Technical Information Report

ANSI/AAMI/IEC 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

AVA Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC 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

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

Approved 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

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

Published by

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

© 2015 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

Publication, reproduction, photocopying, storage, or transmission, electronically or otherwise, of all or any part of this document without the prior written permission of the Association for the Advancement of Medical Instrumentation is strictly prohibited by law. It is illegal under federal law (17 U.S.C. § 101, *et seq*.) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violators risk legal action, including civil and criminal penalties, and damages of $100,000 per offense. For permission regarding the use of all or any part of this document, contact AAMI at 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633. Phone: (703) 525-4890; Fax: (703) 525-1067.

Printed in the United States of America

ISBN 1-57020-579-5

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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 Technical Report

This AAMI TIR has been registered by the American National Standards Institute as an ANSI Technical Report.

Publication of this ANSI Technical Report has been approved by the accredited standards developer (AAMI). This document is registered as a Technical Report series of publications according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standards 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.

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

Contents

Page

Glossary of equivalent standards v
Committee representation vi
Background of AAMI adoption of ISO TR 80001-2-7 Ed.1 vii
Foreword viii
Introduction ix
1 Scope 1
2 Normative References 1
3 Terms and Definitions 1
4 Assessment Method 2
4.1 Prerequisites 2
4.2 Assessment Method Overview 2
4.3 Assessment Stages 2
4.4 Process Attribute Rating Scale 4
4.5 Capability Levels 5
4.6 Tailoring the Assessment Method 5
Annex A (informative) Assessment Method 6
Annex B (informative) Process Reference Model 39
Annex C (informative) Process Assessment Model 53
Annex D (informative) Abbreviations and Process Identifiers 103
Bibliography 104

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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 (and ANSI) have 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.

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, ANSI/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.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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)

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

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

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC 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

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.

© 2015 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC TIR80001-2-7:2014

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

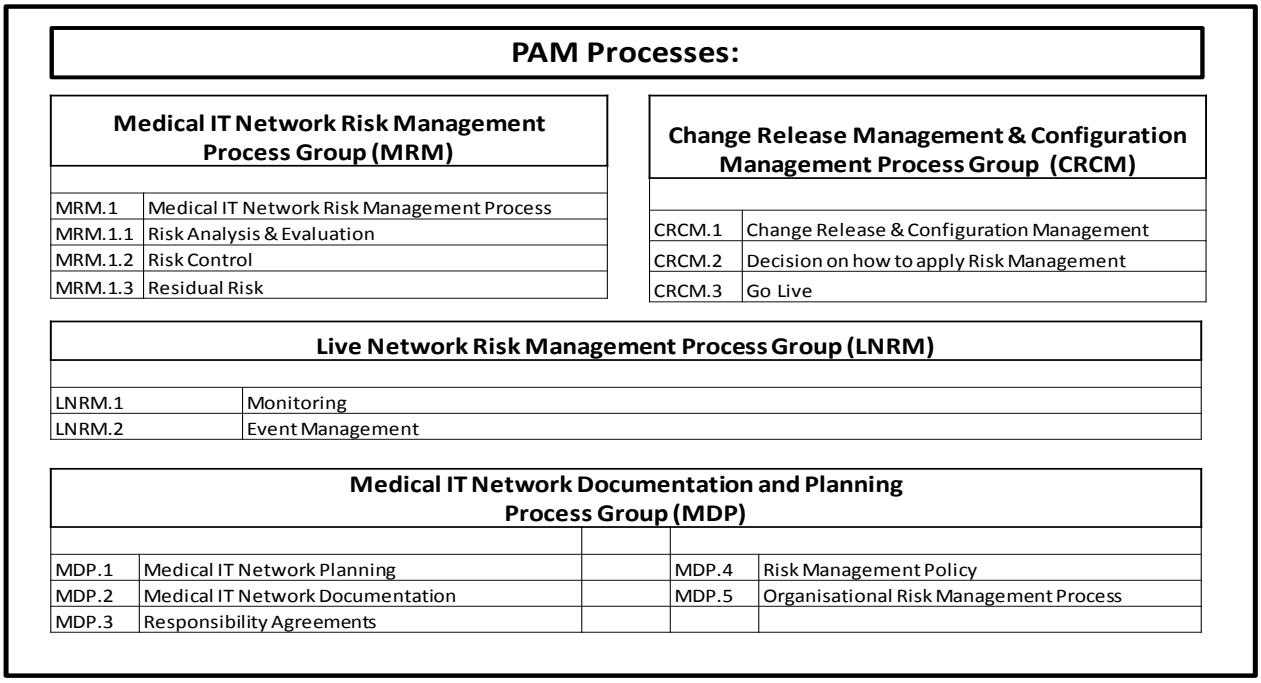

Figure 1 — PAM Processes – Assessment Method

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:

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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).

© 2015 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC TIR80001-2-7:2014
Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

© 2015 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC TIR80001-2-7:2014
Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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)

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.)

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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)

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80001-2-7-2014

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.

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80001-2-7-2014