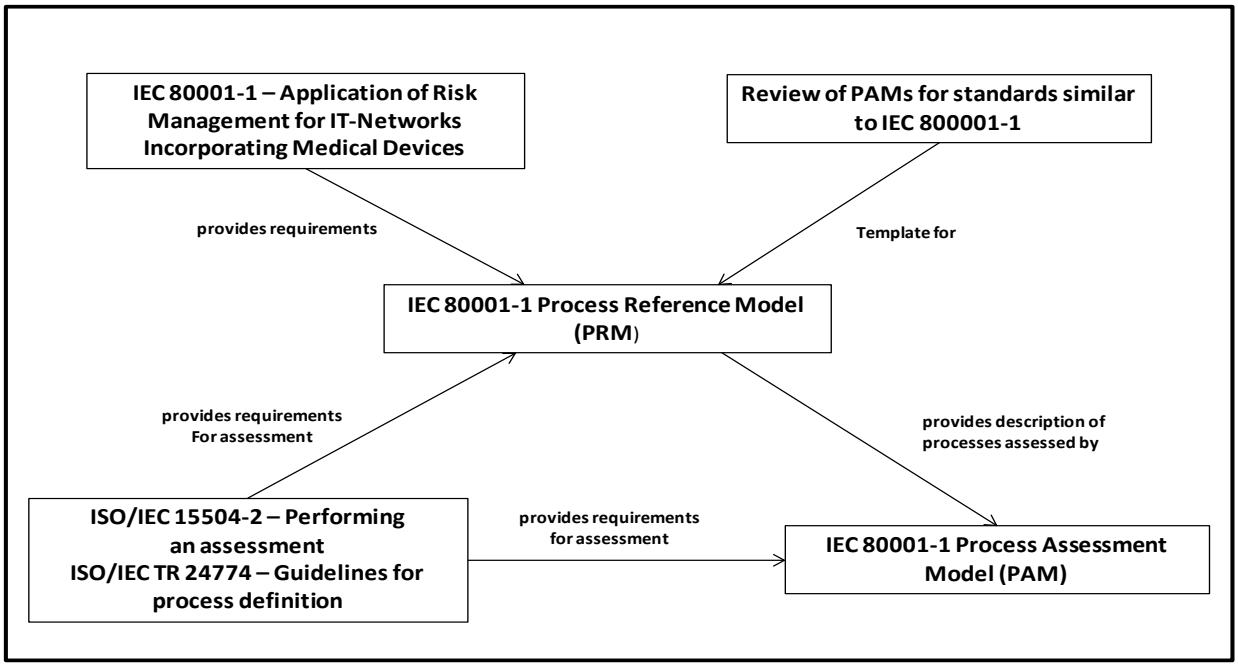

Figure C.1 — Relationship to IEC 80001-1, IEC 80001-1(PRM) and ISO/IEC 15504-2

This example PAM contains a set of indicators to be considered when interpreting the intent of the PRM. It provides greater detail to indicate process performance and capability. The indicators may also be used when implementing a process improvement program or to help evaluate and select an assessment model, method, methodology or tools. This PAM embodies the core characteristics that could be expected of any PAM consistent with ISO/IEC 15504-2. Nevertheless any other PAMs meeting the requirements of ISO/IEC 15504-2 may be used in a conformant assessment.

C.2 Overview of the exemplar Process Assessment Model

C.2.1 Introduction to Overview

This annex provides an exemplar PAM that includes examples of assessment indicators.

The PRM defined in Annex B, associated with the process attributes defined in ISO/IEC 15504-2, establish a PAM used as a common basis for performing assessments of risk management for networks incorporating medical devices process capability, allowing for the reporting of results using a common rating scale.

The PAM is a two-dimensional model of process capability. In one dimension, the process dimension, the processes are defined. In the other dimension, the capability dimension, a set of process attributes grouped into capability levels is defined. The process attributes provide the measurable characteristics of process capability. Figure C.2 shows the relationship between the general structure of the PAM, ISO/IEC 15504-2 and IEC 80001-1.

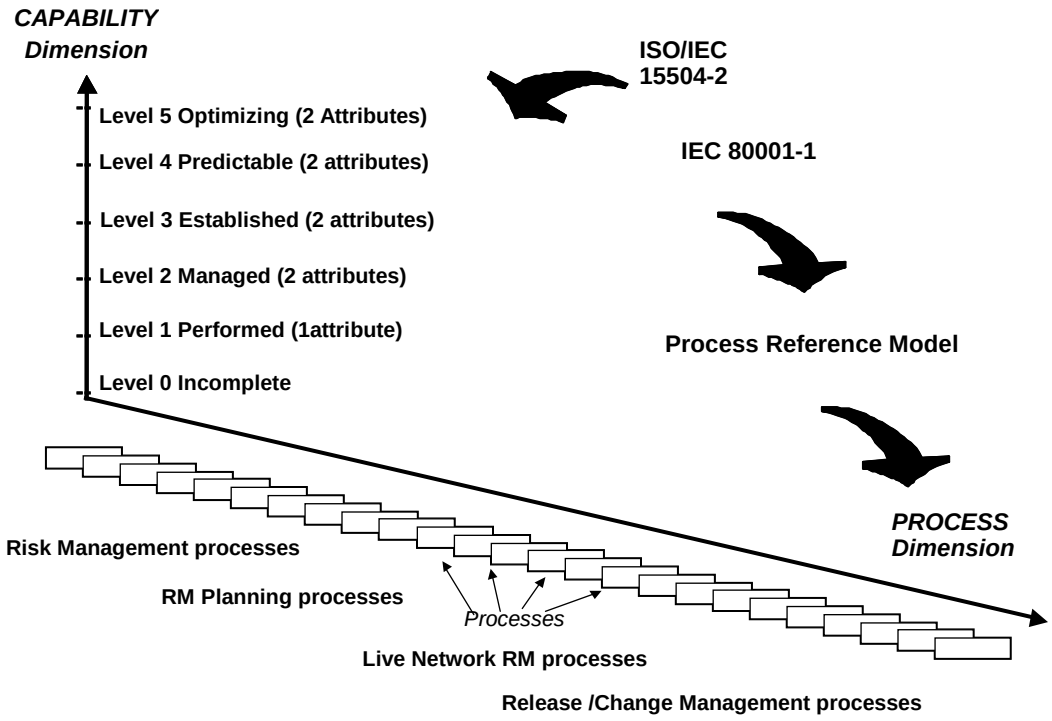

Figure C.2 — Relationship between the Process Assessment Model and its inputs

A PRM and a capability dimension defined in ISO/IEC 15504-2 cannot be used alone as the basis for conducting reliable and consistent assessments of process capability since the level of detail provided is not sufficient. The descriptions of process purpose and outcomes in a PRM, and the process attribute definitions in ISO/IEC 15504-2, need to be supported with a comprehensive set of indicators of process performance and process capability that are used for assessment performance. The assessment indicators are described in subclause C.3.

The exemplar PAM defined in this annex is conformant with the ISO/IEC 15504-2 requirements for a PAM, and can be used as the basis for conducting an assessment of risk management (of IT networks incorporating medical devices) process capability.

C.2.2 Structure of the exemplar Process Assessment Model

NOTE This subclause describes the detailed structure of the PAM and its key components.

C.2.2.1 Processes

Figure C.3 shows the processes from IEC 80001-1, which are included in the process dimension of the exemplar PAM for risk management of Medical IT-Networks.

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 C.3 — Processes in the Process Reference Model

C.2.2.2 Process dimension

The process dimension of the PAM includes all processes from the PRM contained in IEC 80001-1 (PRM) and shown in Figure C.3. Each process in the PAM is described in terms of a purpose statement. These statements contain the unique functional objectives of the process when performed in a particular environment. A list of specific outcomes is associated with each of the process purpose statements, as a list of expected positive results of the performance of the processes. Satisfying the purpose statements of a process represents the first step in building a level 1 process capability where the expected outcomes are observable. The processes are described in subclauses C.5.2 to C.5.15.

C.2.2.3 Capability dimension

For the capability dimension, the process capability levels and process attributes are identical to those defined in ISO/IEC 15504-2.

Evolving process capability is expressed in the PAM in terms of process attributes grouped into capability levels. Process attributes are features of a process that can be evaluated on a scale of achievement, providing a measure of the capability of the process. They are applicable to all processes. Each process attribute describes a facet of the overall capability of managing and improving the effectiveness of a process in achieving its purpose and contributing to the business goals of the organization.

A capability level is a set of process attribute(s) that work together to provide a major enhancement in the capability to perform a process. The levels constitute a rational way of progressing through improvement of the capability of any process and are defined in ISO/IEC 15504-2.

There are six capability levels, incorporating nine process attributes.

Level 0: Incomplete process

The process is not implemented, or fails to achieve its process purpose.

At this level, there is little or no evidence of any systematic achievement of the process purpose.

Level 1: Performed process

The implemented process achieves its process purpose.

Level 2: Managed process

The previously described Performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

Level 3: Established process

The previously described Managed process is now implemented using a defined process that is capable of achieving its process outcomes.

Level 4: Predictable process

The previously described Established process now operates within defined limits to achieve its process outcomes.

Level 5: Optimizing process

The previously described Predictable process is continuously improved to meet relevant current and projected business goals.

Within the PAM, the measure of capability is based upon the nine process attributes (PA) defined in ISO/IEC 15504-2. Process attributes are used to determine whether a process has reached a given capability. Each attribute measures a particular aspect of the process capability.

At each level there is no ordering between the process attributes; each attribute addresses a specific aspect of the capability level with each being of equal importance for the achievement of the relevant capability level. The list of process attributes is shown in Table C.1.

Table C.1 — Capability levels and process attributes

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work Products management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Continuous optimization

The process attributes are evaluated on a four point ordinal scale of achievement, as defined in ISO/IEC 15504-2 and used in the exemplar assessment method. They provide insight into the specific aspects of process capability required to support process improvement and capability determination.

C.3 Assessment Indicators

C.3.1 Overview

The PAM is based on the principle that the capability of a process can be assessed by demonstrating the achievement of process attributes on the basis of evidence related to assessment indicators.

There are two types of assessment indicators: process capability indicators, which apply to capability levels 1 to 5 and process performance indicators, which apply exclusively to capability level 1. These indicators are defined in subclauses C.3.2 and C.3.3.
The process attributes in the capability dimension have a set of process capability indicators that provide an indication of the extent of achievement of the attribute in the instantiated process. These indicators concern significant activities, resources or results associated with the achievement of the attribute purpose by a process.
The process capability indicators are:

— Generic Practice (GP);

— Generic Resource (GR);

— Generic Work Product (GWP).

As additional indicators for supporting the assessment of a process at Level 1, each process in the process dimension has a set of process performance indicators which is used to measure the degree of achievement of the process performance attribute for the process assessed.
The process performance indicators are:

— Base Practice (BP);

— Work Product (WP).

The performance of Base Practices (BPs) provides an indication of the extent of achievement of the process purpose and process outcomes. Work Products (WPs) are either used or produced (or both), when performing the process.

The process performance and process capability indicators defined in the PAM represent types of objective evidence that might be found in an instantiation of a process and therefore could be used to judge achievement of capability.
Figure C.4 shows how the assessment indicators are related to process performance and process capability.

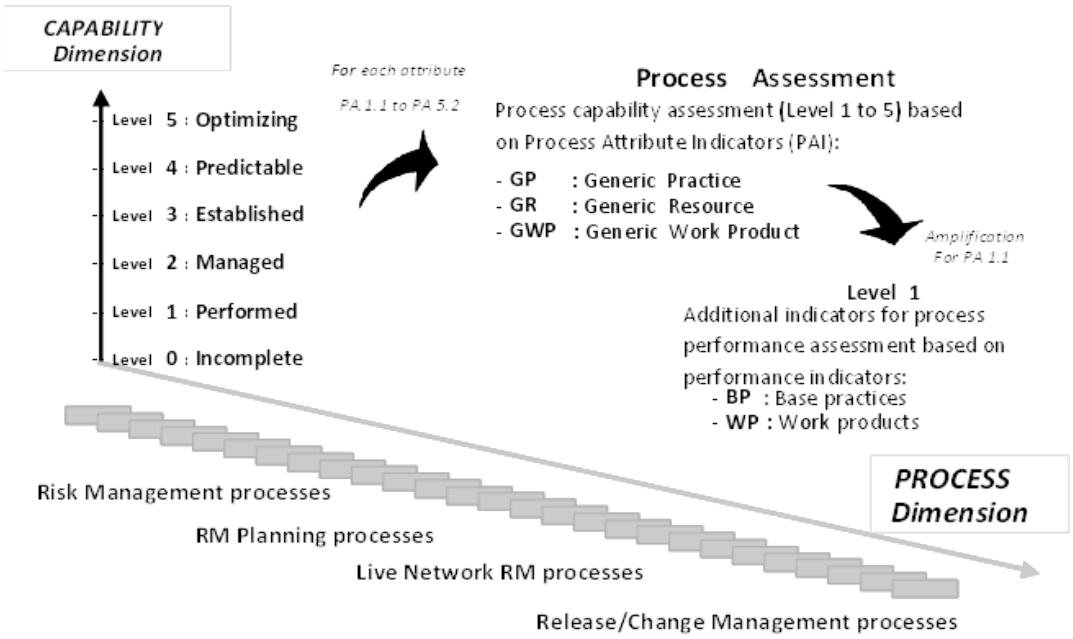

Figure C.4 — Assessment Indicators

C.3.2 Process Capability Indicators

The three types of process capability indicators related to levels 1 to 5 are identified in Figure C.5. They are intended to be applicable to all processes.

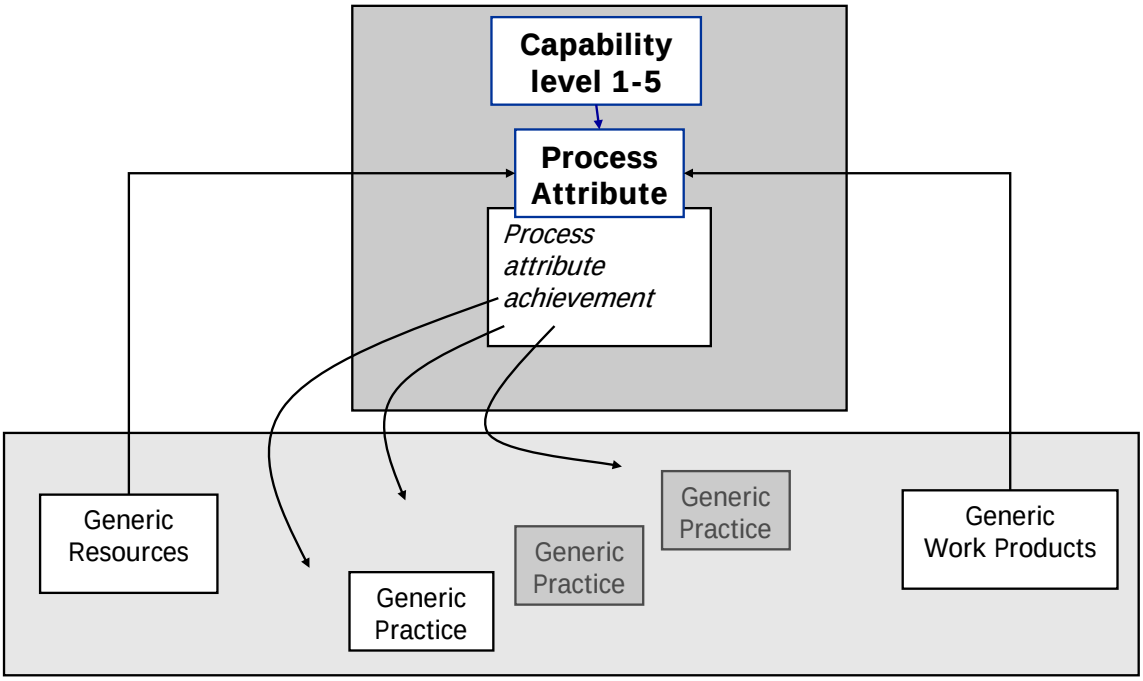

Figure C.5 — Process capability indicators

All the process capability indicators relate to the process attributes defined in the capability dimension of the PAM. They represent the type of evidence that would support judgments of the extent to which the attributes are achieved. Evidence of their effective performance or existence supports the judgment of the degree of achievement of the attribute. The generic practices are the principal indicators of process capability.

The **Generic Practice (GP)** indicators are indicators of activities of a generic type and provide guidance on the implementation of the attribute's characteristics. They support the achievement of the process attribute and many of them concern management practices, i.e. practices that are established to support the process performance as it is characterized at level 1.

During the evaluation of process capability, the primary focus is on the performance of the generic practices. In general, performance of all generic practices is expected for full achievement of the process attribute.

The **Generic Resource (GR)** indicators are associated resources that may be used when performing the process in order to achieve the attribute. These resources may include human resources, tools, methods and infrastructure. The availability of a resource indicates the potential to fulfil the purpose of a specific attribute.

NOTE: The assessor should interpret the generic resources according to the process assessed; e.g. for PA2.1 resources (with identified objectives, responsibilities and authorities), an assessor would look for roles (with identified objectives, responsibilities and authorities) in primary and supporting processes, but for organizational processes would look for governance structures (e.g. mandated committees, positions) with identified objectives, responsibilities and authorities.

The **Generic Work Product (GWP)** indicators are sets of characteristics that would be expected to be evident in work products of generic types as a result of achievement of an attribute. The generic work products form the basis for the classification of the work products defined as process performance indicators; they represent basic types of work products from all types of processes.

These three types of indicators help to establish objective evidence of the extent of achievement of the specified process attribute.

Due to the fact that Level 1 capability of a process is only characterized by the measure of the extent to which the process purpose is achieved, the process performance attribute (PA.1.1) has a single generic practice indicator (GP.1.1.1). In order to support the assessment of PA.1.1 and to amplify the process performance achievement analysis, additional process performance indicators are defined in the PAM.

C.3.3 Process Performance Indicators

There are two types of process performance indicators: **Base Practice (BP)** indicators and **Work Product (WP)** indicators. Process performance indicators relate to individual processes defined in the process dimension of the PAM and are chosen to explicitly address the achievement of the defined process outcomes.

Evidence of performance of the base practices, and the presence of work products with their expected characteristics, provide objective evidence of the achievement of the process outcomes.

A base practice is an activity that addresses the purpose of a particular process. Consistently performing the base practices associated with a process helps the consistent achievement of its purpose. A coherent set of base practices is associated with each process in the process dimension. The base practices are described at an abstract level, identifying "what" should be done without specifying "how". Implementing the base practices of a process should achieve the basic outcomes that reflect the process purpose. Base practices represent only the first step in building process capability, but the base practices represent the unique, functional activities of the process, even if that performance is not systematic. The performance of a process produces work products that are identifiable and usable in achieving the purpose of the process. In this assessment model, each work product has a defined set of example work product characteristics that may be used when reviewing the work product to assess the effective performance of a process. Work product characteristics may be used to identify the corresponding work product produced/used by the assessed organization.

Subclauses C.5.2 to C.5.15 extend the description of the processes contained within the PRM with the inclusion of base practices and the associated work products.

Table C.4 contains a list of generic and specific work products together with the work product characteristics.

C.4 Measuring process capability

The process performance and process capability indicators in this model give examples of evidence that an assessor might obtain, or observe, in the performance of an assessment. The evidence obtained in the assessment, through observation of the implemented process, can be mapped onto the set of indicators to enable correlation between the implemented process and the processes defined in this assessment model. These indicators provide guidance for assessors in accumulating the necessary objective evidence to support judgments of capability. They are not intended to be regarded as a mandatory set of checklists to be followed.

An indicator is defined as an objective characteristic of a practice or work product that supports the judgment of the performance or capability of an implemented process. The assessment indicators, and their relationship to process performance and process capability, are shown in Figure C.6.

Assessment indicators are used to confirm that certain practices were performed, as shown by observable evidence collected during an assessment. All such evidence comes either from the examination of work products of the processes assessed, or from statements made by the performers and managers of the processes.

The existence of base practices, work products, and work product characteristics, provide evidence of the performance of the processes associated with them. Similarly, the existence of process capability indicators provides evidence of process capability.

The evidence obtained should be recorded in a form that clearly relates to an associated indicator, so that the support for the assessor’s judgment can be readily confirmed or verified as required by ISO/IEC 15504-2.

The output from a process assessment is a set of process profiles, one for each process within the scope of the assessment. A typical process profile is illustrated in ISO/IEC 15504-4. Each process profile consists of a set of the process attribute ratings for an assessed process. Each attribute rating represents a judgment by the assessor of the extent to which the attribute is achieved. To improve the reliability and repeatability of the assessment, the judgments of the assessor are based on a coherent set of recorded objective evidences.

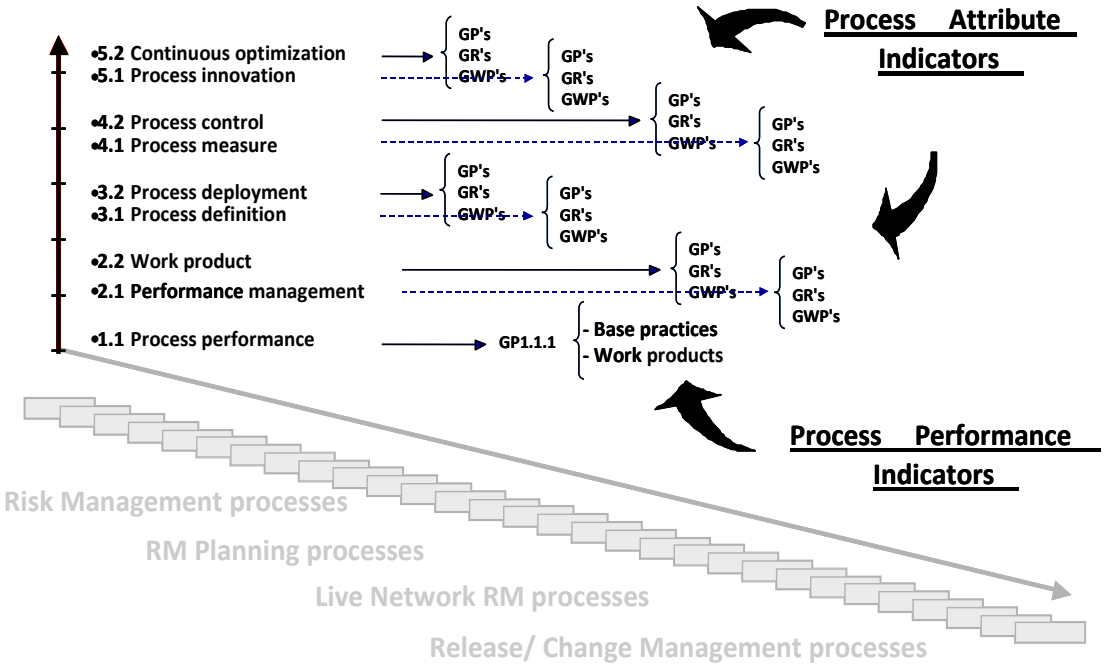

Figure C.6 — Relationship between assessment indicators and process capability

C.5 The process dimension and process performance indicators (Level 1)

C.5.1 General

This subclause defines the processes and the process performance indicators, also known as the process dimension, of the PAM. The processes in the process dimension can be directly mapped to the processes defined in the PRM. The process purposes, outcomes, the practices, the inputs and outputs of processes are included in this subclause. The individual processes are described in terms of process name, process purpose, and process outcomes as defined in IEC 80001-1 (PRM):

In addition, the process dimension of the PAM provides information in the form of:

— a set of base practices for the process needed to accomplish the process outcomes; a single base practice is explicitly associated with one or more process outcome;

— a number of inputs/outputs associated with each process and their relationship to one or more of its outcomes by numbers in square brackets, (i.e. [n]);

— characteristics associated with each input/output.

The Work product identifiers and characteristics are contained in Table C.4.
The process purposes, outcomes, the base practices and the work products associated with the processes are included in this clause. The work product characteristics are contained in clause C.8 of this Annex. The base practices and work products constitute the set of indicators of process performance. The associated work products listed in this clause may be used when reviewing potential inputs and outputs of an organization's process implementation. The associated work products provide objective guidance for potential inputs and outputs to look for, and objective evidence supporting the assessment of a particular process. A documented assessment process and assessor judgment is needed to ensure that process context (application domain, business purpose, development methodology, size of the organization, etc.) is explicitly considered when using this information. This list should not be considered as a checklist of what each organization must have but rather as an example and starting point for considering whether, given the context, the work products are necessary and contributing to the intended purpose of the process. These work products are identified with their work product identifier number as used in the Table C.3

Please note that details of the process context, purpose and outcomes have not been included within the PAM. These details can be found by referring to the individual process in the PRM which can be found subclauses B.3.1 to B.3.14 of Annex B. The process ID used in the PRM is provided in each of the PAM process descriptions that follow in subclauses C.5.2 to C.5.15.

C.5.2 Medical IT-Network Risk Management Process

Process ID:	MRM.1
Name:	Medical IT-Network Risk Management Process (PRM Reference: B.2.1)
Base Practices:	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. [Outcome: 1]. 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. [Outcome: 2, 4]. 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. [Outcome : 5, 6, 8] 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. [Outcome : 7, 9] 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. [Outcome : 1, 10} MRM.1.BP6: Review Risk Management Activities at defined intervals. Risk management activities, including Event Management, are reviewed at defined intervals. [Outcome : 3]
Inputs:	**Outputs:**
08-03 Risk Management Plan [MRM.1, BP.4, BP.6] [Outcome 7,9 & 3]	16-02 Medical IT-Network Risk Management file [MRM.1, BP.1,5] [Outcome 1,10]
	14-01 Risk Management Resource Register [MRM.1, BP.2,3] [Outcome 2, 4 & 5, 6, 8]

C.5.3 Risk Analysis & Evaluation Process

Process ID:	MRM.1.1
Name:	Risk Analysis & Evaluation Process (PRM Reference: B.2.2)
Base Practices:	MRM.1.1.BP1: Identify likely hazards. Identify hazards that are likely to arise from the Medical IT-Network. [Outcome: 1]. MRM.1.1.BP2: Estimate, analyze and evaluate associated risks. Evaluate associated risks using available information or data throughout the lifecycle for each identified hazard. [Outcome: 2]. 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. [Outcome : 3] 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. [Outcome 4, 5].
Inputs:	**Outputs:**
08-03 Risk Management plan [MRM1.1, BP.4] [Outcome 4,5]	03-02Risk log [MRM1.1, BP.1] [Outcome 1]
	15-01 Risk analysis report [MRM1.1, BP.2] [Outcome 2]
	15-02 Risks status report [MRM1.1, BP.2] [Outcome 2]
	07-01 Risk Measure [MRM1.1, BP.2, 3] [Outcome 2, 3]
	03-03 Hazard log [MRM1.1, BP.1] [Outcome1]
	03-04 Consequences log [MRM1.1, BP.3] [Outcome 3]
	16-02 Medical IT-Network Risk Management file [MRM1.1, BP.4] [Outcome 4,5]

C.5.4 Risk Control Process

Process ID:	MRM.1.2
Name:	Risk Control Process (PRM Reference: B.2.3)
Base Practices:	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. [Outcome: 1, 2, 3]. 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. (Changes to a medical device without documented consent of the medical device manufacturer are NOT recommended). [Outcome: 5, 8]. MRM.1.2.BP3: Record selected risk control measures in the Medical IT-Network Risk Management File. [Outcome: 6]. 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. [Outcome: 4, 9]. 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. [Outcome: 7].
Base Practices:	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. [Outcome: 10]. MRM.1.2.BP7: Review and evaluate risk control measures & 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. [Outcome: 11].

Inputs:	**Outputs:**
13-02 Risk action request [MRM1.2, BP.1] [Outcome 1, 2, 3]	13-03 Risk Benefit Analysis Record [MRM1.2, BP.4] [Outcome 4]
08-02 Release plan [MRM1.2, BP.2] [Outcome 5, 8]	16-02 Medical IT-Network Risk Management File [MRM1.2, BP.3, 6, 7] [Outcome 6, 9, 10, 11]
08-05 Change Management plan [MRM1.2, BP.2, BP.6] [Outcome 5, 8, 10]	

C.5.5 Residual Risk Process

Process ID:	MRM.1.3
Name:	Residual Risk Process (PRM Reference: B.2.4)
Base Practices:	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. [Outcome: 1, 3]. 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. [Outcome: 2]. 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. [Outcome: 4]. MRM.1.3.BP4: Define and document residual risk summary. [Outcome: 5]. 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). [Outcome: 6]. 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. [Outcome: 6].

Inputs:	**Outputs:**
13-03 Risk Benefit Analysis record [MRM1.3, BP.1, 2, 3] [Outcome 1, 2, 3, 4]	13-03 Risk Benefit Analysis record [MRM1.3, BP.4, 5] [Outcome 5,6]
	16-02 Medical IT-Network Risk Management File [MRM1.3, BP.4] [Outcome 5]

C.5.6 Change Release & Configuration Management Process

Process ID:	CRCM.1
Name:	Change Release & Configuration Management Process (PRM Reference: B.2.5)
Base Practices:	CRCM.1.BP1. Document & Apply Configuration Management process. Document configuration management process and apply during the risk management of change release management. [Outcome: 5]. CRCM.1.BP2: Document Configuration Management information. Document current configuration management information in the Medical IT-Network Risk Management file. [Outcome: 1]. CRCM.1.BP3: Document Change Release Process. Document and apply change-release management (including Risk Management). [Outcome : 3]. 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. [Outcome: 4]. CRCM.1.BP5: Implement action plans following the Change-Release management process. [Outcome : 2].

Inputs:	**Outputs:**
09-01 Configuration Management Policy [CRCM.1, BP1] [Outcome 5]	09-01 Configuration Management Policy [CRCM.1, BP1] [Outcome 5]
08-05 Configuration Management Plan [CRCM.1, BP1] [Outcome 5]	08-05 Configuration Management Plan [CRCM.1, BP1] [Outcome 5]
09-03 Release Policy [CRCM.1, BP.3] [Outcome 3]	09-02 Configuration item definition policy [CRCM.1, BP.2] [Outcome 1]
08-02 Release Plan [CRCM.1, BP.3] [Outcome 3]	13-01 Configuration Management Record [CRCM.1, BP.2] [Outcome 1]
08-03 Risk Management plan [CRCM.1, BP.4] [Expected Result 4]	03-01 Configuration Item Change log [CRCM.1, BP.2] [Outcome 1]
	16-01 Configuration Management DB repository [CRCM.1, BP.2] [Outcome 1]
	23-01 Configuration item control procedure [CRCM.1, BP.2] [Outcome 1]
	16-02 Medical IT-Network Risk Management File [CRCM.1, BP.2] [Outcome 1]
	09-03 Release Policy [CRCM.1, BP.3] [Outcome 3]
	08-02 Release Plan [CRCM.1, BP.3] [Outcome 3]

C.5.7 Decision on how to apply Risk Management Process

Process ID:	CRCM.2
Name:	Decision on the application of Risk Management Process (PRM Reference: B.2.6)
Base Practices:	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. [Outcome: 1]. 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.] [Outcome: 2]. CRCM.2.BP3: Define change permit. Define change permit and specify what records are to be kept for each permitted change. [Outcome: 3, 4]. CRCM.2.BP4: Specify the constraints of the change permit. [Outcome: 3]. CRCM.2.BP5: Implement routine change. Implement routine change once change permit has been defined and the constraints have been specified. [n/a]. CRCM.2.BP6: Document Change permits. Document change permits and maintain in the Medical IT- Network Risk Management File. [Outcome: 5]. 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). [Outcome: 6]. CRCM.2.BP8: Maintain & revise Project Plan. Maintain project plan and revise to reflect changes to the project. [Outcome: 6, 7]. CRCM.2.BP9: Document Project plan. Document the project plan in the Medical IT-Network Risk management file. [Outcome: 8].

Inputs:	**Outputs**
08-05 Configuration Management Plan [CRCM.2, BP.1] [Outcome1]	13-04 Change Permit Record [CRCM.2, BP.3, 4, 6] [Outcome3,4,5
08-02 Release plan [CRCM.2, BP.1] [Outcome]	08-01 Project Plan [CRCM.2, BP.7, 8, 9] [Outcome6, 7, 8]
Inputs:	Outputs
	16-02 Medical IT-Network Risk Management File [CRCM.2, BP.9] [Outcome8]

C.5.8 Go Live Process

Process ID:	CRCM.3	
Name:	Go-Live Process (PRM Reference: B.2.7)	
Base Practices:	CRCM.3.BP1: Review residual risk. Review Medical IT-Network residual risk summaries for acceptability of risk associated with interactions of recent or pending projects or changes, prior to going live. [Outcome: 1, 2]. CRCM.3.BP2: Approve specified change. Approval is given for the specified change by the Medical IT-Network Risk Manager prior to go-live. [Outcome: 3]. CRCM.3.BP3: Document approval of residual risk. Document the approval of the Medical IT-Network residual risk in the Medical IT-Network risk management file. [Outcome: 4].	
Inputs:		**Outputs:**
13-03 Risk Benefit Analysis Record [CRCM.3, BP1, 2] [Outcome 1, 2, 3]		08-02 Change Request Approval Record [CRCM.3, BP.2, 3] [Outcome 3, 4]
		16-02 Medical IT-Network Risk Management File [CRCM.3, BP.3] [Outcome 4]

C.5.9 Monitoring Process

Process ID:	LNRM.1	
Name:	Monitoring Process (PRM Reference: B.2.8)	
Base Practices:	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. [Outcome: 1]. LNRM.1.BP2: Include monitoring requirements as part of the risk management plan. [Outcome: 2]. LNRM.1.BP3: Initiate Event Management process. Initiate the Event Management process where monitoring initiates actual or potential increase in risk. [Outcome: 3].	
Inputs:		**Outputs:**
08-03 Risk Management plan [LNRM.1, BP.2] [Outcome 2]		23-03 Monitoring Procedure [LNRM.1, BP.1] [Outcome 1]
		08-03 Risk Management plan [LNRM.1, BP.2] [Outcome 2

C.5.10 Event Management Process

Process ID:	LNRM.2
Name:	Event Management Process (PRM Reference: B.2.9)
Base Practices:	LNRM.2.BP1: Establish Event Management Process. Establish Event Management process to ensure that negative events are captured and documented. [Outcome: 1]. LNRM.2.BP2: Evaluate events and proposed changes arising from events. Evaluate events and proposed changes arising from events. [Outcome: 2]. LNRM.2.BP3: Manage proposed changes. Manage proposed changes through the change-release management process. [Outcome: 2]. LNRM.2.BP4: Track corrective and preventive actions. Track all corrective and preventive actions leading to closure. [Outcome: 3]. LNRM.2.BP5: Report significant finds. Report significant finds to the medical IT-network risk manager and/or others in the responsible organization. [Outcome: 4].

Inputs:	**Outputs:**
08-02 Release plan [LNRM.2, BP3] [Outcome 2]	23-04 Event Management Procedure [LNRM.2, BP.1, 2, 4] [Outcome1, 2, 3]
08-05 Change Management plan [LNRM.2, BP3] [Outcome 2]	15-03 Event Management Report [LNRM.2, BP.5] [Outcome 4]

C.5.11 Medical IT-Network Planning Process

Process ID:	MDP.1
Name:	Medical IT-Network Planning Process (PRM Reference: B.2.10)
Base Practices:	MDP.1.BP1: Plan risk management activities. Plan risk management activities considering the current state of the IT network and planned changes. [Outcome: 1]. MDP.1.BP2: 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. [Outcome: 2] MDP.1.BP3: Maintain and update risk management plan for each Medical IT-Network. Risk Management plan is maintained and updated when a project introduces changes to an existing Medical IT-Network. [Outcome: 3, 4].

Inputs:	**Outputs:**
08-03 Risk Management plan [MDP.1, BP1, 3] [Outcome 1, 2, 4]	08-03 Risk Management plan [MDP.1, BP1, 2, 3] [Outcome 1, 2, 4]
	08-01 Project plan [MDP.1, BP.3] [Outcome 3]

C.5.12 Medical IT-Network Documentation Process

Process ID:	MDP.3
Name:	Medical IT-Network Documentation Process (PRM Reference: B.2.11)
Base Practices:	MDP.2.BP1: Obtain/Provide additional documentation for the connection of a medical device to an IT network. Obtain (Responsible organisation) /Provide (medical device manufacturer) instructions for implementing the connection of a medical device to an IT network. [Outcome: 1]. MDP.2.BP2: Maintain accompanying documents in the Medical IT-Network risk management file. Maintain documents and additional documentation (obtained for a medical device incorporated into an IT network) as required for risk management purposes in the Medical IT-Network Risk Management file. [Outcome: 2, 3, 4]. MDP.2.BP3: Maintain risk relevant asset description. Maintain risk relevant asset description, including a list of assets of IT networks interfacing with medical devices, as part of the risk management process. [Outcome: 5, 6]. MDP.1.BP5: Establish document control procedure. [Outcome: 6]. MDP.1.BP4: 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 [Outcome: 7]. MDP.1.BP5: Provide traceability for each identified hazard. Provide traceability for each identified hazard within the Medical IT-Network risk management file. [Outcome: 8].

Inputs:	**Outputs**
03-03 Hazard log [MDP.1, BP.1] [Outcome 1]	03-03 Hazard log [MDP.1, BP.1] [Outcome 1]
03-04 Consequence log [MDP.1, BP.1] [Outcome 1]	03-04 Consequence log [MDP.1, BP.1] [Outcome 1]
	06-01 Installation Guide [MDP.1, BP.1] [Outcome 1]
	06-02 Training Material [MDP.1, BP.1] [Outcome 1]
Inputs:	Outputs
	06-03 Product Operation guide [MDP.1, BP.1] [Outcome 1]
	17-01 Product requirements [MDP.1, BP.1] [Outcome 1]
	17-02 Software Requirements [MDP.1, BP.1] [Outcome 1]
	17-03 System Requirements [MDP.1, BP.1] [Outcome 1]
	22-01 Release Notes [MDP.1, BP.1] [Outcome 1]
	16-02 Medical IT-Network Release Management file [MDP.1, BP.2] [Outcome 2]
	14-02 Risk relevant asset register [MDP.1, BP.3] [Outcome 3]
	23-02 Document Management Procedure [MDP.1, BP.5, 6] [Outcome 7]
	16-02 Medical IT-Network Risk Management File [MDP.1, BP.7] [Outcome 8]

C.5.13 Responsibility Agreements Process

Process ID:	MDP.3
Name:	Responsibility Agreements Process (PRM Reference: B.2.12)
Base Practices:	MDP.3.BP1: Determine the need for a responsibility agreement. Determine the need for one or more documented responsibility agreements whenever a medical device is incorporated into an It network or the configuration of such a connection is changed. [Outcome: 1]. MDP.3.BP2: Define the responsibilities of stakeholders within the responsibility agreement. [Outcome: 2]. MDP.3.BP3: Define the scope of the responsibility agreement. Define the scope of the responsibility agreement including whether the agreement applies to one or more project or the maintenance of one or more Medical IT-Networks. Compliance is checked by inspection of the Medical IT-Network risk management file. [Outcome: 3].

Inputs:	**Outputs:**
n/a	02-01 Responsibility Agreement [MDP.3, BP.1, 2, 3] [Outcome 1, 2, 3]
	16-02 Medical IT-Network Risk Management File [MDP.3, BP.3] [Outcome 3]

C.5.14 Risk Management Policy Process

Process ID:	MDP.4
Name:	Risk Management Policy Process (PRM Reference: B.2.13)
Base Practices:	MDP.4.BP1: Establish Risk Management Policy. Risk Management policy outlines criteria for determining acceptable risk, taking into account relevant international standards and national or regional regulations. [Outcomes: 1, 2]. MDP.4.BP2: Document Risk Management Policy with the Medical IT-Network Risk Management file. [Outcome: 1]. MDP.4.BP3: Design the risk management policy to balance the three key properties with the mission of the responsible organisation. [[Outcome: 1, 3]. MDP.4.BP4: Include description of or reference to processes applying to Medical IT-Networks. Include description of or reference to processes applying to Medical IT-Networks. (Including at least Event Management, Change - Release Management, Configuration Management & Monitoring). [Outcome: 4].

Inputs:	**Outputs:**
09-04 Risk Management Policy [MDP.4, BP.1] [Outcome 1, 2]	09-04 Risk Management Policy [MDP.4, BP.1] [Outcome 1, 2]
Inputs:	Outputs:
	16-02 Medical IT-Network Risk Management file [MDP.4, BP.2] [Outcome 1]

C.5.15 Organisational Risk Management Process

Process ID:	MDP.5
Name:	Organisational Risk Management Process (PRM Reference: B.2.14)
Base Practices:	MDP.5.BP1: Establish & maintain Risk Management Process. Establish and maintain a risk management process which takes into account the defined use of the medical IT-network. [Outcome : 4] MDP.5.BP2: Execute Risk Management Process in line with Risk Management Policy. Medical IT-Network risk Manager executes the risk management process in line with the risk management policy. [Outcome: 1]. MDP.5.BP3: Report on performance of Risk Management Process. Report (made by Medical IT-Network Risk Manager) on the performance of the risk management process to Top Management. [Outcome: 2]. MDP.5.BP4: Manage communications. Manage communications (made by Medical IT-Network Risk Manager) between internal and external participants in risk management. [Outcome: 3].

Inputs:	**Outputs:**
09-04 Risk Management policy [MDP.2, BP.2] [Outcome 1]	15-04 Risk Management Process Report [MDP.5, BP.3] [Outcome 2]
	08-06 Risk Management Communications Plan [MDP.5, BP.4] [Outcome 3]

C.6 Process capability indicators (Level 1 to 5)

This clause presents the process capability indicators related to the process attributes associated with capability levels 1 to 5 defined in the capability dimension of the PAM. Process capability indicators are the means of achieving the capabilities addressed by the considered process attributes. Evidence of process capability indicators supports the judgment of the degree of achievement of the process attribute.

The capability dimension of the PAM consists of six capability levels matching the capability levels defined in ISO/IEC 15504-2. This clause describes the process capability indicators for the nine process attributes included in the capability dimension for levels 1 to 5. Clause 5 describes the assessment indicators for process performance which is characterized by Level 1 process capability.

Level 0 does not include any type of indicators. Level 0 reflects a non-implemented process or a process which fails to partially achieve its outcomes.

NOTE 1 In the next paragraphs, ISO/IEC 15504-2 process attribute definitions and attribute achievements are identified with italic font.

NOTE 2 Following each generic resource and generic input/output is '[PA x.y Achievement 1]'. This refers to process attribute x.y achievement 1 which is satisfied by this indicator.

Level 1: Performed process

PA 1.1 Process performance attribute

The process performance attribute is a measure of the extent to which the process purpose is achieved. As a result of full achievement of this attribute:

— The process achieves its defined outcomes.

Generic Practices for PA 1.1

GP 1.1.1 Achieve the process outcomes
Perform the intent of the practices.
Use inputs and produce outputs that evidence the process

NOTE 3 The assessment of a performed process is based on process performance indicators, which are defined in subclauses.3.1 and 3.2 of this Annex.

Generic Resources for PA 1.1

Resources are used to perform the intent of process specific practices.

[PA 1.1 Achievement a]

Generic Inputs/Outputs for PA 1.1

11-00 Product [PA 1.1 Achievement a]

- Inputs/Outputs exist that provide evidence of the achievement of the process outcomes.

Level 2: Managed process

The previously described *Performed process* is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

The following attributes of the process, together with the previously defined attributes, demonstrate the achievement of this level:

PA 2.1 Performance management attribute

The performance management attribute is a measure of the extent to which the performance of the process is managed. As a result of full achievement of this attribute:

— objectives for the performance of the process are identified;

— performance of the process is planned and monitored;

— performance of the process is adjusted to meet plans;

— responsibilities and authorities for performing the process are defined, assigned and communicated;

— resources and information necessary for performing the process are identified, made available, allocated and used;

— interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.

Generic Practices for PA 2.1

GP 2.1.1 Identify the objectives for the performance of the process.
NOTE: Performance objectives may include – (1) quality of the outputs produced, (2) process cycle time or frequency and (3) resource usage.
Performance objectives are identified based on process requirements and customer requirements.
The scope and boundaries of the process performance is defined.
Assumptions and constraints are considered when identifying the performance objectives.
GP 2.1.2 Plan and monitor the performance of the process to fulfil the identified objectives.
Plan(s) for the performance of the process are developed. The process performance cycle is defined.
Key milestones for the performance of the process are established.
Estimates for process performance attributes are determined and maintained.
Process activities and tasks are defined.
Schedule is defined and aligned with the approach to performing the process.
Process inputs/outputs reviews are planned.
The process is performed according to the plan(s).
Process performance is monitored to ensure planned results are achieved.
GP 2.1.3 Adjust the performance of the process.
Process performance issues are identified.
Appropriate actions are taken when planned results and objectives are not achieved.
The plan(s) are adjusted, as necessary.
Rescheduling is performed as necessary.
GP 2.1.4 Define responsibilities and authorities for performing the process.
Responsibilities, commitments and authorities to perform the process are defined, assigned and communicated.
Responsibilities and authorities to verify process inputs/outputs are defined and assigned.
The needs for process performance experience, knowledge and skills are defined.
GP 2.1.5 Identify and make available resources to perform the process according to plan.
The human and infrastructure resources necessary for performing the process are identified, made available, allocated and used.
The information necessary to perform the process is identified and made available.
GP 2.1.6 Manage the interfaces between involved parties.
The individuals and groups involved in the process performance are determined.
Responsibilities of the involved parties are assigned.
Interfaces between the involved parties are managed.
Communication is assured between the involved parties.
Communication between the involved parties is effective.

Generic Resources for PA 2.1

Human resources with identified objectives, responsibilities and authorities; [PA 2.1 Achievement a, d, e, f]

Facilities and infrastructure resources; [PA 2.1 Achievement a, d, e, f]

— Planning, management and control tools, including time and cost reporting, and feedback;[PA 2.1 Achievement b, c]

— Workflow management system; [PA 2.1 Achievement d, f]

— Email and/or other communication mechanisms; [PA 2.1 Achievement d, f]

— Information and/or experience repository; [PA 2.1 Achievement b, e]

— Problem and issue management mechanisms. [PA 2.1 Achievement c]

Generic Inputs/Outputs for PA 2.1

8-00 Plan [PA 2.1 Achievement a, b, c, d, e, f]

— Defines objectives to perform the process.

— Describes assumptions and constraints considered in defining the objectives.

— Includes milestones and timetable to produce the outputs of the process.

— Identifies tasks, resources, responsibilities and infrastructure needed to perform the process.

— Considers risks related to fulfil defined objectives.

— Identifies stakeholders and communication mechanisms to be used.

— Describes how the plan is controlled and adjusted when needed.

13-00 Record [PA 2.1 Achievement c, d, e, f]

— States results achieved or provide evidence of activities performed in a process.

— Provides evidence of communication, meetings, reviews and corrective actions.

— Contains status information about corrective actions; schedule and work breakdown structure.

— Monitors identified risks.

15-00 Report [PA 2.1 Achievement b, c]

— Monitors process performance against defined objectives and plans.

— Identifies deviations in process performance.

— Describes results and status of the process.

— Provides evidence of management activities.

PA 2.2 Work product management attribute

The work product management attribute is a measure of the extent to which the work products produced by the process are appropriately managed. As a result of full achievement of this attribute:

- requirements for the work products of the process are defined;
- requirements for documentation and control of the work products are defined;
- work products are appropriately identified, documented, and controlled;
- work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

Requirements for documentation and control of work products may include requirements for the identification of changesand revision status, approval and re-approval of work products, and the creation of relevant versions of applicable work products available at points of use.

NOTE The work products referred to in this clause are those that result from the achievement of the process outcomes.

Generic Practices for PA 2.2

GP 2.2.1 Define the requirements for the work products.
The requirements for the outputs to be produced are defined. Requirements may include defining contents and structure.
Quality criteria of the outputs are identified.
Appropriate review and approval criteria for the outputs are defined.
GP 2.2.2 Define the requirements for documentation and control of the outputs.
Requirements for the documentation and control of the outputs are defined. Such requirements may include requirements for (1) distribution, (2) identification of outputs and their components (3) traceability.
Dependencies between outputs are identified and understood.
Requirements for the approval of outputs to be controlled are defined.
GP 2.2.3 Identify, document and control the outputs.
The outputs to be controlled are identified.
Change control is established for the outputs.
The outputs are documented and controlled in accordance with requirements.
Versions of outputs are assigned to product configurations as applicable.
The outputs are made available through appropriate access mechanisms.
The revision status of the outputs may readily be ascertained.
GP 2.2.4 Review and adjust outputs to meet the defined requirements.
Outputs are reviewed against the defined requirements in accordance with planned arrangements.
Issues arising from outputs reviews are resolved.

Generic Resources for PA 2.2

- Requirement management method/toolset; [PA 2.2 Achievement a, b, c]
- Configuration management system; [PA 2.2 Achievement b, c]
- Documentation elaboration and support tool; [PA 2.2 Achievement b, c]
- Output review methods and experiences; [PA 2.2 Achievement d]
- Intranets, extranets and/or other communication mechanisms; [PA 2.2 Achievement b, c]
- Problem and issue management mechanisms. [PA 2.2 Achievement d]

Generic Inputs/Outputs for PA 2.2

8-00 Plan [PA 2.2 Achievement b]

- Expresses selected policy or strategy to manage outputs.
- Describes requirements to develop, distribute, and maintain the outputs.
- Defines quality control actions needed to manage the quality of the outputs.

23-00 Procedure [PA 2.2 Achievement d]

- Output review methods and experiences.
- Review management method/toolset.

13-00 Record [PA 2.2 Achievement b, c, d]

- Demonstrates output reviews and contributes to traceability.
- Records the status of documentation or output.
- Contains and makes available outputs and/or configuration items.
- Supports monitoring of changes to outputs.
- Provides evidence that the changes are under control.
- Supports monitoring of changes to outputs.

25-00 Specification [PA 2.2 Achievement a, b]

- Defines the functional and non-functional requirements for outputs.
- Identifies outputs dependencies.
- Identifies approval criteria for documents.
- Defines the attributes associated with outputs to be created.

Level 3: Established process

The previously described *Managed process* is now implemented using a defined process capable of achieving its process outcomes.

The following attributes of the process demonstrate the achievement of this level:

PA 3.1 Process definition attribute

The process definition attribute is a measure of the extent to which a standard process is maintained to support the deployment of the defined process. As a result of full achievement of this attribute:

- a standard process, including appropriate tailoring guidelines, is defined that describes the fundamental elements that must be incorporated into a defined process;
- the sequence and interaction of the standard process with other processes are determined;
- required competencies and roles for performing a process are identified as part of the standard process;
- required infrastructure and work environment for performing a process are identified as part of the standard process;
- suitable methods for monitoring the effectiveness and suitability of the process are determined.

NOTE A standard process may be used as-is when deploying a defined process, in which case tailoring guidelines would not be necessary.

Generic Practices for PA 3.1

GP 3.1.1 Define the standard process that will support the deployment of the defined process. A standard process is developed that includes the fundamental process elements. The standard process identifies the deployment needs and deployment context. Guidance and/or procedures are provided to support implementation of the process as needed. Appropriate tailoring guideline(s) are available as needed.
GP 3.1.2 Determine the sequence and interaction between processes so that they work as an integrated system of processes. The standard process's sequence and interaction with other processes are determined. Deployment of the standard process as a defined process maintains integrity of processes.
GP 3.1.3 Identify the roles and competencies for performing the standard process. Process performance roles are identified. Competencies for performing the process are identified.
GP 3.1.4 Identify the required infrastructure and work environment for performing the standard process. Process infrastructure components are identified (facilities, tools, networks, methods, etc.). Work environment requirements are identified.
GP 3.1.5 Determine suitable methods to monitor the effectiveness and suitability of the standard process. Methods for monitoring the effectiveness and suitability of the process are determined. Appropriate criteria and data needed to monitor the effectiveness and suitability of the process are defined. The need to establish the characteristics of the process is considered. The need to conduct internal audit and management review is established. Process changes are implemented to maintain the standard process.

Generic Resources for PA 3.1

— Process modelling methods/tools; [PA 3.1 Achievement a, b, c, d]

— Training material and courses; [PA 3.1 Achievement a, b, c]

— Resource management system; [PA 3.1 Achievement b, c]

— Process infrastructure; [PA 3.1 Achievement a, b]

— Audit and trend analysis tools; [PA 3.1 Achievement e]

— Process monitoring method. [PA 3.1 Achievement e]

Generic Inputs/Outputs for PA 3.1

22-00 Description [PA 3.1 Achievement a, b, c, e]

— Describes the standard process, including the fundamental process elements, interactions with other processes and appropriate tailoring guidelines.

— Addresses the performance, management and deployment of the process, as described by capability levels 1 and 2 and the PA 3.2 Process deployment attribute. Addresses methods to monitor process effectiveness and suitability.

— Identifies data and records to be collected when performing the defined process, in order to improve the standard process.

— Identifies and communicates the personnel competencies, roles and responsibilities for the standard and defined process.

— Identifies the personnel performance criteria for the standard and defined process.

— Identifies the tailoring guidelines for the standard process.

8-00 Plan [PA 3.1 Achievement c, d]

— Identifies approaches for defining, maintaining and supporting a standard process, including infrastructure, work environment, training, internal audit and management review.

23-00 Procedure [PA 3.1 Achievement a, b, c, d, e]

— Provides evidence of organizational commitment to maintain a standard process to support the deployment of the defined process.

— Identifies the method to execute a step or activity in the standard process to support the deployment of the defined process.

25-00 Specification [PA 3.1 Achievement a]

— Provides reference for the standards used by the standard process and identification about how they are used.

— Provides a basis to analyze data associated with the performance of the defined process.

PA 3.2 Process deployment attribute

The process deployment attribute is a measure of the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes. As a result of full achievement of this attribute:

— a defined process is deployed based upon an appropriately selected and/or tailored standard process;

— required roles, responsibilities and authorities for performing the defined process are assigned and communicated;

— personnel performing the defined process are competent on the basis of appropriate education, training, and experience;

— required resources and information necessary for performing the defined process are made available, allocated and used;

— required infrastructure and work environment for performing the defined process are made available, managed and maintained;

— appropriate data are collected and analyzed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the process, and to evaluate where continuous improvement of the process can be made.

NOTE Competency results from a combination of knowledge, skills and personal attributes that are gained through education, training and experience.

Generic Practices for PA 3.2

GP 3.2.1 Deploy a defined process that satisfies the context specific requirements of the use of the standard process. The defined process is appropriately selected and/or tailored from the standard process. Conformance of defined process with standard process requirements is verified.
GP 3.2.2 Assign and communicate roles, responsibilities and authorities for performing the defined process. The roles for performing the defined process are assigned and communicated. The responsibilities and authorities for performing the defined process are assigned and communicated.
GP 3.2.3 Ensure necessary competencies for performing the defined process. Appropriate competencies for assigned personnel are identified. Suitable training is available for those deploying the defined process.
GP 3.2.4 Provide resources and information to support the performance of the defined process. Required human resources are made available, allocated and used. Required information to perform the process is made available, allocated and used.
GP 3.2.5 Provide adequate process infrastructure to support the performance of the defined process. Required infrastructure and work environment is available. Organizational support to effectively manage and maintain the infrastructure and work environment is available. Infrastructure and work environment is used and maintained.
GP 3.2.6 Collect and analyze data about performance of the process to demonstrate its suitability and effectiveness. Data required to understand the behaviour, suitability and effectiveness of the defined process are identified. Data are collected and analyzed to understand the behaviour, suitability and effectiveness of the defined process. Results of the analysis are used to identify where continual improvement of the standard and/or defined process can be made.

Generic Resources for PA 3.2

- Feedback mechanisms (customer, staff, other stakeholders); [PA 3.2 Achievement f]
- Process repository; [PA 3.2 Achievement a, b]
- Resource management system; [PA 3.2 Achievement b, c, d]
- Knowledge management system; [PA 3.2 Achievement d]
- Problem and change management system; [PA 3.2 Achievement f]
- Work environment and infrastructure; [PA 3.2 Achievement e]
- Data collection analysis system: [PA 3.2 Achievement f]
- Process assessment framework; [PA 4.1 Achievement f]
- Audit/review system. [PA 3.2 Achievement f]

Generic Inputs/Outputs for PA 3.2

22.0 Description [PA 3.2 Achievement a]

- Describes the defined process.
- Describes the verification activities needed to ensure the conformance of the defined process with the organization's standard process.
- Represents the interactions of the defined process with other processes.

8-00 Plan [PA 3.2 Achievement a, b, f]

- Expresses the strategy for the organizational support, allocation and use of the process infrastructure.
- Describes the resources and the elements of the infrastructure needed to deploy the defined process.
- Expresses the strategy to satisfy the service's training needs.
- Identifies process improvement proposal(s) based on analysis of suitability and effectiveness.

13-00 Record [PA 3.2 Achievement c, d, e, f]

- Is used to support and maintain the standard process assets.
- Provides evidence that the service's defined process performance data was collected.
- Provides evidence that the service personnel possess the required authorities, skills, experience and knowledge.
- Provides evidence that personnel have received the required training.
- Provides evidence that infrastructure and working environment are made available and maintained for performing the defined process.
- Records the status of required corrective actions.
- Captures the work breakdown structure needed to define the tasks and their dependencies.
- Provides evidence that information is made available for performing the defined process.

15-00 Report [PA 3.2 Achievement f]

- Provides results of the analysis, recommended corrective action, feedback to the process owner and to the organization's standard process.
- Identifies improvement opportunities of the defined process.
- Provides evidence on the suitability and effectiveness of the defined process.

Level 4: Predictable process

The previously described Established process now operates within defined limits to achieve its process outcomes. The following attributes of the process demonstrate the achievement of this level:

PA 4.1 Process measurement attribute

The process measurement attribute is a measure of the extent to which measurement results are used to ensure that performance of the process supports the achievement of relevant process performance objectives in support of defined business goals. As a result of full achievement of this attribute:

- process information needs in support of relevant business goals are established;
- process measurement objectives are derived from identified process information needs;
- quantitative objectives for process performance in support of relevant business goals are established;
- measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance;
- results of measurement are collected, analyzed and reported in order to monitor the extent to which the quantitative objectives for process performance are met;
- measurement results are used to characterize process performance.

NOTE 4 Information needs may typically reflect management, technical, service, process or product needs.

NOTE 5 Measures may be either process measures or product measures or both.

Generic Practices for PA 4.1

GP 4.1.1 Identify process information needs, in relation with business goals.
Business goals relevant to establishing quantitative process measurement objectives for the process are identified.
Process stakeholders are identified and their information needs are defined.
Information needs support the relevant business goals.
GP 4.1.2 Derive process measurement objectives from process information needs.
Process measurement objectives to satisfy defined process information needs are defined.
GP 4.1.3 Establish quantitative objectives for the performance of the defined process, according to the alignment of the process with the business goals.
Process performance objectives are defined to explicitly reflect the business goals.
Process performance objectives are verified with organizational management and process owner(s) to be realistic and useful.
GP 4.1.4 Identify product and process measures that support the achievement of the quantitative objectives for process performance.
Detailed measures are defined to support monitoring, analysis and verification needs of process and product goals.
Measures to satisfy process measurement and performance objectives are defined.
Frequency of data collection is defined.
Algorithms and methods to create derived measurement results from base measures are defined, as appropriate.
Verification mechanism for base and derived measures is defined.
GP 4.1.5 Collect product and process measurement results through performing the defined process.
Data collection mechanism is created for all identified measures.
Required data is collected in an effective and reliable manner.
Measurement results are created from the collected data within defined frequency.
Analysis of measurement results is performed within defined frequency.
Analysis results including assumptions are reported to those responsible for monitoring the extent to which qualitative objectives are met.
GP 4.1.6 Use the results of the defined measurement to monitor and verify the achievement of the process performance objectives.
Statistical or other techniques are used to quantitatively understand process performance and capability within defined control limits.
Trends of process behaviour are identified.

Generic Resources for PA 4.1

- Management information (cost, time, reliability, profitability, customer benefits, risks etc.); [PA 4.1 Achievement a, c, d, e, f]
- Applicable measurement techniques; [PA 4.1 Achievement d]
- Process measurement tools and results databases; [PA 4.1 Achievement d, e, f]
- Process measurement framework; [PA 4.1 Achievement d, e, f]
- Tools for data analysis and measurement. [PA 4.1 Achievement b, c, d, e]
- Process measurement framework [PA 4.1 e]

Generic Inputs/Outputs for PA 4.1

22-00 Description [PA 4.1 Achievement a, d]

— Defines information needs for the process.

— Specifies candidate measures and frequency of measurement.

8-00 Plan [PA 4.1 Achievement b, c]

— Defines quantitative objectives for process performance.

— Specifies measures for the process.

— Defines tasks and schedules to collect and analyze data.

— Allocates responsibilities and resources for measurement.

13-00 Record [PA 4.1 Achievement e]

— Defines data to be collected as specified in plans and measures.

15-00 Report [PA 4.1 Achievement e, f]

— Provides results of process data analysis to identify process performance parameters.

— Monitors process performance based on results of measurement.

25-00 Specification [PA 4.1 Achievement a, b, d]

— Describes information needs and performance objectives.

— Provides a basis for analysing process performance.

— Defines explicit criteria for data validation.

— Defines frequency of data collection.

PA 4.2 Process control attribute

The process control attribute is a measure of the extent to which the process is quantitatively managed to produce a process that is stable, capable, and predictable within defined limits. As a result of full achievement of this attribute:

- suitable analysis and control techniques where applicable, are determined and applied;
- control limits of variation are established for normal process performance;
- measurement data are analyzed for special causes of variation;
- corrective actions are taken to address special causes of variation;
- control limits are re-established (as necessary) following corrective action.

Generic Practices for PA 4.2

GP 4.2.1 Determine analysis and control techniques, appropriate to control the process performance. Process control analysis techniques are defined. Selected techniques are validated against process control objectives.
GP 4.2.2 Define parameters suitable to control the process performance. Standard process definition is modified to include selection of parameters for process control. Control limits for selected base and derived measurement results are defined.
GP 4.2.3 Analyze process and product measurement results to identify variations in process performance. Measures are used to analyze process performance. All situations are recorded when defined control limits are exceeded. Each out-of-control case is analyzed to identify potential cause(s) of variation. Assignable causes of variation in performance are determined. Results are provided to those responsible for taking action.
GP 4.2.4 Identify and implement corrective actions to address assignable causes. Corrective actions are determined to address each assignable cause. Corrective actions are implemented to address assignable causes of variation. Corrective action results are monitored. Corrective actions are evaluated to determine their effectiveness.
GP 4.2.5 Re-establish control limits following corrective action. Process control limits are re-calculated (as necessary) to reflect process changes and corrective actions.

Generic Resources for PA 4.2

- Process control and analysis techniques; [PA 4.2 Achievement a, c]
- Statistical analysis tools; [PA 4.2 Achievement b, c, e]
- Process control tools. [PA 4.2 Achievement d, e]

Generic Inputs/Outputs for PA 4.2

22-00 Description [PA 4.2 Achievement b, e]

- Defines parameters for process control.
- Defines and maintains control limits for selected base and derived measurement results.

8-00 Plan [PA 4.2 Achievement a]

- Defines analysis methods and techniques at detailed level.

13-00 Record [PA 4.2 Achievement a, b, c, d, e]

- Provides measurement data to identify special causes of variation.
- Provides information on defects and problems.
- Records the changes.
- Documents corrective actions to be implemented.
- Monitors the status of corrective actions.
- Collects the data and provides the basis for analysis, corrective actions and results reporting.

15-00 Report [PA 4.2 Achievement a, c, d, e]

- Provides analyzed measurement results of process performance.
- Identifies corrective actions to address assignable causes of variation.
- Ensures that selected techniques are effective and measures are validated.

Level 5: Optimizing process

The previously described Predictable process is continuously improved to meet relevant current and projected business goals.

The following attributes of the process demonstrate the achievement of this level:

PA 5.1 Process innovation attributes

The process innovation attribute is a measure of the extent to which changes to the process are identified from analysis of common causes of variation in performance, and from investigations of innovative approaches to the definition and deployment of the process. As a result of full achievement of this attribute:

— process improvement objectives for the process are defined that support the relevant business goals;

— appropriate data are analyzed to identify common causes of variations in process performance;

— appropriate data are analyzed to identify opportunities for best practice and innovation;

— improvement opportunities derived from new technologies and process concepts are identified;

— an implementation strategy is established to achieve the process improvement objectives.

Generic Practices for PA 5.1

GP 5.1.1 Define the process improvement objectives for the process that support the relevant business goals. Directions to process innovation are set. New business visions and goals are analyzed to give guidance for new process objectives and potential areas of process change. Quantitative and qualitative process improvement objectives are defined and documented.
GP 5.1.2 Analyze measurement data of the process to identify real and potential variations in the process performance. Measurement data are analyzed and made available. Causes of variation in process performance are identified and classified. Common causes of variation are analyzed to get quantitative understanding of their impact.
GP 5.1.3 Identify improvement opportunities of the process based on innovation and best practices. Industry best practices are identified and evaluated. Feedback on opportunities for improvement is actively sought. Improvement opportunities are identified.
GP 5.1.4 Derive improvement opportunities of the process from new technologies and process concepts. Impact of new technologies on process performance is identified and evaluated. Impact of new process concepts are identified and evaluated. Improvement opportunities are identified. Emergent risks are considered in identifying improvement opportunities.
GP 5.1.5 Define an implementation strategy based on long-term improvement vision and objectives. Commitment to improvement is demonstrated by organizational management and process owner(s). Proposed process changes are evaluated and piloted to determine their benefits and expected impact on defined business objectives. Changes are classified and prioritized based on their impact on defined improvement objectives. Measures that validate the results of process changes are defined to determine expected effectiveness of the process change. Implementation of the approved change(s) is planned as an integrated program or project. Implementation plan and impact on business goals are discussed and reviewed by organizational management.

Generic Resources for PA 5.1

- Process improvement framework; [PA 5.1 Achievement a, d, e]
- Process feedback and analysis system (measurement data, causal analysis results etc.); [PA 5.1 Achievement b, c]
- Piloting and trialling mechanism. [PA 5.1 Achievement c, d]

Generic Inputs/Outputs for PA 5.1

22-00 Description [PA 5.1 Achievement c, d]

- Identifies potential areas of innovation and new technology.
- Incorporates approaches to perform root cause analysis.

8-00 Plan [PA 5.1 Achievement a, e]

- Defines improvement objectives for the process
- Allocates resources for improvement activities.
- Schedules activities for root cause analysis.
- Defines an approach to implementing selected improvements.

— Identifies scope of pilot improvement activities.

23-00 Procedure [PA 5.2 Achievement a]

— Establishes expectations for conduct and evaluation of pilot improvements.

13-00 Record [PA 5.1 Achievement b, c, d, e]

— Provides analytical data to identify common causes of variation.

— Provides analytical data to identify opportunities for best practice and innovation.

— Records data relevant to root cause analysis.

— Identifies potential improvement opportunities.

— Records information on new technology and techniques.

15-00 Report [PA 5.1 Achievement b, d]

— Identifies potential innovations and process changes.

— Provides information for an analysis to identify common causes of variation in performance.

— Identifies common causes of defects and appropriate corrective actions.

25-00 Specification [PA 5.1 Achievement a]

— Define and maintain business goals.

— Provides evidence of management commitment.

PA 5.2 Process optimization attribute

The process optimization attribute is a measure of the extent to which changes to the definition, management and performance of the process result in effective impact that achieves the relevant process improvement objectives. As a result of full achievement of this attribute:

— impact of all proposed changes is assessed against the objectives of the defined process and standard process;

— implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted upon;

— effectiveness of process change on the basis of actual performance is evaluated against the defined product requirements and process objectives to determine whether results are due to common or special causes.

Generic Practices of PA 5.2

GP 5.2.1 Assess the impact of each proposed change against the objectives of the defined and standard process. Objective priorities for process improvement are established. Specified changes are assessed against product quality and process performance requirements and goals. Impact of changes to other defined and standard processes is considered.
GP 5.2.2. Manage the implementation of agreed changes to selected areas of the defined process and standard process according to the implementation strategy. A mechanism is established for incorporating accepted changes into the defined process(es) and standard process(es) effectively and completely. The factors that impact the effectiveness and full deployment of the process change are identified and managed, such as: • Economic factors (productivity, profit, growth, efficiency, quality, competition, resources, and capacity); • Human factors (job satisfaction, motivation, morale, conflict/cohesion, goal consensus, participation, training, span of control); • Management factors (skills, commitment, leadership, knowledge, ability, organizational culture and risks); • Technology factors (sophistication of system, technical expertise, development methodology, need of new technologies). Training is provided to users of the process. Process changes are effectively communicated to all affected parties. Records of the change implementation are maintained.
GP 5.2.3 Evaluate the effectiveness of process change on the basis of actual performance against process performance and capability objectives and business goals. Performance and capability of the changed process are measured and compared with historical data. A mechanism is available for documenting and reporting analysis results to management and owners of standard and defined processes. Measures are analyzed to determine whether results are due to common or special causes. Other feedback is recorded, such as opportunities for further improvement of the standard process.

Generic Resources for PA 5.2

— Change management system; [PA 5.2 Achievement a, b, c]

— Process evaluation system (impact analysis, etc.). [PA 5.2 Achievement a, c]

Generic Inputs/Outputs for PA 5.2

22-00 Description [PA 5.2 Achievement b]

— Documents changes as a result of process improvement actions.

8-00 Plan [PA 5.2 Achievement a, b]

- Defines activities and schedule for pilot change implementation.

— Allocates resources for pilot implementation.

— Assigns responsibility for pilot implementation.

— Defines activities and schedule for organizational implementation of process change.

— Allocates resources and responsibilities for organizational implementation.

— Specifies scope of pilot implementation of proposed change.

13-00 Record [PA 5.2 Achievement b]

— Contains records of all completed and in-progress pilot implementations.

— Records history of and justification for changes.

15-00 Report [PA 5.2 Achievement a, b, c]

— Describes results of pilot implementation of process change.

— Evaluates effectiveness of process compared to process improvement objectives.

— Provides details on implementation of organizational changes.

— Describes proposed changes to standard and defined process.

25-00 Specification [PA 5.2 Achievement c]

— Specifies measures derived from process improvement objectives.

C.7 Conformity of the exemplar Process Assessment Model

C.7.1 General

Annex C sets out a PAM that meets the requirements for conformance defined in ISO/IEC 15504-2. This PAM can be used in the performance of assessments that meet the requirements of ISO/IEC 15504. It may also be used as an example for a PAM developer.

This clause serves as the statement of conformance of the PAM to the requirements defined in ISO/IEC 15504-2. For ease of reference, the requirements from Clause 6.3 of ISO/IEC 15504-2 are embedded verbatim in the text of this Clause. They should not be construed as normative elements of this technical report.

Since this PAM has been explicitly constructed to be an elaboration of the PRM defined in IEC 80001-1, the conformance claim is relatively simple. For other models, particularly ones with a different architecture, the demonstration of conformance may be more difficult requiring more detail in the mapping.

Requirements for PAMs (from ISO/IEC 15504-2)

C.7.2 Introduction

In order to assure that assessment results are translatable into an ISO/IEC 15504 process profile in a repeatable and reliable manner, PAMs shall adhere to certain requirements. A PAM shall contain a definition of its purpose, scope and elements; its mapping to the Measurement Framework and specified PRM(s); and a mechanism for consistent expression of results.

A PAM is considered suitable for the purpose of assessing process capability by conforming to 6.3.2, 6.3.3, and 6.3.4.

[ISO/IEC 15504-2, 6.3.1]

The purpose of this PAM is to support assessment of process capability in accordance with the requirements of ISO/IEC 15504-2 (Refer Clause 1).

C.7.3 Process Assessment Model Scope

6.3.2.1 *A PAM shall relate to at least one process from the specified PRM(s).*

6.3.2.2 *A PAM shall address, for a given process, all, or a continuous subset, of the levels (starting at level 1) of the Measurement Framework for process capability for each of the processes within its scope.*

NOTE: It would be permissible for a model, for example, to address solely level 1, or to address levels 1, 2 and 3, but it would not be permissible to address levels 2 and 3 without level 1.

6.3.2.3 *A PAM shall declare its scope of coverage in the terms of:*

a) the selected PRM(s);
b) the selected processes taken from the PRM(s);
c) the capability levels selected from the Measurement Framework.

[ISO/IEC 15504-2, 6.3.2]

This PAM is based upon the PRM defined in IEC 80001-1(PRM).
In the capability dimension of this PAM, the model addresses all of the capability levels defined in the Measurement Framework in ISO/IEC 15504-2, Clause 5.

C.7.4 Process Assessment Model elements and indicators

A PAM shall be based on a set of indicators that explicitly addresses the purposes and outcomes, as defined in the selected PRM, of all the processes within the scope of the PAM; and that demonstrates the achievement of the process attributes within the capability level scope of the PAM. The indicators focus attention on the implementation of the processes in the scope of the model.

[ISO/IEC 15504-2, 6.3.3]

The PAM provides a two-dimensional view of process capability for the processes in the PRM, through the inclusion of assessment indicators as shown in Figure 5. The Assessment Indicators used are:

— base practices and inputs/outputs; and

— generic practices, generic resources and generic inputs/outputs as shown in Figure 5. They support the judgment of the performance and capability of an implemented process.

C.7.5 Mapping Process Assessment Models to Process Reference Models

A PAM shall provide an explicit mapping from the relevant elements of the model to the processes of the selected PRM and to the relevant process attributes of the Measurement Framework.

The mapping shall be complete, clear and unambiguous. The mapping of the indicators within the PAM shall be to:

a) the purposes and outcomes of the processes in the specified PRM;
b) the process attributes (including all of the results of achievements listed for each process attribute) in the Measurement Framework.

This enables PAMs that are structurally different to be related to the same PRM.

[ISO/IEC 15504-2, 6.3.4]

Table C.2 — Mapping of Generic Practices

GP	Practice Name	Maps To
PA 1.1: Process performance attribute		
GP 1.1.1	Achieve the process outcomes.	PA.1.1.a
PA 2.1: Performance management attribute		
GP 2.1.1	Identify the objectives for the performance of the process.	PA.2.1.a
GP 2.1.2	Plan and monitor the performance of the process to fulfil the identified objectives.	PA.2.1.b
GP 2.1.3	Control the performance of the process.	PA.2.1.c
GP 2.1.4	Define responsibilities and authorities for performing the process.	PA.2.1.d
GP 2.1.4	Define responsibilities and authorities for performing the process.	PA.2.1.d
GP 2.1.5	Identify and make available resources to perform the process according to plan.	PA.2.1.e
GP 2.1.6	Manage the interfaces between involved parties.	PA.2.1.f
PA 2.2: Work Products management attribute		
GP 2.2.1	Define the requirements for the outputs.	PA.2.2.a
GP 2.2.2	Define the requirements for documentation and control of the outputs.	PA.2.2.b
GP 2.2.3	Identify, document and control the outputs.	PA.2.2.c
GP 2.2.4	Review and adjust outputs to meet the defined requirements.	PA.2.2.d
PA 3.1: Process definition attribute		
GP 3.1.1	Define the standard process that will support the deployment of the defined process.	PA.3.1.a
GP 3.1.2	Determine the sequence and interaction between processes so that they work as an integrated system of processes.	PA.3.1.b
GP 3.1.3	Identify the roles and competencies for performing the process.	PA.3.1.c
GP 3.1.4	Identify the required infrastructure and work environment for performing the process.	PA.3.1.d
GP 3.1.5	Determine suitable methods to monitor the effectiveness and suitability of the process.	PA.3.1.e
PA 3.2: Process deployment attribute		
GP 3.2.1	Deploy a defined process that satisfies the context specific requirements of the use of the standard process.	PA.3.2.a
GP 3.2.2	Assign and communicate roles, responsibilities and authorities for performing the defined process.	PA.3.2.b
GP 3.2.3	Ensure necessary competencies for performing the defined process.	PA.3.2.c
GP.3.2.4	Provide resources and information to support the performance of the defined process.	PA.3.2.d
GP 3.2.5	Provide process infrastructure to support the performance of the defined process.	PA.3.2.e
GP 3.2.6	Collect and analyze data about performance of the process to demonstrate its suitability and effectiveness.	PA.3.2.f
PA 4.1 Process measurement attribute		
GP 4.1.1	Identify process information needs, in relation with business goals.	PA.4.1.a
GP.4.1.2	Derive process measurement objectives from process information needs.	PA.4.1.b
GP 4.1.3	Establish quantitative objectives for the performance of the defined process, according to the alignment of the process with the business goals.	PA.4.1.c
GP 4.1.4	Identify product and process measures that support the achievement of the quantitative objectives for process performance.	PA.4.1.d
GP 4.1.5	Collect product and process measurement results through performing the defined process.	PA.4.1.e

GP 4.1.6	Use the results of the defined measurement to monitor and verify the achievement of the process performance objectives.	PA.4.1.f
PA 4.2 Process control attribute		
GP 4.2.1	Determine analysis and control techniques, appropriate to control the process performance.	PA.4.2.a
GP 4.2.2	Define parameters suitable to control the process performance.	PA.4.2.b
GP 4.2.3	Analyze process and product measurement results to identify variations in process performance.	PA.4.2.c
GP 4.2.4	Identify and implement corrective actions to address assignable causes.	PA.4.2.d
GP.4.2.5	Re-establish control limits following corrective action.	PA.4.2.e
PA 5.1 Process innovation attribute		
GP 5.1.1	Define the process improvement objectives for the process that support the relevant business goals.	PA.5.1.a
GP 5.1.2	Analyze measurement data of the process to identify real and potential variations in the process performance.	PA.5.1.b
GP 5.1.3	Identify improvement opportunities of the process based on innovation and best practices.	PA.5.1.c
GP.5.1.4	Derive improvement opportunities from new technologies and process concepts.	PA.5.1.d
GP 5.1.5	Define an implementation strategy based on long-term improvement vision and objectives.	PA.5.1.e
PA 5.2 Process optimization attribute		
GP 5.2.1	Assess the impact of each proposed change against the objectives of the defined and standard process.	PA.5.2.a
GP 5.2.2	Manage the implementation of agreed changes according to the implementation strategy.	PA.5.2.b
GP 5.2.3	Evaluate the effectiveness of process change on the basis of actual performance against process objectives and business goals.	PA.5.2.c

C.7.6 Expression of assessment results

A PAM shall provide a formal and verifiable mechanism for representing the results of an assessment as a set of process attribute ratings for each process selected from the specified PRM(s).

NOTE: The expression of results may involve a direct translation of PAM ratings into a process profile as defined in this international standard, or the conversion of the data collected during the assessment (with the possible inclusion of additional information) through further judgment on the part of the assessor.

[ISO/IEC 15504-2, 6.3.5]

The processes in this PAM are identical to those defined in the PRM. The Process Attributes and the Process Attributes Rating in this PAM are identical to those defined in the Measurement Framework. As a consequence, results of Assessments based upon this PAM are expressed directly as a set of process attribute ratings for each process within the scope of the assessment. No form of translation or conversion is required.

C.8 Work Product characteristics

C.8.1 General

Characteristics of work products listed in this Clause can be used when reviewing potential inputs and outputs of process implementation. The characteristics are provided as guidance for the attributes to look for to provide objective evidence supporting the assessment of a particular process. A documented process and assessor judgment is needed to ensure that the process context (application domain, business purpose, development methodology, size of the organization, etc.) is considered when using this information. Work products are defined using the schema in Table C.3 Work products and their characteristics should be considered as a starting point for considering whether, given the context, they are contributing to the intended purpose of the process.

Table C.3 — Input/Output identification

Work Product identifier #	An identifier number for the input/output which is used to reference the input/output.
Work Product name	Provides an example of a typical name associated with the input/output characteristics. This name is provided as an identifier of the type of input/output the practice or process might produce. Organizations may call these input/outputs by different names. The name of the input/output in the organization is not significant. Similarly, organizations may have several equivalent input/outputs which contain the characteristics defined in one input/output type. The formats for the input/outputs can vary. It is up to the assessor and the organizational unit coordinator to map the actual input/outputs produced in their organization to the examples given here.
Work Product characteristics	Provides examples of the potential characteristics associated with the input/output types. The assessor may look for these in the samples provided by the organizational unit.

C.8.2 Generic Work Products

The Generic Work Product Indicators are sets of characteristics that would be expected to be evident in work products of a generic type as a result of achievement of an attribute. The generic work products form the basis for the classification of the work products defined as process performance indicators. These work product types are basic input types to process owners of all types of processes.

C.8.3 Specific inputs and outputs

Specific outputs are typically created by process owners and applied by process deployers in order to satisfy an outcome of a particular process purpose.

Table C.4 shows a list of generic outputs (ending 00 e.g. 01-00 Configuration Item) and specific outputs (not ending 00 e.g. 02-01 Responsibility Agreements).

Table C.4 (1 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
01-00	Configuration Item	– Item which is maintained under configuration control: – – may include modules, subsystems, libraries, test cases, compilers, data, documentation, physical media, and external interfaces – Version identification is maintained – Description of the item is available including: – – type of item – – associated configuration management library, file, system – – responsible owner – – date when placed under configuration control – – status information (i.e., development, baselined, released) – – relationship to lower level configured items – – identifies the change control records – – identifies change history – – relationship to previous versions and/or baselines (for recovery, if necessary) – – approval status information (i.e., development, baselined, released) – – revision status information (i.e., checked in, checked out, read only)
02-00	Contract	– Defines what is to be purchased or delivered – Identifies time frame for delivery or contracted service dates – Identifies any statutory requirements – Identifies monetary considerations – Identifies any warranty information – Identifies any copyright and licensing information (patent, copyright, confidentiality, proprietary, usage, ownership, warranty and licensing rights associated with all relevant work products) – Identifies any customer service requirements – Identifies service level requirements – References to any performance and quality expectations/constraints/monitoring – Standards and procedures to be used – Evidence of review and approval by authorized signatories – As appropriate to the contract the following are considered: – – references to any acceptance criteria – – references to any special customer needs (i.e., confidentiality requirements, security, hardware, etc.) – – references to any change management and problem resolution procedures – – identifies any interfaces to independent agents and subcontractors – – identifies customer's role in the development and maintenance process – – identifies resources to be provided by the customer
02-01	Responsibility Agreement	Whenever a medical device is incorporated into an IT network, or the configuration of such a connection is changed, the RO shall determine the need for one or more documented responsibility agreements (RA) that define (e.g. by contract) the responsibilities of all relevant stakeholders. An RA may cover one or more projects or the maintenance of one or more Medical IT-Networks and shall identify responsibility for all aspects of the Medical IT-Network life cycle and all activities that form part of that life cycle. NOTE In order to support incorporating medical devices into an IT network, the medical device manufacturers make available technical information appropriate to the creation of RO Risk Management documentation. Where the process requires information that a medical device manufacturer believes is sensitive in nature, the provision of the information is determined by the RA and can be protected by a confidentiality agreement. The RA shall contain (or refer to documents which contain) at a minimum: a) the name of the person responsible for Risk Management for the activities covered by the RA; b) the scope of the activities covered by the RA, including a summary of and/or reference to the requirements;

Table C.4 (2 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics (continued):
02-01 (cont.)	Responsibility Agreement (continued)	c) a list of the medical devices and other equipment which are to be incorporated into the IT network or changed, together with the names of medical device manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project; d) a list of documents to be supplied by the medical device manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT network; e) technical information to be supplied by the medical device or IT manufacturers and other equipment suppliers that is necessary to perform risk analysis for the It network; and f) definition of roles and responsibilities in managing potentially adverse events. The RO shall provide a summary of responsibilities as appropriate. NOTE 1 The manufacturer of a medical device is responsible for making available technical documentation on how to use the medical devices interfaces to connect to an IT network, provided that such a connection is intended by the manufacturer. There is no such obligation on the supplier of other equipment, and it might be necessary to make a specific arrangement to gain access to such technical documentation. If the co-operation of manufacturers of medical devices, suppliers of other equipment or other organizations is necessary in addition to the listed documents supplied by the manufacturers or organizations, a RA shall: g) identify the nature of the co-operation required; and h) state: • who is responsible for requesting such co-operation; • who is responsible for responding to such requests; and • what criteria will be used to judge the adequacy of such response. NOTE 2 Since this information can change through the lifecycle of a Medical IT-Network, it is recommended that it be updated periodically in the RA. Compliance is checked by inspection of the Medical IT-Network risk management file.
03-00	Data	– Result of applying a measure – Available to those who need to know within defined timeframe
03-01	Configuration item change log	Changes to CIs are traceable and auditable to ensure integrity of the CIs and the data in the CMDB.
03-02	Risk Log	A log of identified risks, their categorisation, prioritisation, and analysis.
03-03	Hazard log	Log of hazards that are likely to arise from the Medical IT-Network
03-04	Consequences log	List of possible consequences of harm
04-00	Design	– Describes the overall product/system structure – Identifies the required product/system elements – Identifies the relationship between elements – Consideration is given to: – – any required performance characteristics – – any required interfaces – – any required security characteristics
05-00	Goals	– Identifies the objective to be achieved – Identifies who is expected to achieve the goal – Identifies any incremental supporting goals – Identifies any conditions/constraints – Identifies the timeframe for achievement – Are reasonable and achievable within the resources allocated – Are current, established for current project, organization – Are optimized to support known performance criteria and plans

Table C.4 (3 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
06-00	User documentation	– Identifies: – – external documents – – internal documents – – current site distribution and maintenance list maintained – Documentation kept synchronized with latest product release – Addresses technical issues
06-01	Installation guide	– Tasks for loading/installing product sequentially order by execution requirements: – – downloading of software from delivery files – – up-loading to appropriate software to files, folders, libraries, etc. – – partial or upgrade installation instructions, where applicable – – initialization procedures – – conversion procedures – – customization/configuration procedures – – verification procedures – – bring-up procedures – – operations instructions – Installation requirements identified: – – associated hardware, software, customer documentation – – conversion programs and instructions – – initialization programs, system generation information – – components and descriptions – – minimum configuration of hardware/software required – – backup/recovery instructions – – validation programs – – configuration parameters (e.g. size requirements, memory) – Customer/technical support contacts – Troubleshooting guide – Rollback plan
06-02	Training material	– Updated and available for new releases – Coverage of system, application, operations, maintenance as appropriate to the application – Courses listings and availability
06-03	Product operation guide	– Criteria for operational use – Provides a description of how to operate the product including: – – operational environment required – – supporting tools and material (e.g. user manuals) required – – possible safety warnings – – start-up preparations and sequence – – frequently asked questions (FAQ) – – sources of further information and help to operate the product – Certification and safety approvals – Warranty and replacement instructions
07-00	Measure	– Quantitative or qualitative attribute for a product or process. – Defines the method for collecting data – Understood by those expected to use them – Provides value to the organization/project – References any relevant goals – Non-disruptive to the work flow – Appropriate to the process, life cycle model, organization – Has appropriate analysis and commentary to allow meaningful interpretation by users
07-01	Risk Measure	– Identifies the probability of risk occurring – Identifies the impact of risk occurring – Identifies the change in the risk state

Table C.4 (4 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
08-00	Plan	(As appropriate to the application and purpose) – Identifies the plan owner – Includes: – – the objective and scope of what is to be accomplished – – assumptions made – – constraints – – risks – – tasks to be accomplished – – schedules, milestones and target dates – – critical dependencies – – maintenance disposition for the plan – Method/approach to accomplish plan – Identifies: – – task ownership, including tasks performed by other parties (e.g. supplier, customer) – – quality criteria – – required work products – Includes resources to accomplish plan objectives: – – time – – staff (key roles and authorities e.g. sponsor) – – materials/equipment – – budget – Includes contingency plan for non-completed tasks – Plan is approved
08-01	Project plan	– Defines: – – work products to be developed – – life cycle model and methodology to be used – – customer requirements related to project management – – tasks to be accomplished – – task ownership – – project resources – – schedules, milestones and target dates – – estimates – – quality criteria – Identifies: – – critical dependencies – – required work products – – project risks and risk mitigation plan – – contingency actions for non-completed tasks
08-02	Release plan	– Identifies the functionality to be included in each release – Identifies the associated elements required (i.e., hardware, software, documentation etc.) – Mapping of the customer requests, requirements satisfied to particular releases of the product
08-03	Risk management plan	– Project risks identified and prioritized – Mechanism to track the risk – Threshold criteria to identify when corrective action required – Proposed ways to mitigate risks: – – risk mitigator – – work around – – corrective actions activities/tasks – – monitoring criteria – – mechanisms to measure risk

Table C.4 (5 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
08-04	Risk mitigation plan	– Planned risk treatment activities and tasks: – – describes the specifics of the risk treatment selected for a risk or combination of risks found to be unacceptable – – describes any difficulties that may be found in implementing the treatment – Treatment schedule – Treatment resources and their allocation – Responsibilities and authority: – – describes who is responsible for ensuring that the treatment is being implemented and their authority – Treatment control measures: – – defines the measures that will be used to evaluate the effectiveness of the risk treatment – Treatment cost – Interfaces among parties involved: – – describes any coordination among stakeholders or with the project's master plan that must occur for the treatment to be properly implemented – Environment/infrastructure: – – describes any environmental or infrastructure requirements or impacts (e.g., safety or security impacts that the treatment may have) – Risk treatment plan change procedures and history
08-05	Change management plan	– Defines change management activities including identification, recording, description, analysis and implementation – Defines approach to track status of change requests – Defines verification and validation activities – Change approval and implication review
08-06	Risk Management Communications Plan	The Medical IT-Network risk manager shall be responsible for the following aspects of the risk management of IT networks incorporating Medical Devices: *-establishing a plan* for managing the necessary communication between the internal and external participants in risk management. Such participants may include, as appropriate: 1) medical device manufacturers; 2) other suppliers of IT equipment, software and services; 3) internal IT function and other facilities management functions; 4) clinical users; and 5) technical support function responsible for medical devices (for example biomedical engineering).
09-00	Policy	– Authorized – Available to all personnel impacted by the policy – Establishes practices/rules to be adhered to
09-01	Change Management policy	A change management policy is established that defines: a) CIs which are under the control of change management; b) criteria to determine changes with potential to have a major impact on services or the customer.
09-02	Configuration item definition policy	Technical considerations: [9.1] There is a definition of each type of CI.
09-03	Release Policy	The provider establishes with the customer a release policy stating the frequency and type of releases.
09-04	Risk Management policy	To support the Medical IT-Network life cycle, the top management shall define and document a risk management policy for incorporating medical devices into an IT network. The risk management policy shall include:

Table C.4 (6 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics (continued):
09-04 (cont.)	Risk Management policy (continued)	a) balancing the three key properties with the mission of the responsible organisation; b) a means to establish risk acceptability criteria for each of the key properties taking into account relevant international standards and national or regional regulations; and c) a description of or reference to processes applying to Medical IT-Networks including, at least, 1) event management, 2) Change Release management, 3) configuration management, and 4) monitoring. NOTE Medical IT-Networks life cycle activities can be captured in an IT service management policy (e.g. per ISO 20000) provided there is a clear relationship to the Risk Management policy. The policy shall be expressed in terms that can be interpreted throughout all risk management activities. Compliance is checked by inspection of the Medical IT-Network risk management file.
10-00	Process description	– A detailed description of the process/procedure which includes: – – tailoring of the standard process (if applicable) – – purpose of the process – – outcomes of the process – – task and activities to be performed and ordering of tasks – – critical dependencies between task activities – – expected time required to execute task – – input/output work products – – links between input and output work products – Identifies process entry and exit criteria – Identifies internal and external interfaces to the process – Identifies process measures – Identifies quality expectations – Identifies functional roles and responsibilities – Approved by authorized personnel
11-00	Product	– Is a result/deliverable of the execution of a process, includes services, systems (software and hardware) and processed materials – Has elements that satisfy one or more aspects of a process purpose – May be represented on various media (tangible and intangible)
12-00	Proposal	– Defines the proposed solution – Defines the proposed schedule – Identifies the coverage identification of initial proposal: – – the requirements that would be satisfied – – the requirements that could not be satisfied, and provides a justification of variants – Identifies conditions (e.g. time, location) that affect the validity of the proposal – Identifies obligations of the acquirer and the consequences of these not being met – Defines the estimated price of proposed development, product, or service
13-00	Record	– Work product stating results achieved or provides evidence of activities performed in a process – An item that is part of a set of identifiable and retrievable data
13-01	Configuration management record	– Status of the work products/items and modifications – Identifies items under configuration control – Identifies activities performed e.g. backup, storage, archiving, handling and delivery of configured items – Supports consistency of the product

Table C.4 (7 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
13-02	Risk action request	– Date of initiation – Scope – Subject – Request originator – Risk management process context: – – this section may be provided once, and then referenced in subsequent action requests if no changes have occurred – – process scope – – stakeholder perspective – – risk categories – – risk thresholds – – project objectives – – project assumptions – – project constraints – Risks: – – this section may cover one risk or many, as the user chooses – – where all the information above applies to the whole set of risks, one action request may suffice – – where the information varies, each request may cover the risk or risks that share common information – – risk description(s) – – risk probability – – risk consequences – – expected timing of risk – Risk treatment alternatives: – – alternative descriptions – – recommended alternative(s) – – justifications – Risk action request disposition: – – each request should be annotated as to whether it is accepted, rejected, or modified, and the rationale provided for whichever decision is taken
13-03	Risk Benefit analysis record	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.
13-04	Change permit record	An outcome of the risk management process consisting of a document that allows a specified change or type of change without further risk management activities subject to specified constraints
14-00	Register	– A register is a compilation of data or information captured in a defined sequence to enable: – – an overall view of evidence of activities that have taken place – – monitoring and analyses – – provides evidence of performance of a process over time
14-01	Risk Management Resource Register	- Identifies: - -appropriately qualified Risk Management Resources including stakeholders to carry out management, performance of work and assessment activities. - - Details responsibilities of each of the assigned resources including responsibilities in relation to co-operation with the Medical IT-Network Risk Manager.
14-02	Risk relevant asset register	The Responsible Organisation shall establish a list of assets of IT networks interfacing with Medical devices. Typical assets include, but are not limited to hardware, software, and data essential to the Intended Use of the Medical Device and the defined use of the Medical IT-Network. The asset list may include for example:

Table C.4 (8 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics (continued):
14-02 (cont.)	Risk relevant asset register (continued)	a) specific components of the Medical IT-Network and all incorporated Medical Devices and other equipment (e.g. image creating modalities, network components) of the IT infrastructure; b) operational characteristics of the IT infrastructure of the Medical IT-Network (e.g. performance properties such as bandwidth); c) Configuration Management information; d) medical application software; e) data about configuration of hardware and software; f) characterization of identifiable patient data on the Medical IT-Network or used by the incorporated Medical Device including its nature, volume, and sensitivity; g) healthcare procedure support information, including history of use and Operator/user details; and h) a security description and other materials relevant to total system Safety considerations (in case security is an aspect of Safety). Compliance is checked by inspection of the Medical IT-Network Risk Management File.
15-00	Report	– A work product describing a situation that: – – includes results and status – – identifies applicable/associated information – – identifies considerations/constraints – – provides evidence/verification
15-01	Risk analysis report	– Identifies the risks analyzed – Records the results of the analysis: – – potential ways to mitigate the risk – – assumptions made – – constraints
15-02	Risk status report	– Identifies the status of an identified risk: – – related project or activity – – risk statement – – condition – – consequence – – changes in priority – – duration of mitigation, when started – – risk mitigation activities in progress – – responsibility – – constraints
15-03	Event Management Report	Report significant finds to the Medical IT-Network Risk Manager and/or others in the responsible organisation
15-04	Risk Management process Report	Report on the Risk Management process presented by the Medical IT-Network Risk Manager to Top Management.
16-00	Repository	– Repository for components – Storage and retrieval capabilities – Ability to browse content – Listing of contents with description of attributes – Sharing and transfer of components between affected groups – Effective controls over access – Maintain component descriptions – Recovery of archive versions of components – Ability to report component status – Changes to components are tracked to change/user requests
16-01	Configuration Management DB repository	Technical considerations: [9.1] CIs are recorded in a CMDB.
16-02	Medical IT-Network Risk Management file	Repository for all documents related to risk management activities within the Medical IT-Network.

Table C.4 (9 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
17-00	Requirement specification	– Each requirement is identified – Each requirement is unique – Each requirement is verifiable or can be assessed – Includes statutory and regulatory requirements – Includes issues/requirements from (contract) review
17-01	Product requirements	– Identifies any: – – required feature and functional characteristics – – necessary performance considerations/constraints – – necessary internal/external interface considerations/constraints – – required system characteristics/constraints – – human engineering considerations/constraints – – security considerations/constraints – – environmental considerations/constraints – – operational considerations/constraints – – maintenance considerations/constraints – – associated documentation considerations/constraints – – installation considerations/constraints – – support considerations/constraints – – design constraints – – safety/reliability considerations/constraints – – quality requirements/expectations – Includes storage requirements (products)
17-02	Software requirements	– Identifies standards to be used – Identifies any software structure considerations/constraints – Identifies the required software elements – Identifies the relationship between software elements – Consideration is given to: – – any required software performance characteristics – – any required software interfaces – – any required security characteristics – – any database design requirements – – any required error handling and recovery attributes
17-03	System requirements	– System requirements include: functions and capabilities of the system; business, organizational and user requirements; safety, security, human-factors engineering (ergonomics), interface, operations, and maintenance requirements; design constraints and qualification requirements (ISO/IEC 12207) – Identifies the required system overview – Identifies any interrelationship considerations/constraints between system elements – Identifies any relationship considerations/constraints between the system elements and the software – Identifies any design considerations/constraints for each required system element, including: – – memory/capacity requirements – – hardware interfaces requirements – – user interfaces requirements – – external system interface requirements – – performance requirements – – commands structures – – security/data protection characteristics – – system parameter settings – – manual operations – – reusable components

18-00	Standard	– Identifies who/what they apply to – Expectations for conformance are identified – Conformance to requirements can be demonstrated – Provisions for tailoring or exception to the requirements are included

Table C.4 (10 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
19-00	Strategy	– Identifies what needs and objectives or goals there are to be satisfied – Establishes the options and approach for satisfying the needs, objectives, or goals – Establishes the evaluation criteria against which the strategic options are evaluated – Identifies any constraints/risks and how these will be addressed
20-00	Template	– Defines the attributes associated with a work product to be created as a consequence of a process execution – Identifies technical elements typically associated with this product type – Defines expected form and style
21-00	Work product	– Defines the attributes associated with an artefact from a process execution: – – key elements to be represented in the work product
22-00	Description	A description includes the following elements: a) Date of issue and status; b) Scope; c) Issuing organization; d) References; e) Context; f) Notation for description; g) Body; h) Summary; i) Glossary; j) Change history.
22-01	Release notes	Notes regarding a release. Purpose of Release Notes; Release Scope; Release Contents; Release Installation/Rollback Procedure; References.
23-00	Procedure	These documents shall include: g) documented procedures [and records] required by this standard
23-01	Configuration item control procedure	Configuration control procedures ensure that the integrity of services and service components is maintained. The CIs affected by new or changed services in the scope of Clause 5 are controlled by the configuration management process. The degree of control takes into consideration the service requirements and risks associated with the CIs. There is a procedure for recording, controlling and tracking versions of CIs.
23-02	Document management procedure	A procedure including authorities and responsibilities is established to define the controls needed: a) to create and approve documents prior to issue; b) to communicate to interested parties about new or changed documents; c) to review and maintain documents as necessary; d) to ensure that changes and the current revision status of documents are identified; e) to ensure that relevant versions of applicable documents are available at points of use; f) to ensure that documents are readily identifiable and legible; g) to ensure that documents of external origin are identified and their distribution controlled; h) to prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained.

23-03	Monitoring Procedure	The Responsible Organisation shall establish and maintain a process to monitor each installed Medical IT-Network for emerging risks, effectiveness of risk control measures, and accuracy of original estimations of RISK. Requirements for monitoring shall be established as part of the risk management plan of the Medical IT-Network. Examples of what to monitor are: a) environment changes (including local/connected environment as well as relevant network or component Data and systems security vulnerabilities); b) operational/performance feedback e.g., user feedback, speed problems, high error rates, failure, malicious software attacks; c) information about the incorporated components; d) information about similar Medical IT-Networks; e) reported events; and f) auditing of non-technical risk control measures such as organizational policies and procedures. If monitoring indicates actual or potential increase in risk associated with the Medical IT-Network or its components (potential or actual negative impact), the event management process shall be initiated and significant findings reported to the appropriate party in the responsible organisation. NOTE In some cases, the responsible organisation might be required to report observations to regulatory bodies.

Table C.4 (11 of 11) — Specific inputs and outputs

Ref:	Name:	Characteristics:
23-04	Event Management Procedure	The responsible organisation shall establish event management to: a) capture and document negative events; b) evaluate events and propose changes as appropriate through change release management; c) track all corrective and preventive actions leading to closure; and d) report significant finds to the Medical IT-Network risk manager and/or others in the responsible organisation.
24-00	Request	A request includes the following elements: a) Date of initiation; b) Scope; c) Subject; d) Originator of request; e) Identification of requested item, service, or response; f) Detailed description of requested item, service, or response, including due date; g) Justifications.
25-00	Specification	A specification shall include the following elements: a) Date of issue and status; b) Scope; c) Issuing organization; d) References; e) Approval authority; f) Body; g) Assurance requirements; h) Conditions, constraints, and characteristics; i) Glossary; j) Change history.

Annex D
(informative)

Abbreviations and Process Identifiers

D.1 Abbreviations

A list of abbreviations used in this document is provided below:

PRM	Process Reference Model
PAM	Process Assessment Model
HDO	Healthcare Delivery Organization
BP	Base Practice
WP	Work Product

D.2 Process Group

A list of Process Group Prefixes is provided below:

Process Group Prefixes:	**Process Group Name:**
MRM	Medical IT Network Risk Management Process Group
CRCM	Change Release Management & Configuration Management Process Group
LNRM	Live Network Monitoring Risk Management Process Group
MDP.1	Medical IT Network Documentation and Planning Process Group

D.3 Process IDs

A list of Process IDs is provided below:

Process ID:	**Process Name:**
MRM.1	Medical IT Network Risk Management Process
MRM.1.1	Risk Analysis and Evaluation Process
MRM.1.2	Risk Control Process
MRM.1.3	Residual Risk Process
CRCM.1	Change Release & Configuration Management Process
CRCM.2	Decision on how to apply Risk Management Process
CRCM.3	Go Live Process
LNRM.1	Monitoring Process
LNRM.2	Event Management Process
MDP.1	Medical IT Network Planning Process
MDP.2	Medical IT Network Documentation Process
MDP.3	Responsibility Agreements Process
MDP.4	Risk Management Policy Process
MDP.5	Organizational Risk Management Process

Bibliography

The following documents contain definitions and may provide general guidance to terms in the indicator set.

[1] ISO/IEC IS 12207:2008, Systems and software engineering — Software Life Cycle Processes

[2] ISO/IEC FDIS 15289:2011, Systems and software engineering — Content of systems and software life cycle process information products (Documentation)

[3] ISO/IEC 15504-5:2006, Information technology – Process assessment – Part 5: An exemplar Process Assessment Model

[4] ISO/IEC TR 15504-6:2008, Information technology -- Process assessment -- Part 6: An exemplar system life cycle process assessment model

[5] IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities

[6] IEC/TR 80001-2-1:2012 *Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples*

[7] IEC/TR 80001-2-2:2012 *Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

[8] IEC/TR 80001-2-3:2012 *Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks*

[9] IEC/TR 80001-2-4:2012 *Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations*

[10] ISO/IEC TR 24774:2010, Software and systems engineering – Life cycle management – Guidelines for process description