Abstract: This helps a RESPONSIBLE ORGANIZATION through the key decisions and steps required to establish a RISK MANAGEMENT framework, before the organization embarks on a detailed RISK ASSESSMENT of an individual instance of a MEDICAL IT-NETWORK. This Technical Report is addressed to all Healthcare Delivery Organizations. A Healthcare Delivery Organization includes hospitals, doctors' offices, community care homes and clinics. It identifies a series of decision points to steer the RESPONSIBLE ORGANIZATION through the process of understanding the MEDICAL IT-NETWORK context and identifying any organizational changes required before undertaking the RISK MANAGEMENT PROCESS identified in IEC 80001-1.

Keywords: HDO, IT-networks, risk management
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that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years.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 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glossary of equivalent standards</td>
<td>v</td>
</tr>
<tr>
<td>Committee representation</td>
<td>vi</td>
</tr>
<tr>
<td>Background of AAMI adoption of IEC/TR 80001-2-4:2012</td>
<td>vii</td>
</tr>
<tr>
<td>FOREWORD</td>
<td>viii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>ix</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Purpose</td>
<td>1</td>
</tr>
<tr>
<td>1.2 HEALTHCARE DELIVERY ORGANIZATION</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Field of application</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Prerequisites</td>
<td>1</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>2</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>4 RESPONSIBLE ORGANIZATION</td>
<td>7</td>
</tr>
<tr>
<td>4.1 TOP MANAGEMENT responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>4.2 Small RESPONSIBLE ORGANIZATION – points to consider</td>
<td>7</td>
</tr>
<tr>
<td>4.3 Large RESPONSIBLE ORGANIZATION – points to consider</td>
<td>8</td>
</tr>
<tr>
<td>5 RISK MANAGEMENT implementation steps</td>
<td>8</td>
</tr>
<tr>
<td>5.1 Overview</td>
<td>8</td>
</tr>
<tr>
<td>5.2 Determine the clinical context within which the healthcare provision is made</td>
<td>9</td>
</tr>
<tr>
<td>5.3 Establish underlying risk framework</td>
<td>9</td>
</tr>
<tr>
<td>5.4 Determining and understanding a MEDICAL IT-NETWORK</td>
<td>10</td>
</tr>
<tr>
<td>5.4.1 Performing a RISK ASSESSMENT</td>
<td>10</td>
</tr>
<tr>
<td>5.4.2 MEDICAL IT-NETWORK configuration</td>
<td>10</td>
</tr>
<tr>
<td>5.4.3 Development status of MEDICAL IT-NETWORK</td>
<td>13</td>
</tr>
<tr>
<td>5.4.4 Manufacturer identification</td>
<td>13</td>
</tr>
<tr>
<td>5.4.5 External IT and bio-medical engineering support</td>
<td>14</td>
</tr>
<tr>
<td>6 RESPONSIBILITY AGREEMENTS</td>
<td>14</td>
</tr>
<tr>
<td>Annex A (informative) MEDICAL IT-NETWORK configuration examples</td>
<td>15</td>
</tr>
<tr>
<td>Bibliography</td>
<td>20</td>
</tr>
</tbody>
</table>

| Figure A.1 – Standalone MEDICAL IT-NETWORK outside the scope of IEC 80001-1 | 16   |
| Figure A.2 – Standalone MEDICAL IT-NETWORK                                 | 17   |
| Figure A.3 – Collaborative MEDICAL IT-NETWORK                              | 18   |
| Figure A.4 – Centralized MEDICAL IT-NETWORK                                | 19   |
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

Information Technology Working Group


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

**Cochairs:**
- William Hintz, Medtronic Inc. WHQ Campus
- Richard A. Schrenker, Massachusetts General Hospital

**Members:**
- John T. Collins, MSEE, American Society for Healthcare Engineering
- Todd Cooper, 80001 Experts (Independent Expert)
- Rebecca K. Crossley, CBET, Susquehanna Health System (Independent Expert)
- Conor Curtin, Fresenius Medical Care Renal Therapies Group
- Yadin David, EdD CCE PE HCSP, Biomedical Engineering Consultants LLC (Independent Expert)
- Karen S. Delvecchio, GE Healthcare
- Christina DeMur, Draeger Medical Systems Inc.
- Sherman Eagles, SoftwareCPR
- Donald J. Fournier, Draeger Medical Systems Inc.
- Kenneth J. Fluchs, Mindray DS USA Inc.
- George W. Gray, Fluidnet Corporation
- Thomas Grobaski, Belimed Inc.
- William Hintz, Medtronic Inc. WHQ Campus
- Yimin Li, Stryker Instruments Division
- Jared Mauldin, Integrated Medical Systems
- Mary Beth McDonald, STJude Medical Inc.
- Tresia L. O'Shea, Getinge USA
- Geoffrey A. Pascoe, MSCCS BEE GSEC, (Independent Expert)
- Steven R. Rakitin, Software Quality Consulting (Independent Expert)
- Terrie L. Reed, MSIE, FDA/CDRH
- Richard A. Schrenker, Massachusetts General Hospital
- Bob Steurer, Spacelabs Medical Inc.
- Donna-Bea Tillman, PhD, (Independent Expert)
- Daidi Zhong, PhD, Chongqing University (Independent Expert)

**Alternates:**
- James Dundon, Spacelabs Medical Inc.
- Brian J. Fitzgerald, Eur Ing MIMM, FDA/CDRH
- Thomas W. Schultz, Medtronic Inc. WHQ Campus
- Xianyu Shea, Stryker Instruments Division
- Fei Wang, Fresenius Medical Care Renal Therapies Group

**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 ANSI/AAMI adoption of IEC/TR 80001-2-4:2012

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

International technical report IEC/TR 80001-2-4:2012 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.


AAMI encourages its committees to harmonize their work with International Standards in the area of risk management of information technology as it relates to medical devices. The AAMI Information Technology Working Group together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC/TR 80001-2-4 to formulate the U.S. position and comments 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, AdvaMed granted AAMI permission to consider adoption of IEC/TR 80001-2-4 as a new AAMI Technical Information Report. Following AAMI procedures, the AAMI Information Technology Working Group voted to adopt the IEC technical report as written.

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

The concepts incorporated in this technical information 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 data comes to light.

As used within the context of this document, “should” indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action should be avoided but is not prohibited. “May” is used to indicate that a course of action is permissible within the limits of the technical information report. “Can” is used as a statement of possibility and capability. Finally, “must” is used only to describe “unavoidable” situations, including those mandated by government regulation.

Suggestions for improving this document are invited. Comments and suggested revisions should be sent to Standards Department, AAMI, 4301 N. Fairfax Dr. Suite 301, Arlington, VA 22203-1633.

NOTE: Beginning with the IEC foreword on page x, this AAMI Technical Information Report is identical to IEC/TR 80001-2-4:2012.
INTERNATIONAL ELECTROTECHNICAL COMMISSION

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-4: General implementation guidance for healthcare delivery organizations

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-4, which is a technical report, has been prepared by a Joint Working Group of subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice and ISO technical committee 215: Health informatics.

The text of this technical report is based on the following documents:
Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table. In ISO, the technical report has been approved by 15 P-members out of 16 having cast a vote.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

A list of all parts of the IEC 80001 series, published under the general title Application of risk management for IT-networks incorporating medical devices, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

• reconfirmed,
• withdrawn,
• replaced by a revised edition, or
• amended

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'color inside' logo on the cover page of this publication indicates that it contains colors which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a color printer.
INTRODUCTION

This technical report is a guide to help a HEALTHCARE DELIVERY ORGANIZATION (see 1.2) fulfilling its obligations as a RESPONSIBLE ORGANIZATION in the application of IEC 80001-1, in conjunction with other technical reports in this series. Specifically, this guide helps the HEALTHCARE DELIVERY ORGANIZATION assess the impact of the standard on the organization and establish a series of business as usual PROCESSES to manage RISK in the creation, maintenance and upkeep of its MEDICAL IT-NETWORKS. Whilst this document is aimed solely at HEALTHCARE DELIVERY ORGANIZATIONS, the term RESPONSIBLE ORGANIZATION is used throughout this document to ensure consistency with IEC 80001-1. In this respect the two terms are synonymous.

This technical report will be useful to those responsible for establishing an IEC 80001-1 compliant RISK MANAGEMENT framework within a RESPONSIBLE ORGANIZATION that is expecting to establish one or more MEDICAL IT-NETWORKS. In particular, the RISK MANAGEMENT framework should address the KEY PROPERTIES – SAFETY, DATA AND SYSTEM SECURITY and EFFECTIVENESS –as defined in IEC 80001-1. The purpose of the framework is to ensure that the potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, identified in IEC 80001-1, are avoided.

Defining and implementing the RISK MANAGEMENT framework and the business change that can result, will require the RESPONSIBLE ORGANIZATION to draw upon a range of skills from within the organization, managerial, clinical and technical. Where such skills are not available within the RESPONSIBLE ORGANIZATION, consideration should be given to collaboration with similar organizations or through experts in the field. It is important that the RESPONSIBLE ORGANIZATION be able to draw upon expertise with respect to appropriate standards and their corresponding technical reports.

In establishing a RISK MANAGEMENT framework, a RESPONSIBLE ORGANIZATION will need to take account of:

– the size and capabilities of the organization;
– the extent of its IT operations and the complexity of its current infrastructure and systems; and
– the cost of implementing IEC 80001-1.

It is expected that some of the above factors, for example size of IT operations and complexity of the networks, will be proportionate to the size of the organization. It is important that the framework itself does not create patient RISK by placing unnecessary demands on clinical staff, yet at the same time this workload should not introduce avoidable new RISKS when implementing a new technology.

In taking a RESPONSIBLE ORGANIZATION through the key decisions and steps required to successfully establish a RISK MANAGEMENT framework for MEDICAL IT-NETWORKS this document refers to small and large organizations. These are subjective terms, for which no precise measures are given, though:

• a small organization could be a doctor’s practice with:
  – a few clinicians, or
  – with many clinicians, a consolidated IT function and a highly centralized governance structure
• a large organization could be:
  – a multi-hospital conglomerate, or
  – an organization with distributed clinics and a mixture of in-house and outsourced clinical and IT governance.
Small organizations may also find the guidance identified under large organization relevant.

The RISK MANAGEMENT framework developed by a RESPONSIBLE ORGANIZATION following the guidance in this technical report needs to fit into the formal management systems that are routinely used for normal business: the business as usual PROCESSES. Such business as usual PROCESSES need to ensure RISK MANAGEMENT is part of the on-going requirement when systems are changed or new systems are deployed by:

- including the RISK MANAGEMENT PROCESSES in the existing management PROCESSES, for example the organization’s Quality Management System;
- ensuring that the internal audit schedule includes the RISK MANAGEMENT PROCESSES;
- making sure RISK MANAGEMENT training is included on induction of new staff and provided to existing staff; and
- ensuring RISK MANAGEMENT is undertaken for both new work and changes to existing MEDICAL IT-NETWORKS.

Having established a RISK MANAGEMENT framework, the RESPONSIBLE ORGANIZATION will be ready to undertake a detailed RISK ASSESSMENT (see IEC/TR 80001-2-1 [1]).
This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.
APPLICATION OF RISK MANAGEMENT FOR
IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-4: General implementation guidance
for healthcare delivery organizations

1 Scope

1.1 Purpose

This technical report helps a RESPONSIBLE ORGANIZATION through the key decisions and steps required to establish a RISK MANAGEMENT framework, before the organization embarks on a detailed RISK ASSESSMENT of an individual instance of a MEDICAL IT-NETWORK. The steps are supported by a series of decision points to steer the RESPONSIBLE ORGANIZATION through the PROCESS of understanding the MEDICAL IT-NETWORK context and identifying any organizational changes required to execute the responsibilities of TOP MANAGEMENT as defined in Figure 1 of IEC 80001-1:2010.

1.2 HEALTHCARE DELIVERY ORGANIZATION

This technical report is addressed to all HEALTHCARE DELIVERY ORGANIZATIONS. A HEALTHCARE DELIVERY ORGANIZATION includes hospitals, doctors’ offices, community care homes and clinics.

In the provision of a MEDICAL IT-NETWORK containing a MEDICAL DEVICE within a HEALTHCARE DELIVERY ORGANIZATION there can be a number of RESPONSIBLE ORGANIZATIONS. For the purpose of this document the focus is the HEALTHCARE DELIVERY ORGANIZATION and its obligations with respect to IEC 80001-1.

It is important for the HEALTHCARE DELIVERY ORGANIZATION to identify the RESPONSIBLE ORGANIZATION(S) responsible for any aspect of the network which is subject to IEC 80001-1. This allows a clear assignment of the roles and responsibilities of that standard.

1.3 Field of application

This technical report details the steps to be undertaken by the RESPONSIBLE ORGANIZATION in implementing the requirements of 3.1 to 3.3 and 4.1 to 4.6 of IEC 80001-1:2010.

NOTE It is assumed that the RESPONSIBLE ORGANIZATION will consider IEC/TR 80001-2-1 [1] for detailed advice in satisfying 4.4 of IEC 80001-1:2010.

1.4 Prerequisites

The International Standard IEC 80001-1:2010 is prerequisite to this technical report. The guidance in this technical report is intended to help a RESPONSIBLE ORGANIZATION establish a RISK MANAGEMENT framework to satisfy the underlying requirements of IEC 80001-1, ensuring:

- RISK MANAGEMENT policy and PROCESSES are in place;
– probability, severity, and risk acceptability scales are specified; and
– medical IT-networks are well defined.

2 Normative references

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