American National Standard

ANSI/AAMI/IEC 80001-1:2010

Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities

Association for the Advancement of Medical Instrumentation

Objectives and uses of AAMI standards and recommended practices

It is most important that the objectives and potential uses of an AAMI product standard or recommended practice are clearly understood. The objectives of AAMI's technical development program derive from AAMI's overall mission: the advancement of medical instrumentation. Essential to such advancement are (1) a continued increase in the safe and effective application of current technologies to patient care, and (2) the encouragement of new technologies. It is AAMI's view that standards and recommended practices can contribute significantly to the advancement of medical instrumentation, provided that they are drafted with attention to these objectives and provided that arbitrary and restrictive uses are avoided.

A voluntary *standard* for a *medical device* recommends to the manufacturer the information that should be provided with or on the product, basic safety and performance criteria that should be considered in qualifying the device for clinical use, and the measurement techniques that can be used to determine whether the device conforms with the safety and performance criteria and/or to compare the performance characteristics of different products. Some standards emphasize the information that should be provided with the device, including performance characteristics, instructions for use, warnings and precautions, and other data considered important in ensuring the safe and effective use of the device in the clinical environment. Recommending the disclosure of performance characteristics often necessitates the development of specialized test methods to facilitate uniformity in reporting; reaching consensus on these tests can represent a considerable part of committee work. When a drafting committee determines that clinical concerns warrant the establishment of *minimum* safety and performance criteria, referee tests must be provided and the reasons for establishing the criteria must be documented in the rationale.

A *recommended practice* provides guidelines for the use, care, and/or processing of a medical device or system. A recommended practice does not address device performance *per se*, but rather procedures and practices that will help ensure that a device is used safely and effectively and that its performance will be maintained.

Although a device standard is primarily directed to the manufacturer, it may also be of value to the potential purchaser or user of the device as a frame of reference for device evaluation. Similarly, even though a recommended practice is usually oriented towards healthcare professionals, it may be useful to the manufacturer in better understanding the environment in which a medical device will be used. Also, some recommended practices, while not addressing device performance criteria, provide guidelines to industrial personnel on such subjects as sterilization processing, methods of collecting data to establish safety and efficacy, human engineering, and other processing or evaluation techniques; such guidelines may be useful to health care professionals in understanding industrial practices.

In determining whether an AAMI standard or recommended practice is relevant to the specific needs of a potential user of the document, several important concepts must be recognized:

All AAMI standards and recommended practices are *voluntary* (unless, of course, they are adopted by government regulatory or procurement authorities). The application of a standard or recommended practice is solely within the discretion and professional judgment of the user of the document.

Each AAMI standard or recommended practice reflects the collective expertise of a committee of health care professionals and industrial representatives, whose work has been reviewed nationally (and sometimes internationally). As such, the consensus recommendations embodied in a standard or recommended practice are intended to respond to clinical needs and, ultimately, to help ensure patient safety. A standard or recommended practice is limited, however, in the sense that it responds generally to perceived risks and conditions that may not always be relevant to specific situations. A standard or recommended practice is an important *reference* in responsible decision-making, but it should never *replace* responsible decision-making.

Despite periodic review and revision (at least once every five years), a standard or recommended practice is necessarily a static document applied to a dynamic technology. Therefore, a standards user must carefully review the reasons why the document was initially developed and the specific rationale for each of its provisions. This review will reveal whether the document remains relevant to the specific needs of the user.

Particular care should be taken in applying a product standard to existing devices and equipment, and in applying a recommended practice to current procedures and practices. While observed or potential risks with existing equipment typically form the basis for the safety and performance criteria defined in a standard, professional judgment must be used in applying these criteria to existing equipment. No single source of information will serve to identify a particular product as "unsafe". A voluntary standard can be used as one resource, but the ultimate decision as to product safety and efficacy must take into account the specifics of its utilization and, of course, cost-benefit considerations. Similarly, a recommended practice should be analyzed in the context of the specific needs and resources of the individual institution or firm. Again, the rationale accompanying each AAMI standard and recommended practice is an excellent guide to the reasoning and data underlying its provision.

In summary, a standard or recommended practice is truly useful only when it is used in conjunction with other sources of information and policy guidance and in the context of professional experience and judgment.

INTERPRETATIONS OF AAMI STANDARDS AND RECOMMENDED PRACTICES

Requests for interpretations of AAMI standards and recommended practices must be made in writing, to the AAMI Vice President, Standards Policy and Programs. An official interpretation must be approved by letter ballot of the originating committee and subsequently reviewed and approved by the AAMI Standards Board. The interpretation will become official and representation of the Association only upon exhaustion of any appeals and upon publication of notice of interpretation in the "Standards Monitor" section of the *AAMI News*. The Association for the Advancement of Medical Instrumentation disclaims responsibility for any characterization or explanation of a standard or recommended practice which has not been developed and communicated in accordance with this procedure and which is not published, by appropriate notice, as an *official interpretation* in the *AAMI News*.

American National Standard **ANSI/AAMI/IEC 80001-1:2010**

Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities

Approved 14 October 2010 by
Association for the Advancement of Medical Instrumentation

Approved 6 October 2010 by
American National Standards Institute, Inc.

Abstract: This standard defines 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.

Keywords: medical device, risk management, information technology, interoperability

AAMI Standard

This Association for the Advancement of Medical Instrumentation (AAMI) standard implies a consensus of those substantially concerned with its scope and provisions. The existence of an AAMI standard does not in any respect preclude anyone, whether they have approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. AAMI standards are subject to periodic review, and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This AAMI standard may be revised or withdrawn at any time. AAMI procedures require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of publication. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI, or by visiting the AAMI website at www.aami.org.

All AAMI 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.

Published by

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

Printed in the United States of America

ISBN 1–57020–400-4

Contents

Glossary of equivalent standards

International Standards adopted in the United States may include normative references to other International Standards. For each International Standard that has been adopted by AAMI (and ANSI), the table below gives the corresponding U.S. designation and level of equivalency to the International Standard. NOTE: Documents are sorted by international designation. The code in the US column, "(R)20xx" indicates the year the document was officially reaffirmed by AAMI. E.g., ANSI/AAMI/ISO 10993-4:2002/(R)2009 indicates that 10993-4, originally approved and published in 2002, was reaffirmed without change in 2009.

Other normatively referenced International Standards may be under consideration for U.S. adoption by AAMI; therefore, this list should not be considered exhaustive.

International designation	U.S. designation	Equivalency
IEC 60601-1:2005 Technical Corrigendum 1 and 2	ANSI/AAMI ES60601-1:2005 and ANSI/AAMI ES60601-1:2005/A2:2010 ANSI/AAMI ES60601-1:2005/C1:2009 (amdt)	Major technical variations C1 Identical to Corrigendum 1 & 2
IEC 60601-1-2:2007	ANSI/AAMI/IEC 60601-1-2:2007	Identical
IEC 60601-2-2:2009	ANSI/AAMI/IEC 60601-2-2:2009	Identical
IEC 60601-2-4:2002	ANSI/AAMI DF80:2003/(R)2010	Major technical variations
IEC 60601-2-16:2008	ANSI/AAMI/IEC 60601-2-16:2008	Identical
IEC 60601-2-19:2009	ANSI/AAMI/IEC 60601-2-19:2009	Identical
IEC 60601-2-20:2009	ANSI/AAMI/IEC 60601-2-20:2009	Identical
IEC 60601-2-21:2009	ANSI/AAMI/IEC 60601-2-21:2009	Identical
IEC 60601-2-24:1998	ANSI/AAMI ID26:2004/(R)2009	Major technical variations
IEC 60601-2-47:2001	ANSI/AAMI EC38:2007	Major technical variations
IEC 60601-2-50:2009	ANSI/AAMI/IEC 60601-2-50:2009	Identical
IEC 80001-1:2010	ANSI/AAMI/IEC 80001-1:2010	Identical
IEC 80601-2-30:2009 and Technical Corrigendum 1	ANSI/AAMI/IEC 80601-2-30:2009 and ANSI/AAMI/IEC 80601-2-30:2009/ C1:2009 (amdt) – consolidated text	Identical (with inclusion) C1 Identical to Corrigendum 1
IEC 80601-2-58:2008	ANSI/AAMI/IEC 80601-2-58:2008	Identical
IEC/TR 60878:2009	ANSI/AAMI/IEC TIR60878:2003	Identical
IEC/TR 62296:2009	ANSI/AAMI/IEC TIR62296:2009	Identical
IEC 62304:2006	ANSI/AAMI/IEC 62304:2006	Identical
IEC/TR 62348:2006	ANSI/AAMI/IEC TIR62348:2006	Identical
IEC/TR 62354:2009	ANSI/AAMI/IEC TIR62354:2009	Identical
IEC 62366:2007	ANSI/AAMI/IEC 62377:2007	Identical
IEC/TR 80002-1:2009	ANSI/IEC/TR 80002-1:2009	Identical
ISO 5840:2005	ANSI/AAMI/ISO 5840:2005/(R)2010	Identical
ISO 7198:1998	ANSI/AAMI/ISO 7198:1998/2001/(R)2010	Identical
ISO 7199:2009	ANSI/AAMI/ISO 7199:2009	Identical
ISO 8637:2010	ANSI/AAMI/ISO 8637:2010	Identical
ISO 8638:2010	ANSI/AAMI/ISO 8638:2010	Identical
ISO 10993-1:2009	ANSI/AAMI/ISO 10993-1:2009	Identical
ISO 10993-2:2006	ANSI/AAMI/ISO 10993-2:2006	Identical
ISO 10993-3:2003	ANSI/AAMI/ISO 10993-3:2003/(R)2009	Identical
ISO 10993-4:2002 and Amendment 1:2006	ANSI/AAMI/ISO 10993-4:2002/(R)2009 and Amendment 1:2006/(R)2009	Identical
ISO 10993-5:2009	ANSI/AAMI/ISO 10993-5:2009	Identical
ISO 10993-6:2007	ANSI/AAMI/ISO 10993-6:2007	Identical
ISO 10993-7:2008	ANSI/AAMI/ISO 10993-7:2008	Identical
ISO 10993-9:2009	ANSI/AAMI/ISO 10993-9:2009	Identical
ISO 10993-10:2010	ANSI/AAMI/ISO 10993-10:2010	Identical
ISO 10993-11:2006	ANSI/AAMI/ISO 10993-11:2006	Identical
ISO 10993-12:2007	ANSI/AAMI/ISO 10993-12:2007	Identical
ISO 10993-13:2010	ANSI/AAMI/ISO 10993-13:2010	Identical
ISO 10993-14:2001	ANSI/AAMI/ISO 10993-14:2001/(R)2006	Identical
ISO 10993-15:2000	ANSI/AAMI/ISO 10993-15:2000/(R)2006	Identical
ISO 10993-16:2010	ANSI/AAMI/ISO 10993-16:2010	Identical
ISO 10993-17:2002	ANSI/AAMI/ISO 10993-17:2002/(R)2008	Identical
ISO 10993-18:2005	ANSI/AAMI BE83:2006	Major technical variations
ISO/TS 10993-19:2006	ANSI/AAMI/ISO TIR10993-19:2006	Identical

International designation	U.S. designation	Equivalency
ISO/TS 10993-20:2006	ANSI/AAMI/ISO TIR10993-20:2006	Identical
ISO 11135-1:2007	ANSI/AAMI/ISO 11135-1:2007	Identical
ISO/TS 11135-2:2008	ANSI/AAMI/ISO TIR11135-2:2008	Identical
ISO 11137-1:2006	ANSI/AAMI/ISO 11137-1:2006/(R)2010	Identical
ISO 11137-2:2006 (2006-08-01 corrected version)	ANSI/AAMI/ISO 11137-2:2006	Identical
ISO 11137-3:2006	ANSI/AAMI/ISO 11137-3:2006/(R)2010	Identical
ISO 11138-1: 2006	ANSI/AAMI/ISO 11138-1:2006/(R)2010	Identical
ISO 11138-2: 2006	ANSI/AAMI/ISO 11138-2:2006/(R)2010	Identical
ISO 11138-3: 2006	ANSI/AAMI/ISO 11138-3:2006/(R)2010	Identical
ISO 11138-4: 2006	ANSI/AAMI/ISO 11138-4:2006/(R)2010	Identical
ISO 11138-5: 2006	ANSI/AAMI/ISO 11138-5:2006/(R)2010	Identical
ISO/TS 11139:2006	ANSI/AAMI/ISO 11139:2006	Identical
ISO 11140-1:2005	ANSI/AAMI/ISO 11140-1:2005/(R)2010	Identical
ISO 11140-3:2007	ANSI/AAMI/ISO 11140-3:2007	Identical
ISO 11140-4:2007	ANSI/AAMI/ISO 11140-4:2007	Identical
ISO 11140-5:2007	ANSI/AAMI/ISO 11140-5:2007	Identical
ISO 11607-1:2006	ANSI/AAMI/ISO 11607-1:2006	Identical
ISO 11607-2:2006	ANSI/AAMI/ISO 11607-2:2006	Identical
ISO 11663:2009	ANSI/AAMI/ISO 11633:2009	Identical
ISO 11737-1: 2006	ANSI/AAMI/ISO 11737-1:2006	Identical
ISO 11737-2:2009	ANSI/AAMI/ISO 11737-2:2009	Identical
ISO 13408-1:2008	ANSI/AAMI/ISO 13408-1:2008	Identical
ISO 13408-2:2003	ANSI/AAMI/ISO 13408-2:2003	Identical
ISO 13408-3:2006	ANSI/AAMI/ISO 13408-3:2006	Identical
ISO 13408-4:2005	ANSI/AAMI/ISO 13408-4:2005	Identical
ISO 13408-5:2006	ANSI/AAMI/ISO 13408-5:2006	Identical
ISO 13408-6:2006	ANSI/AAMI/ISO 13408-6:2006	Identical
ISO 13485:2003	ANSI/AAMI/ISO 13485:2003/(R)2009	Identical
ISO 14155-1:2003	ANSI/AAMI/ISO 14155-1:2003/(R)2008	Identical
ISO 14155-2:2003	ANSI/AAMI/ISO 14155-2:2003/(R)2008	Identical
ISO 14160:1998	ANSI/AAMI/ISO 14160:1998/(R)2008	Identical
ISO 14161:2009	ANSI/AAMI/ISO 14161:2009	Identical
ISO 14708-3:2008	ANSI/AAMI/ISO 14708-3:2008	Identical
ISO 14708-4:2008	ANSI/AAMI/ISO 14708-4:2008	Identical
ISO 14708-5:2010	ANSI/AAMI /ISO 14708-5:2010	Identical
ISO 14937:2009	ANSI/AAMI/ISO 14937:2009	Identical
ISO/TR 14969:2004	ANSI/AAMI/ISO TIR14969:2004	Identical
ISO 14971:2007	ANSI/AAMI/ISO 14971:2007/(R)2010	Identical
ISO 15223-1:2007 and A1:2008	ANSI/AAMI/ISO 15223-1:2007 and A1:2008	Identical
ISO 15223-2:2010	ANSI/AAMI/ISO 15223-2:2010	Identical
ISO 15225:2010	ANSI/AAMI/ISO 15225:2010	Identical
ISO 15674:2009	ANSI/AAMI/ISO 15674:2009	Identical
ISO 15675:2009	ANSI/AAMI/ISO 15675:2009	Identical
ISO 15882:2008	ANSI/AAMI/ISO 15882:2008	Identical
ISO 15883-1:2006	ANSI/AAMI ST15883-1:2009	Major technical variations
ISO/TR 16142:2006	ANSI/AAMI/ISO TIR16142:2005	Identical
ISO 17664:2004	ANSI/AAMI ST81:2004	Major technical variations
ISO 17665-1:2006	ANSI/AAMI/ISO 17665-1:2006	Identical (with inclusions)
ISO/TS 17665-2:2009	ANSI/AAMI/ISO TIR17665-2:2009	Identical
ISO 18472:2006	ANSI/AAMI/ISO 18472:2006	Identical
ISO/TS 19218:2005	ANSI/AAMI/ISO 19218:2005	Identical
ISO 22442-1:2007	ANSI/AAMI/ISO 22442-1:2007	Identical
ISO 22442-2:2007	ANSI/AAMI/ISO 22442-2:2007	Identical
ISO 22442-3:2007	ANSI/AAMI/ISO 22442-3:2007	Identical
ISO 25539-1:2003 and A1:2005	ANSI/AAMI/ISO 25539-1:2003/(R)2009 and A1:2005/(R)2009	Identical
ISO 25539-2:2008	ANSI/AAMI/ISO 25539-2:2008	Identical
ISO 27186:2010	ANSI/AAMI/ISO 27186:2010	Identical
ISO 81060-1:2007	ANSI/AAMI/ISO 81060-1:2007	Identical
ISO 81060-2:2009	ANSI/AAMI/ISO 81060-2:2009	Identical

Committee representation

Association for the Advancement of Medical Instrumentation

Information Technology Networks Incorporating Medical Devices Committee

The adoption of IEC 80001-1 as a new American National Standard was initiated by the AAMI Information Technology Networks Incorporating Medical Devices (IT) Committee. U.S. cochairs of the AAMI IT Committee, William Hintz of Medtronic Inc and Richard Schrenker of Massachusettes General Hospital, played an active part in developing the IEC standard.

Committee approval of this document does not necessarily imply that all committee members voted for its approval.

At the time this document was published, the **AAMI Information Technology Networks Incorporating Medical Devices Committee** had the following members:

Cochairs

William Hintz, Medtronic Inc.
Richard A. Schrenker, Massachusetts General Hospital (Independent Expert)

Members

Jon Camp, Philips Electronics North America
Todd Cooper, (Independent Expert)
Leanne Cordisco, GE Healthcare
Rebecca K. Crossley, CBET, (Independent Expert)
Conor Curtin, Fresenius Medical Care Renal Therapies Group
Yadin David, EdD CCE PE HCSP, (Independent Expert)
Christina DeMur, Draeger Medical Systems Inc.
Sherman Eagles, SoftwareCPR
Joseph Freitas, CareFusion
Kenneth J. Fuchs, Mindray DS USA Inc.
William Hintz, Medtronic Inc
Yimin Li, Stryker Instruments Division
Marshall Magee, Welch Allyn Inc.
Mary Beth McDonald, St Jude Medical Inc.
Sean Murphy, Lt Col, Air Force Medical Operations Agency SGALE (Independent Expert)
Kenneth Olbrish, (Independent Expert)
Tresia L. O'Shea, Getinge USA
Steven R. Rakitin, (Independent Expert)
Terrie L. Reed, FDA/CDRH
Richard A. Schrenker, Massachusetts General Hospital (Independent Expert)
Rabin Srestha, Spacelabs Medical Inc.
Micheal T. Suelzer, PhD, Baxter Healthcare Corporation
Donna-Bea Tillman, PhD, Microsoft Health Soutions Group

Alternates

Karen S. Delvecchio, GE Healthcare
Brian J. Fitzgerald, Eur Ing MIMM, FDA/CDRH
Xianyu Shea, Stryker Instruments Division
Thomas W. Schultz, Medtronic Inc.
Fei Wang, Fresenius Medical Care

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

Background of ANSI/AAMI adoption of IEC 80001-1:2010

As indicated in the foreword to the main body of this document (page ix), 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 standard.

International standard IEC 80001-1:2010 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 the Advanced Medical Technology Association (AdvaMed) on behalf of the American National Standards Institute. AAMI administers the International Secretariat for IEC/SC 62A on behalf of the United States, and U.S. experts made a considerable contribution to this International Standard.

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 Networks Incorporating Medical Devices (IT) Committee together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC 80001-1 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 80001-1 as a new American national Standard. Following AAMI procedures, the AAMI IT Committee voted to adopt the IEC international standard as written.

AAMI and ANSI procedures require that standards be reviewed every five years and, if necessary, revised to reflect technological advances that may have occurred since publication.

AAMI (and ANSI) have adopted other IEC and ISO standards. 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 standard should not be considered inflexible or static. This standard, 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.

Suggestions for improving this standard 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 foreword on page ix, this American National Standard is identical to IEC 80001-1:2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Roles, responsibilities and activities

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 co-operation 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.

International Standard IEC 80001-1 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.

It is published as a double logo standard.

The text of this standard is based on the following documents:

FDIS	Report on voting
62A/703/FDIS	62A/718/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 17 P-members out of 18 having cast a vote.

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

Terms defined in Clause 2 of this standard are printed in SMALL CAPITALS.

For the purposes of this standard:

- "shall" means that compliance with a requirement is mandatory for compliance with this standard;
- "should" means that compliance with a requirement is recommended but is not mandatory for compliance with this standard;
- "may" is used to describe a permissible way to achieve compliance with a requirement; and
- "establish" means to define, document, and implement.

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 web site 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.

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

An increasing number of MEDICAL DEVICEs are designed to exchange information electronically with other equipment in the user environment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature.

At the same time, IT-NETWORKS are becoming increasingly vital to the clinical environment and are now required to carry increasingly diverse traffic, ranging from life-critical patient data requiring immediate delivery and response, to general corporate operations data and to email containing potential malicious content (e.g. viruses).

For many jurisdictions, design and production of MEDICAL DEVICES is subject to regulation, and to standards recognized by the regulators. Traditionally, regulators direct their attention to MEDICAL DEVICE manufacturers, by requiring design features and by requiring a documented PROCESS for design and manufacturing. MEDICAL DEVICES cannot be placed on the market in these jurisdictions without evidence that those requirements have been met.

The use of the MEDICAL DEVICES by clinical staff is also subject to regulation. Members of clinical staff have to be appropriately trained and qualified, and are increasingly subject to defined PROCESSES designed to protect patients from unacceptable RISK.

In contrast, the incorporation of MEDICAL DEVICES into IT-NETWORKS in the clinical environment is a less regulated area. IEC 60601-1:2005 [1][1)] requires MEDICAL DEVICE manufacturers to include some information in ACCOMPANYING DOCUMENTS if the MEDICAL DEVICE is intended to be connected to an IT-NETWORK. Standards are also in place covering common information technology activities including planning, design and maintenance of IT-NETWORKS, for instance ISO 20000-1:2005 [9]. However, until the publication of this standard, no standard addressed how MEDICAL DEVICES can be connected to IT-NETWORKS, including general-purpose IT-NETWORKS, to achieve INTEROPERABILITY without compromising the organization and delivery of health care in terms of SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY.

There remain a number of potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, including:

– lack of consideration for RISK from use of IT-NETWORKS during evaluation of clinical RISK;
– lack of support from manufacturers of MEDICAL DEVICES for the incorporation of their products into IT-NETWORKS, (e.g. the unavailability or inadequacy of information provided by the manufacturer to the OPERATOR of the IT-NETWORK);
– incorrect operation or degraded performance (e.g. incompatibility or improper configuration) resulting from combining MEDICAL DEVICES and other equipment on the same IT-NETWORK;
– incorrect operation resulting from combining MEDICAL DEVICE SOFTWARE and other software applications (e.g. open email systems or computer games) in the same IT-NETWORK;
– lack of security controls on many MEDICAL DEVICES; and
– the conflict between the need for strict change control of MEDICAL DEVICES and the need for rapid response to the threat of cyberattack.

When these problems manifest themselves, unintended consequences frequently follow.

---

1) Numbers in square brackets refer to the Bibliography.

This standard is addressed to RESPONSIBLE ORGANIZATIONS, to manufacturers of MEDICAL DEVICES, and to providers of other information technology.

This standard adopts the following principles as a basis for its normative and informative sections:

– The incorporation or removal of a MEDICAL DEVICE or other components in an IT-NETWORK is a task which requires design of the action; this might be out of the control of the manufacturer of the MEDICAL DEVICE.

– RISK MANAGEMENT should be used before the incorporation of a MEDICAL DEVICE into an IT-NETWORK takes place, and for any changes during the entire life cycle of the resulting MEDICAL IT-NETWORK, to avoid unacceptable RISKS, including possible RISK to patients, resulting from the incorporation of the MEDICAL DEVICE into the IT-NETWORK. Many things are part of a RISK decision, such as liability, cost, or impact on mission. These should be considered in determining acceptable RISK in addition to the requirements described in this standard.

– Aspects of removal, maintenance, change or modification of equipment, items or components should be addressed adequately in addition to the incorporation of MEDICAL DEVICES.

– The manufacturer of the MEDICAL DEVICE is responsible for RISK MANAGEMENT of the MEDICAL DEVICE during the design, implementation, and manufacturing of the MEDICAL DEVICE. This standard does not cover the RISK MANAGEMENT PROCESS for the MEDICAL DEVICE.

– The manufacturer of a MEDICAL DEVICE intended to be incorporated into an IT-NETWORK might need to provide information about the MEDICAL DEVICE that is necessary to allow the RESPONSIBLE ORGANIZATION to manage RISK according to this standard. This information can include, as part of the ACCOMPANYING DOCUMENTS, instructions specifically addressed to the person who incorporates a MEDICAL DEVICE into an IT-NETWORK.

– Such ACCOMPANYING DOCUMENTS should convey instructions about how to incorporate the MEDICAL DEVICE into the IT-NETWORK, how the MEDICAL DEVICE transfers information over the IT-NETWORK, and the minimum IT-NETWORK characteristics necessary to enable the INTENDED USE of the MEDICAL DEVICE when it is incorporated into the IT-NETWORK. The ACCOMPANYING DOCUMENTS should warn of possible hazardous situations associated with failure or disruptions of the IT-NETWORK, and the misuse of the IT-NETWORK connection or of the information that is transferred over the IT-NETWORK.

– RESPONSIBILITY AGREEMENTS can establish roles and responsibilities among those engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK, all aspects of the life cycle of the resulting MEDICAL IT-NETWORK and all activities that form part of that life cycle.

– The RESPONSIBLE ORGANIZATION is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of those roles. The most important of those roles is the MEDICAL IT-NETWORK RISK MANAGER. This role can be assigned to someone within the RESPONSIBLE ORGANIZATION or to an external contractor.

– The MEDICAL IT-NETWORK RISK MANAGER is responsible for ensuring that RISK MANAGEMENT is included during the PROCESSES of:

  - planning and design of new incorporations of MEDICAL DEVICES or changes to such incorporations;
  - putting the MEDICAL IT-NETWORK into use and the consequent use of the MEDICAL IT-NETWORK; and
  - CHANGE-RELEASE MANAGEMENT and change management of the IT-NETWORK during the IT-NETWORK'S entire life cycle.

– RISK MANAGEMENT should be applied to address the following KEY PROPERTIES appropriate for the IT-NETWORK incorporating a MEDICAL DEVICE:

  - SAFETY (freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment);
  - EFFECTIVENESS (ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION); and
  - DATA AND SYSTEM SECURITY (an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability).

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

Part 1: Roles, responsibilities and activities

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines 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 (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.

This standard applies where there is no single MEDICAL DEVICE manufacturer assuming responsibility for addressing the KEY PROPERTIES of the IT-NETWORK incorporating a MEDICAL DEVICE.

NOTE 4 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, the installation or assembly of the MEDICAL DEVICE according to the manufacturer's ACCOMPANYING DOCUMENTS is not subject to the provisions of this standard regardless of who installs or assembles the MEDICAL DEVICE.

NOTE 5 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, additions to that MEDICAL DEVICE or modification of the configuration of that MEDICAL DEVICE, other than as specified by the manufacturer, is subject to the provisions of this standard.

This standard applies to RESPONSIBLE ORGANIZATIONS, MEDICAL DEVICE manufacturers and providers of other information technology for the purpose of RISK MANAGEMENT of an IT-NETWORK incorporating MEDICAL DEVICES as specified by the RESPONSIBLE ORGANIZATION.

This standard does not apply to personal use applications where the patient, OPERATOR and RESPONSIBLE ORGANIZATION are one and the same person.

NOTE 6 In cases where a MEDICAL DEVICE is used at home under the supervision or instruction of the provider, that provider is deemed to be the RESPONSIBLE ORGANIZATION. Personal use where the patient acquires and uses a MEDICAL DEVICE without the supervision or instruction of a provider is out of scope of this standard.

This standard does not address regulatory or legal requirements.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

2.1
ACCOMPANYING DOCUMENT
a document accompanying a MEDICAL DEVICE or an accessory and containing information for the RESPONSIBLE ORGANIZATION or OPERATOR, particularly regarding SAFETY

NOTE Adapted from IEC 60601-1:2005, definition 3.4.

2.2
CHANGE-RELEASE MANAGEMENT
PROCESS that ensures that all changes to the IT-NETWORK are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with CONFIGURATION MANAGEMENT

NOTE Adapted from ISO/IEC 20000-1:2005, Subclauses 9.2 (change management) and 10.1 (release management).

2.3
CHANGE PERMIT
an outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT Activities subject to specified constraints

2.4
CONFIGURATION MANAGEMENT
a PROCESS that ensures that configuration information of components and the IT-NETWORK are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the IT-NETWORK

NOTE Adapted from ISO/IEC 20000-1:2005, Subclause 9.1.

2.5
DATA AND SYSTEMS SECURITY
an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

NOTE 1 Security, when mentioned in this standard, should be taken to include DATA AND SYSTEMS SECURITY.

NOTE 2 DATA AND SYSTEMS SECURITY is assured through a framework of policy, guidance, infrastructure, and services designed to protect information assets and the systems that acquire, transmit, store, and use information in pursuit of the organization's mission.

2.6
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

2.7
EVENT MANAGEMENT
a PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

NOTE Adapted from ISO/IEC 20000-1:2005, Subclauses 8.2 (incident management) and 8.3 (problem management).

2.8
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY

NOTE Adapted from ISO 14971:2007, definition 2.2.

2.9
HAZARD
potential source of HARM

[ISO 14971:2007, definition 2.3]

2.10
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

[ISO 14971: 2007, definition 2.5]

2.11
INTEROPERABILITY
a property permitting diverse systems or components to work together for a specified purpose

2.12
IT-NETWORK (INFORMATION TECHNOLOGY NETWORK)
a system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

NOTE 1 Adapted from IEC 61907:2009, definition 3.1.1.

NOTE 2 The scope of the MEDICAL IT-NETWORK in this standard is defined by the RESPONSIBLE ORGANIZATION based on where the MEDICAL DEVICES in the MEDICAL IT-NETWORK are located and the defined use of the network. It can contain IT infrastructure, home health and non-clinical contexts. See also 4.3.3.

2.13
KEY PROPERTIES
three risk managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

2.14
MEDICAL DEVICE
means any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
   – diagnosis, prevention, monitoring, treatment or alleviation of disease,
   – diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
   – investigation, replacement, modification, or support of the anatomy or of a physiological process,
   – supporting or sustaining life,

– control of conception,

– disinfection of medical devices,

– providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

NOTE 1 The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

NOTE 2 Products which may be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

– aids for disabled/handicapped people;
– devices for the treatment/diagnosis of diseases and injuries in animals;
– accessories for medical devices (see Note 3);
– disinfection substances;
– devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

NOTE 3 Accessories intended specifically by manufacturers to be used together with a 'parent' medical device to enable that medical device to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the 'parent' device.

NOTE 4 Components to medical devices are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[GHTF SG1/N29R16:2005]

2.15
MEDICAL DEVICE SOFTWARE
software system that has been developed for the purpose of being incorporated into the MEDICAL DEVICE or that is intended for use as a MEDICAL DEVICE in its own right

[IEC 62304:2006, definition 3.12, modified]

2.16
MEDICAL IT-NETWORK
an IT-NETWORK that incorporates at least one MEDICAL DEVICE

2.17
MEDICAL IT-NETWORK RISK MANAGER
person accountable for RISK MANAGEMENT of a MEDICAL IT-NETWORK

2.18
OPERATOR
person handling equipment

[IEC 60601-1:2005, definition 3.73]

2.19
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 14971:2007, definition 2.13]

NOTE The term “activities” covers use of resources.

2.20
RESIDUAL RISK
RISK remaining after RISK CONTROL measures have been taken

[ISO 14971:2007, definition 2.15]

2.21
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

NOTE This agreement can be a legal document, e.g. a contract.

2.22
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

NOTE 1 The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

NOTE 2 Adapted from IEC 60601-1:2005 definition 3.101.

2.23
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[ISO 14971:2007, definition 2.16]

2.24
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[ISO 14971:2007, definition 2.17]

2.25
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[ISO/IEC Guide 51:1999, definition 3.12]

2.26
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[ISO 14971:2007, definition 2.19]

2.27
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[ISO 14971:2007, definition 2.21]

2.28
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

[ISO 14971:2007, definition 2.22]

2.29
RISK MANAGEMENT FILE
set of records and other documents that are produced by RISK MANAGEMENT

[ISO 14971:2007, definition 2.23]

2.30
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

NOTE Adapted from ISO 14971:2007, definition 2.24.

2.31
TOP MANAGEMENT
person or group of people who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level

NOTE Adapted from ISO 9000:2005, definition 3.2.7.

2.32
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

NOTE 1 The term “verified” is used to designate the corresponding status.

NOTE 2 Confirmation can comprise activities such as:

– performing alternative calculations;
– comparing a new design specification with a similar proven design specification;
– undertaking tests and demonstrations; and
– reviewing documents prior to issue.

[ISO 14971:2007, definition 2.28]

NOTE 3 In design and development, VERIFICATION concerns the PROCESS of examining the result of a given activity to determine conformity with the stated requirement for that activity.

3 Roles and responsibilities

3.1 General

Incorporation and modification of equipment or software of a MEDICAL IT-NETWORK shall be performed under a framework of clearly defined responsibilities. At a minimum, the parties, responsibilities and requirements identified in subclauses 3.2 through 3.6 shall be defined.

For the particular MEDICAL IT-NETWORK being considered, the RESPONSIBLE ORGANIZATION shall establish and maintain a MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

All documentation related to the requirements of this standard for RESPONSIBLE ORGANIZATIONS as well as all supporting documentation shall be maintained in a MEDICAL IT-NETWORK RISK MANAGEMENT FILE. This file shall contain the current CONFIGURATION MANAGEMENT information for the MEDICAL IT-NETWORK.

NOTE 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.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

3.2 RESPONSIBLE ORGANIZATION

The overall responsibility for RISK MANAGEMENT for a MEDICAL IT-NETWORK shall stay within the RESPONSIBLE ORGANIZATION.

The RESPONSIBLE ORGANIZATION shall be the owner of the RISK MANAGEMENT PROCESS for the MEDICAL IT-NETWORK, spanning planning, design, installation, device connection, configuration, use/operation, maintenance, and device decommissioning.

Compliance is checked by assessment of the RESPONSIBLE ORGANIZATION.

3.3 TOP MANAGEMENT responsibilities

For RISK MANAGEMENT of MEDICAL IT-NETWORKS, TOP MANAGEMENT shall be accountable for:

a) establishing a policy for RISK MANAGEMENT for incorporating MEDICAL DEVICES;

b) defining the policy for determining acceptable RISK, taking into account relevant international standards and national or regional regulations;

c) ensuring the provision of adequate resources;

d) ensuring the assignment of qualified personnel for management, performance of work and assessment activities; and

e) reviewing the results of RISK MANAGEMENT activities, including EVENT MANAGEMENT (see 4.6.2), at defined intervals to ensure the continuing suitability and the effectiveness of the RISK MANAGEMENT PROCESS.

The above shall be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

TOP MANAGEMENT shall appoint a MEDICAL IT-NETWORK RISK MANAGER, who has the necessary qualifications, knowledge and competence for RISK MANAGEMENT applied to MEDICAL IT-NETWORKS (see 3.4).

TOP MANAGEMENT shall identify the people responsible for the following tasks and ensure that they co-operate with the MEDICAL IT-NETWORK RISK MANAGER:

f) gathering, analysis, assessment and storage of information needed for RISK MANAGEMENT;

g) lifecycle management of MEDICAL DEVICES incorporated in IT-NETWORKS;

h) reviewing and accepting RESIDUAL RISK on behalf of TOP MANAGEMENT;

i) maintenance of MEDICAL IT-NETWORKS; and

j) choice of and procurement of MEDICAL DEVICES.

TOP MANAGEMENT shall ensure that participation in the RISK MANAGEMENT PROCESS for MEDICAL IT-NETWORKS includes management responsible for:

k) MEDICAL IT-NETWORKS;

l) general IT activities;

m) life-cycle management of MEDICAL DEVICES connected to IT-NETWORKS;

EXAMPLE biomedical engineering, radiological engineering

n) the use of MEDICAL DEVICES; and

EXAMPLE experienced users from clinical departments

o) maintenance and technical support for MEDICAL DEVICES.

EXAMPLE biomedical engineering department

TOP MANAGEMENT shall ensure:

p) that all supervision, operation, installation and maintenance of MEDICAL IT-NETWORK(S) throughout the life cycle is made according to the RISK MANAGEMENT plan and follows the results of the IT-NETWORK RISK MANAGEMENT PROCESS, whoever performs these tasks;

q) that all parties performing supervision, operation, installation, service, troubleshooting and maintenance of MEDICAL IT-NETWORK(S) are adequately informed about their responsibility according to this standard, including their responsibility for maintaining the effectiveness of RISK CONTROLS.

NOTE The TOP MANAGEMENT responsibilities are illustrated in Figure 1.

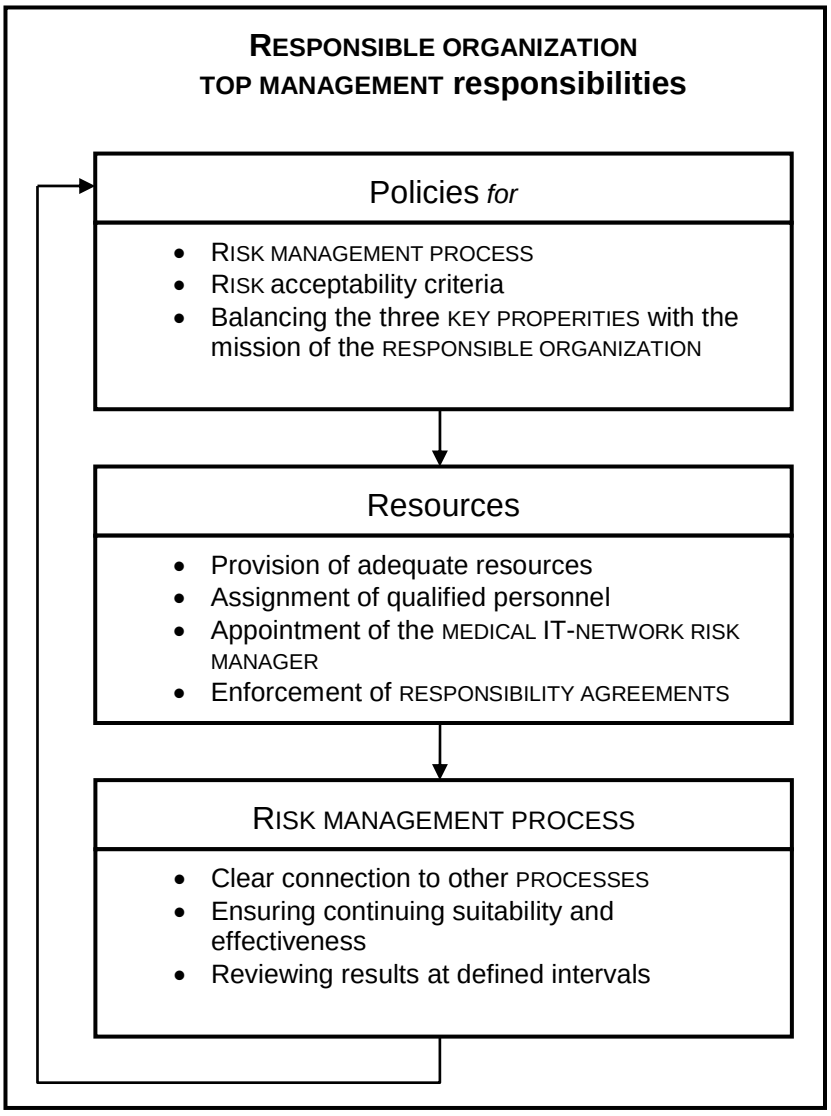


Figure 1 – Illustration of TOP MANAGEMENT responsibilities

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

3.4 MEDICAL IT-NETWORK RISK MANAGER

The MEDICAL IT-NETWORK RISK MANAGER shall be responsible for the management of the RISK MANAGEMENT PROCESS.

The MEDICAL IT-NETWORK RISK MANAGER shall supervise the execution of the RISK MANAGEMENT PROCESS to maintain the KEY PROPERTIES of the MEDICAL IT-NETWORK.

The MEDICAL IT-NETWORK RISK MANAGER shall be responsible for the following aspects of the RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES:

a) Overall management of the RISK MANAGEMENT PROCESS;

b) reporting on the RISK MANAGEMENT PROCESS to the TOP MANAGEMENT; and

c) managing the necessary communication between the internal and external participants in RISK MANAGEMENT. Such participants may include, as appropriate:

   1) MEDICAL DEVICE manufacturers;

   2) other suppliers of IT equipment, software and services;

   3) internal IT function and other facilities management functions;

   4) clinical users; and

   5) technical support function responsible for MEDICAL DEVICES (for example biomedical engineering).

The MEDICAL IT-NETWORK RISK MANAGER shall be responsible for the performance of the RISK MANAGEMENT PROCESS. This includes but is not limited to responsibility for:

d) collection of all RISK-relevant information on the MEDICAL DEVICES;

e) planning the incorporation of the MEDICAL DEVICES in accordance with the instructions provided by the various MEDICAL DEVICE manufacturers and the policies of the RESPONSIBLE ORGANIZATION;

f) the performance of the RISK MANAGEMENT PROCESS whenever a MEDICAL DEVICE is added to an IT-NETWORK;

g) the performance of the RISK MANAGEMENT PROCESS whenever an incorporated MEDICAL DEVICE or the MEDICAL IT-NETWORK is changed;

h) authorization to proceed with go-live following a change to the MEDICAL IT-NETWORK;

i) informing the RESPONSIBLE ORGANIZATION about unacceptable RISK related to the MEDICAL IT-NETWORK and the associated HAZARDS arising from any changes in configuration; and

j) monitoring all MEDICAL IT-NETWORK projects or changes to the MEDICAL IT-NETWORK for which the MEDICAL IT-NETWORK RISK MANAGER is responsible.

These tasks may be delegated, but the MEDICAL IT-NETWORK RISK MANAGER remains responsible for ensuring their adequate performance.

Compliance is checked by assessment of the RESPONSIBLE ORGANIZATION.

3.5 MEDICAL DEVICE manufacturer(s)

Pursuant to applicable regulations and relevant standards, each MEDICAL DEVICE manufacturer shall make available ACCOMPANYING DOCUMENTS to the RESPONSIBLE ORGANIZATION that describe the INTENDED USE and give instructions necessary for the safe and effective use of the MEDICAL DEVICE.

For a MEDICAL DEVICE that can be connected to an IT-NETWORK, the MEDICAL DEVICE manufacturer shall make available, instructions for implementing such connection, including but not limited to the following:

a) the purpose of the MEDICAL DEVICE'S connection to an IT-NETWORK;

b) the required characteristics for the IT-NETWORK incorporating the MEDICAL DEVICE;

c) the required configuration of the IT-NETWORK incorporating the MEDICAL DEVICE;

d) the technical specifications of the network connection of the MEDICAL DEVICE including security specifications;

e) the intended information flow between the MEDICAL DEVICE, the MEDICAL IT-NETWORK and other devices on the MEDICAL IT-NETWORK and, if relevant to the KEY PROPERTIES, the intended routing through the MEDICAL IT-NETWORK; and

f) a list of the hazardous situations resulting from a failure of the IT-NETWORK to provide the characteristics required to meet the purpose of the MEDICAL DEVICE connection to the IT-NETWORK.

Compliance is checked by availability of the MEDICAL DEVICE manufacturer's ACCOMPANYING DOCUMENTS and other available instructions for implementing such connection.

NOTE 1 Where the content made available does not meet the RESPONSIBLE ORGANIZATION'S RISK MANAGEMENT need, additional content can be made available under a RESPONSIBILITY AGREEMENT.

The RESPONSIBLE ORGANIZATION shall obtain the ACCOMPANYING DOCUMENTS for a MEDICAL DEVICE incorporated in a MEDICAL IT-NETWORK. These documents shall be maintained in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

The RESPONSIBLE ORGANIZATION shall obtain additional documentary information for a MEDICAL DEVICE incorporated in an IT-NETWORK as necessary to perform RISK MANAGEMENT for the MEDICAL IT-NETWORK, including any known hazardous situations that need to be managed by the RESPONSIBLE ORGANIZATION. These documents shall be maintained in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

NOTE 2 A RESPONSIBILITY AGREEMENT between the RESPONSIBLE ORGANIZATION and a MEDICAL DEVICE manufacturer can be used to identify and share the documentation needed.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

3.6 Providers of other information technology

Providers of other (not MEDICAL DEVICES) information technology may provide:

a) infrastructure components;

b) infrastructure services;

c) client devices not being MEDICAL DEVICES;

d) servers;

e) application software; or

f) middleware.

Pursuant to applicable regulations and relevant standards, each provider of other information technology (equipment and/or software) shall make available documentary information applicable to the technology being supplied as follows:

g) technical descriptions and technical manuals;

h) required IT-NETWORK characteristics;

i) recommended product configurations;

j) known incompatibilities and restrictions;

k) operating requirements;

l) product corrective actions and recalls; and

m) cyber security notices (warnings of known security vulnerabilities).

Compliance is checked by confirming the availability of the documentary information from each provider of other information technology.

NOTE 1 Where the content made available does not meet the RESPONSIBLE ORGANIZATION'S RISK MANAGEMENT need, additional content can be made available under a RESPONSIBILITY AGREEMENT.

The RESPONSIBLE ORGANIZATION shall obtain the documentary information specified above for other information technology incorporated in a MEDICAL IT-NETWORK. This documentary information shall be maintained in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

The RESPONSIBLE ORGANIZATION shall obtain supplementary documentary information for other information technology as necessary to further support the RISK MANAGEMENT activities of the MEDICAL IT-NETWORK. This supplementary documentary information shall be maintained in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Examples of supplementary information are:

- test strategies and test acceptance criteria;
- disclosure of failure modes;
- system reliability statistics;
- safety assurance cases; and
- performance.

NOTE 2 A RESPONSIBILITY AGREEMENT between the RESPONSIBLE ORGANIZATION and a provider of other information technology can be used to identify and share the documentation needed.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

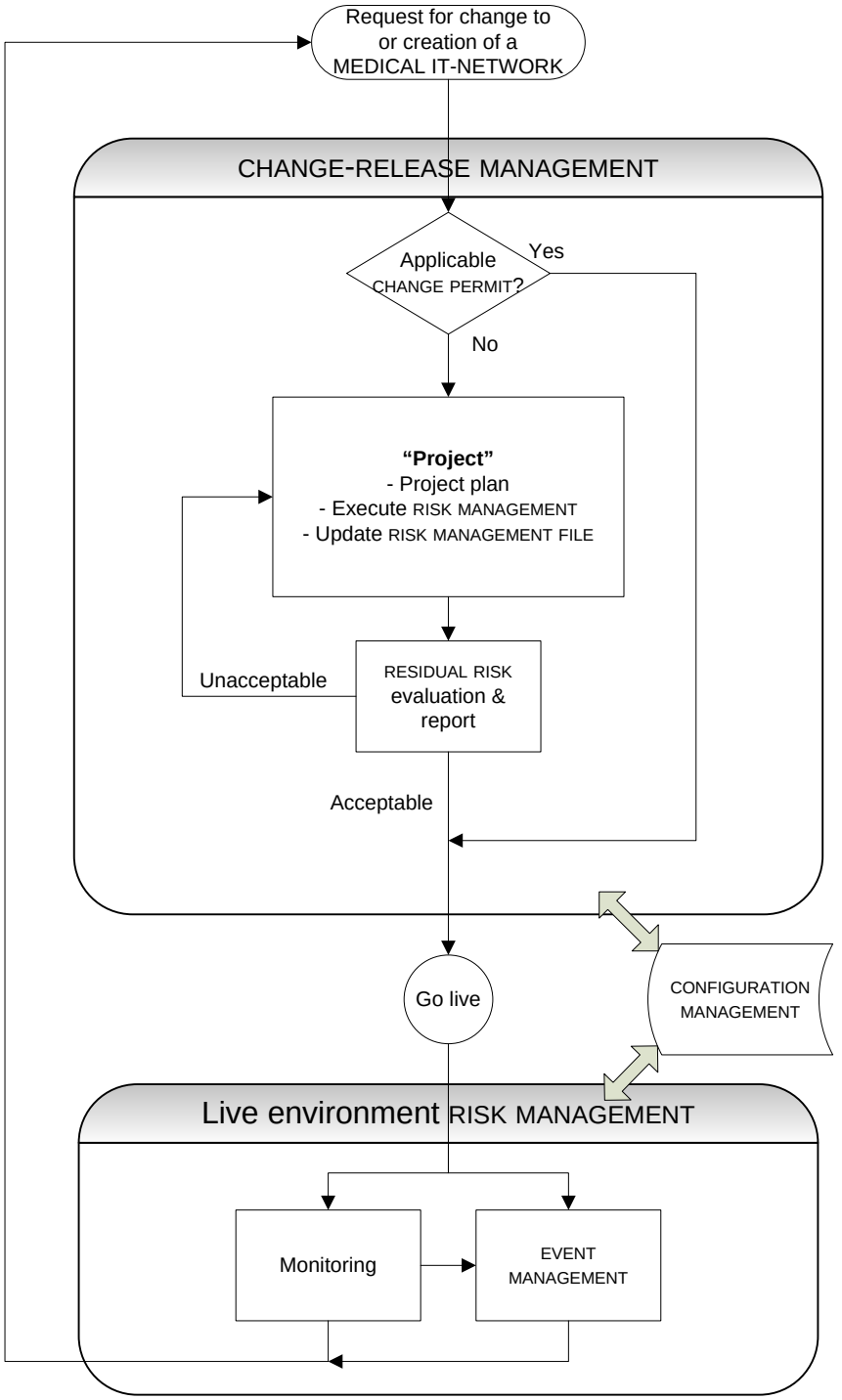
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS

4.1 Overview

The RESPONSIBLE ORGANIZATION shall maintain the KEY PROPERTIES of the MEDICAL IT-NETWORK throughout the life cycle.

NOTE The life cycle of MEDICAL IT-NETWORKS including RISK MANAGEMENT is illustrated in Figure 2.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.



NOTE A request for change can be a request to decommission a MEDICAL DEVICE or the MEDICAL IT-NETWORK. This decommissioning requires planning and RISK MANAGEMENT similar to other changes.

Figure 2 – Overview of life cycle of MEDICAL IT-NETWORKS including RISK MANAGEMENT

4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT

4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES

To support the MEDICAL IT-NETWORK life cycle, the TOP MANAGEMENT shall define and document a RISK MANAGEMENT policy for incorporating MEDICAL DEVICES into an IT-NETWORK. The RISK MANAGEMENT policy shall include:

a) balancing the three KEY PROPERTIES with the mission of the RESPONSIBLE ORGANIZATION;

b) a means to establish RISK acceptability criteria for each of the KEY PROPERTIES taking into account relevant international standards and national or regional regulations; and

c) a description of or reference to PROCESSES applying to MEDICAL IT-NETWORKS including, at least,

   1) EVENT MANAGEMENT,

   2) CHANGE-RELEASE MANAGEMENT,

   3) CONFIGURATION MANAGEMENT, and

   4) monitoring.

NOTE MEDICAL IT-NETWORK life cycle activities can be captured in an IT service management policy (e.g. per ISO 20000) provided there is a clear relationship to the RISK MANAGEMENT policy.

The policy shall be expressed in terms that can be interpreted throughout all RISK MANAGEMENT activities.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.2.2 RISK MANAGEMENT PROCESS

The MEDICAL IT-NETWORK RISK MANAGER shall establish and maintain a PROCESS for identifying HAZARDS, estimating and evaluating the associated RISKS, controlling these RISKS, and monitoring the effectiveness of the RISK CONTROLS, taking the defined use of the MEDICAL IT-NETWORK into account.

NOTE Subsequent changes to the MEDICAL IT-NETWORK could introduce new RISKS and require additional analyses.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation

4.3.1 Overview

The RESPONSIBLE ORGANIZATION shall plan RISK MANAGEMENT of the MEDICAL IT-NETWORK by providing

a) RISK-relevant asset description,

   NOTE 1 See 4.3.2 for a description and examples of RISK-relevant assets.

b) IT-NETWORK documentation, and

c) a RISK MANAGEMENT plan for the MEDICAL IT-NETWORK.

NOTE 2 Assessment and documentation of the structure of the network is essential to provide the necessary information for RISK ANALYSIS and RISK EVALUATION.

Because of the nature of IT-NETWORKS, both the current state of the IT-NETWORK and planned changes shall be considered.

Initial development of new MEDICAL IT-NETWORKS as well as changes to existing MEDICAL IT-NETWORKS not covered by documented CHANGE PERMITS shall be managed by projects.

NOTE 3 A MEDICAL IT-NETWORK can have multiple concurrent or sequential projects.

NOTE 4 See also 4.5.2.3 for MEDICAL IT-NETWORK projects and 4.5.2.2 for CHANGE PERMITS.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.3.2 RISK-relevant asset description

The RESPONSIBLE ORGANIZATION shall establish a list of assets of IT-NETWORKS interfacing with MEDICAL DEVICES. Typical assets include, but are not limited to hardware, software, and data essential to the INTENDED USE of the MEDICAL DEVICE and the defined use of the MEDICAL IT-NETWORK. The asset list may include for example:

a) specific components of the MEDICAL IT-NETWORK and all incorporated MEDICAL DEVICES and other equipment (e.g. image creating modalities, network components) of the IT infrastructure;

b) operational characteristics of the IT infrastructure of the MEDICAL IT-NETWORK (e.g. performance properties such as bandwidth);

c) CONFIGURATION MANAGEMENT information;

d) medical application software;

e) data about configuration of hardware and software;

f) characterization of identifiable patient data on the MEDICAL IT-NETWORK or used by the incorporated MEDICAL DEVICE including its nature, volume, and sensitivity;

g) healthcare procedure support information, including history of use and OPERATOR/user details; and

h) a security description and other materials relevant to total system SAFETY considerations (in case security is an aspect of SAFETY).

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.3.3 MEDICAL IT-NETWORK documentation

The RESPONSIBLE ORGANIZATION shall establish and maintain network documentation necessary to support the RISK MANAGEMENT of the MEDICAL IT-NETWORK for the interfaces between the MEDICAL DEVICE(S) and all network components (both software and hardware). This documentation shall include but not be limited to:

a) physical and logical network configuration;

NOTE 1 The network configuration includes defining the boundaries of the network.

NOTE 2 Documentation can contain IT-NETWORK electrical properties that might impact the performance of the MEDICAL IT-NETWORK and incorporated devices. Examples include, but are not limited to, grounding, galvanic (de)coupling, stray currents, and power over Ethernet.

b) applied standards and conformance statements;

c) physical and logical client / server structure;

d) network security, reliability and data integrity;

e) network communication requirements for each MEDICAL DEVICE as specified by the manufacturer; and

f) future (planned / reasonably foreseeable) changes / upgrades / enhancements.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.3.4 RESPONSIBILITY AGREEMENT

Whenever a MEDICAL DEVICE is incorporated into an IT-NETWORK, or the configuration of such a connection is changed, the RESPONSIBLE ORGANIZATION shall determine the need for one or more documented RESPONSIBILITY AGREEMENTS that define (e.g. by contract) the responsibilities of all relevant stakeholders.

A RESPONSIBILITY AGREEMENT may cover one or more projects or the maintenance of one or more MEDICAL IT-NETWORKS, and shall identify responsibility for all aspects of the MEDICAL IT-NETWORK life cycle and all activities that form part of that life cycle.

NOTE In order to support incorporating MEDICAL DEVICES into an IT-NETWORK, the MEDICAL DEVICE manufacturers make available technical information appropriate to the creation of RESPONSIBLE ORGANIZATION RISK MANAGEMENT documentation. Where the PROCESS requires information that a MEDICAL DEVICE manufacturer believes is sensitive in nature, the provision of the information will be determined by the RESPONSIBILITY AGREEMENT and can be protected by a confidentiality agreement.

The RESPONSIBILITY AGREEMENTS shall contain (or refer to documents which contain) at a minimum:

a) the name of the person responsible for RISK MANAGEMENT for the activities covered by the RESPONSIBILITY AGREEMENT;

b) the scope of the activities covered by the RESPONSIBILITY AGREEMENT, including a summary of and/or reference to the requirements;

c) a list of the MEDICAL DEVICES and other equipment which are to be incorporated into the IT-NETWORK or changed, together with the names of MEDICAL DEVICE manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project;

d) a list of documents to be supplied by the MEDICAL DEVICE manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT-NETWORK;

e) technical information to be supplied by the MEDICAL DEVICE or IT manufacturers and other equipment suppliers that is necessary to perform RISK ANALYSIS for the IT-NETWORK; and

f) definition of roles and responsibilities in managing potentially adverse events.

The RESPONSIBLE ORGANIZATION shall provide a summary of responsibilities as appropriate.

NOTE 1 The manufacturer of a MEDICAL DEVICE is responsible for making available technical documentation on how to use the MEDICAL DEVICE'S interfaces to connect to an IT-NETWORK, provided that such a connection is intended by the

manufacturer. There is no such obligation on the supplier of other equipment, and it might be necessary to make a specific arrangement to gain access to such technical documentation.

If the co-operation of manufacturers of MEDICAL DEVICES, suppliers of other equipment or other organizations is necessary in addition to the listed documents supplied by the manufacturers or organizations, a RESPONSIBILITY AGREEMENT shall:

g) identify the nature of the co-operation required; and

h) state:

— who is responsible for requesting such co-operation;

— who is responsible for responding to such requests; and

— what criteria will be used to judge the adequacy of such response.

NOTE 2 Since this information can change through the lifecycle of a MEDICAL IT-NETWORK, it is recommended that it be updated periodically in the RESPONSIBILITY AGREEMENT.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK

The RESPONSIBLE ORGANIZATION shall establish and maintain a RISK MANAGEMENT plan for each MEDICAL IT-NETWORK. The RISK MANAGEMENT plan shall include:

a) a description of the MEDICAL IT-NETWORK, including:

1) identified stakeholders within the RESPONSIBLE ORGANIZATION that shall be informed about HAZARDS to ensure their RISK awareness;

2) the defined use and expected benefits of the MEDICAL IT-NETWORK;

3) the reason for each MEDICAL DEVICE incorporation; and

4) the use of each MEDICAL DEVICE, due to its incorporation into the MEDICAL IT-NETWORK that is not included in the manufacturer's INTENDED USE.

b) a description of activities, roles and responsibilities for all parties involved in operating/maintaining the MEDICAL IT-NETWORK, with respect to RISK MANAGEMENT.

c) requirements for monitoring the MEDICAL IT-NETWORK (refer to 4.6.1).

d) criteria for RISK acceptability, based on the RESPONSIBLE ORGANIZATION'S policy for determining acceptable RISK, including criteria for accepting RISKS when the probability of occurrence of HARM cannot be estimated.

When a project introduces changes to an existing MEDICAL IT-NETWORK, the RISK MANAGEMENT plan for the MEDICAL IT-NETWORK shall be updated.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4 MEDICAL IT-NETWORK RISK MANAGEMENT

4.4.1 Overview

This section describes RISK MANAGEMENT PROCESSES that support both the execution of a MEDICAL IT-NETWORK project as well as the decision to go live on any particular change.

The RISK MANAGEMENT activities of RISK ANALYSIS, RISK EVALUATION, RISK CONTROL, RESIDUAL RISK evaluation and reporting and approval shall be documented. This documentation may be integral to the RISK MANAGEMENT plan or exist as separate documents in the RISK MANAGEMENT FILE associated with the MEDICAL IT-NETWORK. Action plans arising from RISK ASSESSMENT shall follow the CHANGE-RELEASE MANAGEMENT PROCESS.

NOTE 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.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.2 RISK ANALYSIS

The RESPONSIBLE ORGANIZATION shall identify HAZARDS that are likely to arise from the MEDICAL IT–NETWORK.

For each identified HAZARD, the RESPONSIBLE ORGANIZATION shall estimate the associated RISKS using available information or data.

NOTE RISKS to be analyzed cover the entire life cycle, especially including the implementation of the change and the regular use of the MEDICAL IT-NETWORK.

If the probability of the occurrence of HARM cannot be estimated, the possible consequences shall be listed for use in RISK EVALUATION and RISK CONTROL.

The results of these activities shall be recorded in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.3 RISK EVALUATION

For each identified HAZARD, the RESPONSIBLE ORGANIZATION shall decide, using the criteria defined in the RISK MANAGEMENT plan, whether:

a) the estimated RISK(S) is so low that RISK reduction need not to be pursued. In this case the rationale for this decision shall be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

b) the estimated RISK(S) are not acceptable. In this case RISK CONTROL measures shall be implemented according to 4.4.4.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.4 RISK CONTROL

4.4.4.1 RISK CONTROL option analysis

The RESPONSIBLE ORGANIZATION shall identify and document proposed RISK CONTROL measures for each unacceptable RISK until the RESIDUAL RISK(S) is judged acceptable.

One or more RISK CONTROL options shall be used in the priority order listed:

a) inherent control by design (e.g. physical isolation of a network from external threats);

b) protective measures (e.g. including alarms);

c) information for assurance (e.g. warnings, user documentation, training).

NOTE 1 RISK CONTROL measures can include for example:

- instructions and constraints documented as a CHANGE PERMIT (see 2.3 and 4.5.2.2);
- network components;
- change of network configuration;
- organizational considerations; or
- changes to the incorporated MEDICAL DEVICES.

NOTE 2 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.

To the extent that RISK CONTROL entails tradeoffs in KEY PROPERTIES, the KEY PROPERTIES shall be considered in priority order of SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY.

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 (see 4.4.5).

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.4.2 RISK CONTROL measures

When a specific RISK CONTROL measure is selected that requires a change to the MEDICAL IT-NETWORK, CHANGE-RELEASE MANAGEMENT PROCESSES shall be followed.

The RISK CONTROL measures selected shall be recorded in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.4.3 Implementation of RISK CONTROL measures

The selected RISK CONTROL measures shall be implemented.

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.

Any changes to a MEDICAL DEVICE undertaken by the RESPONSIBLE ORGANIZATION without documented consent of the MEDICAL DEVICE manufacturer are not recommended. If such a change is undertaken, the RESPONSIBLE ORGANIZATION shall notify the manufacturer and shall follow all necessary regulatory steps for putting such a modified MEDICAL DEVICE into service.

Any RESIDUAL RISK shall be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.4.4 VERIFICATION of RISK CONTROL measures

The implementation of all RISK CONTROL measures in the operational system shall be VERIFIED and documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

The effectiveness of the RISK CONTROL measures shall be VERIFIED and documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

NOTE It might be necessary to verify the effectiveness of RISK CONTROL measures in a test environment prior to implementation in the operational system.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.4.5 New RISKS arising from RISK CONTROL

The implemented RISK CONTROL measures and the installed operational system shall be reviewed for new, unacceptable RISKS (i.e. degraded KEY PROPERTIES or other important attributes essential in realizing the defined use of the MEDICAL IT-NETWORK).

The evaluation shall be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.4.5 RESIDUAL RISK evaluation and reporting

Based on a pre-release assessment of the effectiveness of the implemented RISK CONTROL measures, the RESIDUAL RISK shall be evaluated.

Both the individual RESIDUAL RISKS and the overall RESIDUAL RISK shall be assessed for acceptability.

NOTE See 4.4.3 for RISK EVALUATION.

If an individual RESIDUAL RISK or the overall RESIDUAL RISK is not determined to be acceptable, additional RISK CONTROL measures shall be applied.

The RESPONSIBLE ORGANIZATION shall define and document a RESIDUAL RISK summary containing a list of all individual RESIDUAL RISKS and the overall RESIDUAL RISK remaining after the RISK CONTROL measures have been implemented (see 4.4.4.3), including the RESIDUAL RISKS associated with a particular MEDICAL IT-NETWORK project, and the MEDICAL IT-NETWORK RESIDUAL RISK.

If reduction of RESIDUAL RISK to an acceptable level is not practicable, using the RESPONSIBLE ORGANIZATION'S policy for determining acceptable RISK (see 3.3), the person identified by the TOP MANAGEMENT (see 3.3) to review RESIDUAL RISKS (who may be the MEDICAL IT-NETWORK RISK MANAGER) shall conduct and document a RISK/benefit analysis of the individual or overall RESIDUAL RISK against the health benefit accrued from the incorporation of the MEDICAL DEVICE into the IT-NETWORK, and decide whether to approve the MEDICAL IT-NETWORK RESIDUAL RISK.

NOTE See ISO 14971 [4] for RISK/benefit analysis.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT

4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS

The RESPONSIBLE ORGANIZATION shall document and apply a CHANGE-RELEASE MANAGEMENT PROCESS.

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.

The MEDICAL IT-NETWORK RISK MANAGER shall use the results of the RISK MANAGEMENT PROCESS to determine approval and acceptability of changes during the CHANGE-RELEASE MANAGEMENT PROCESS.

NOTE Unintended consequences can occur when two or more projects running in parallel are insufficiently coordinated.

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.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.5.2 Decision on how to apply RISK MANAGEMENT

4.5.2.1 Overview

For any new MEDICAL IT-NETWORK or a change to an existing MEDICAL IT-NETWORK, the CHANGE-RELEASE MANAGEMENT PROCESS shall be initiated.

The RESPONSIBLE ORGANIZATION shall 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.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.5.2.2 CHANGE PERMITS

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.

NOTE 1 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.

NOTE 2 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.

A CHANGE PERMIT shall specify what records are to be kept for each permitted change.

CHANGE PERMITS shall be maintained in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

NOTE 3 CHANGE PERMITS can only be established as an outcome of the RISK MANAGEMENT PROCESS (see 4.4.4.2).

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.5.2.3 MEDICAL IT-NETWORK projects

The RESPONSIBLE ORGANIZATION shall 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 typical first project plan would be for development of a new MEDICAL IT-NETWORK. The project plan shall provide:

a) requirements for RISK MANAGEMENT activities including:
   1) 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;
   2) a plan to meet the requirements stated in the RISK MANAGEMENT plan for the affected MEDICAL IT-NETWORK(S); and
   3) activities for VERIFICATION of RISK CONTROL measures.

b) a description of the project including:
   1) identification of MEDICAL IT-NETWORK(S) developed or affected by the project;
   2) requirements specification for the project; and
   3) specification of minimum set of documents required for the MEDICAL IT-NETWORK project.

c) the scope of the planned changes to the MEDICAL IT-NETWORK, including but not limited to:
   1) physical and logical configuration of the MEDICAL IT-NETWORK before and after the planned changes;
   2) information flow before and after the planned changes;
   3) components to be acquired or removed;
   4) specifications of non-medical network components where relevant; and
   5) constraints on the extendibility of the existing MEDICAL IT-NETWORK.

The project plan shall be revised whenever necessary to reflect changes to the project.

The project plan shall be kept in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE in accordance with the life cycle PROCESSES of EVENT MANAGEMENT, CHANGE-RELEASE MANAGEMENT, AND CONFIGURATION MANAGEMENT.

NOTE Where changes to the IT-NETWORK occur frequently, the project plan may be established as a reusable protocol document containing all these essential elements.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.5.3 Go-live

The transition of the MEDICAL IT-NETWORK to the “live environment” (Figure 2) is the goal of all project or change initiatives. Before going live, the RESPONSIBLE ORGANIZATION shall review the MEDICAL IT-NETWORK RESIDUAL RISK.

The MEDICAL IT-NETWORK RISK MANAGER shall examine all project or change RESIDUAL RISK summaries to determine acceptability of RISK associated with interactions with recent or pending

projects or changes (e.g., the incorporation of the MEDICAL DEVICE into an operational, evolving IT-NETWORK).

The MEDICAL IT-NETWORK RISK MANAGER shall approve the specified change to the MEDICAL IT-NETWORK prior to go-live.

The approval of the MEDICAL-IT NETWORK RESIDUAL RISK shall be documented and the configuration information recorded in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.6 Live network RISK MANAGEMENT

4.6.1 Monitoring

The RESPONSIBLE ORGANIZATION shall establish and maintain a PROCESS to monitor each installed MEDICAL IT-NETWORK for emerging RISKS, effectiveness of RISK CONTROL measures, and accuracy of original estimations of RISK.

Requirements for monitoring shall be established as part of the RISK MANAGEMENT plan of the MEDICAL IT-NETWORK. Examples of what to monitor are:

a) environment changes (including local/connected environment as well as relevant network or component DATA AND SYSTEMS SECURITY vulnerabilities);

b) operational/performance feedback e.g., user feedback, speed problems, high error rates, failure, malicious software attacks;

c) information about the incorporated components;

d) information about similar MEDICAL IT-NETWORKS;

e) reported events; and

f) auditing of non-technical RISK CONTROL measures such as organizational policies and procedures.

If monitoring indicates actual or potential increase in RISK associated with the MEDICAL IT-NETWORK or its components (potential or actual negative impact), the EVENT MANAGEMENT PROCESS shall be initiated and significant findings reported to the appropriate party in the RESPONSIBLE ORGANIZATION.

NOTE In some cases, the RESPONSIBLE ORGANIZATION might be required to report observations to regulatory bodies.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

4.6.2 EVENT MANAGEMENT

The RESPONSIBLE ORGANIZATION shall establish EVENT MANAGEMENT to:

a) capture and document negative events;

b) evaluate events and propose changes as appropriate through CHANGE-RELEASE MANAGEMENT;

c) track all corrective and preventive actions leading to closure; and

d) report significant finds to the MEDICAL IT-NETWORK RISK MANAGER and/or others in the RESPONSIBLE ORGANIZATION.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

5 Document control

5.1 Document control procedure

All relevant documents in the MEDICAL IT-NETWORK life cycle shall be revised, amended, reviewed, and approved in accordance with a document control procedure.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE

In addition to the requirements of other clauses of this standard, the MEDICAL IT-NETWORK RISK MANAGEMENT FILE shall provide traceability for each identified HAZARD to:

a) the RISK ANALYSIS;

b) the RISK EVALUATION;

c) the implementation and VERIFICATION of the RISK CONTROL measures; and

d) the assessment of the acceptability of any RESIDUAL RISK(S) with approval.

NOTE 1 The records and other documents that make up the MEDICAL IT-NETWORK RISK MANAGEMENT FILE can form part of other documents and files. The MEDICAL IT-NETWORK RISK MANAGEMENT FILE need not physically contain all the records and other documents; however, it should contain at least references or pointers to all required documentation. The RESPONSIBLE ORGANIZATION should be able to assemble the information referenced in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE in a timely fashion.

NOTE 2 The MEDICAL IT-NETWORK RISK MANAGEMENT FILE can be in any form or type of medium.

NOTE 3 In those organizations where an “assurance case” is the means of organizing the MEDICAL IT-NETWORK RISK MANAGEMENT FILE, refer to ISO/IEC 15026-2 [5] (under development) for more information.

Compliance is checked by inspection of the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

Annex A
(informative)

Rationale

A.1 General

The convergence of MEDICAL DEVICES and information management systems has resulted in a need for changes in the way the SAFETY and EFFECTIVENESS of MEDICAL DEVICES is maintained following their placement into service. While the responsibility of the MEDICAL DEVICE manufacturer (often referred to as an "MDM") for placing a safe and effective MEDICAL DEVICE on the market has not changed, the environment (i.e. the IT-NETWORK) that the MEDICAL DEVICE is placed into is constantly changing. The MEDICAL DEVICE manufacturer cannot foresee all the potential changes and has no way of ensuring that the MEDICAL DEVICE will function properly in all possible cases.

At the same time, the RESPONSIBLE ORGANIZATION (often referred to as a healthcare delivery organization or HDO) has requirements relating to their ability to deliver high quality health care, and security and privacy of patient data that must be achieved under the same constantly changing environment. Achieving these requirements cannot be accomplished without the proper functioning of MEDICAL DEVICES that are part of the environment, i.e. incorporated in their IT-NETWORK.

This International Standard recognizes that co-operation is required between those involved in supplying and connecting MEDICAL DEVICES in IT-NETWORKS to achieve all these requirements with today's rapidly changing technology. It identifies the necessary roles and responsibilities, and a PROCESS for managing the RISK posed by the incorporation of MEDICAL DEVICES into the information technology infrastructure of the healthcare delivery organization. While the RESPONSIBLE ORGANIZATION takes responsibility for the decisions they make about incorporation of MEDICAL DEVICES into IT-NETWORKS, these decisions are partly based on claims made and information shared by their suppliers. In some cases the documentation made available when products are placed on the market will be sufficient to support the RESPONSIBLE ORGANIZATION'S decisions. In other cases, the RESPONSIBLE ORGANIZATION will need to obtain additional information that might not normally be available. This standard suggests using a RESPONSIBILITY AGREEMENT to identify what information is needed throughout life of the MEDICAL IT-NETWORK and the responsibilities for providing and controlling access to that information.

In order to maintain evidence of conformance to the requirements of this standard, it is necessary to collect and maintain documentation in a RISK MANAGEMENT FILE for each MEDICAL IT-NETWORK.

A.2 Clause 3 – Roles and responsibilities

This clause identifies the roles and responsibilities that need to cooperate to manage the RISK of incorporating MEDICAL DEVICES into IT-NETWORKS.

The healthcare delivery organization that owns and utilizes the MEDICAL IT-NETWORK has overall responsibility for its functioning. It is the RESPONSIBLE ORGANIZATION. To ensure that RISK MANAGEMENT is properly addressed for the MEDICAL IT-NETWORK, the TOP MANAGEMENT of the RESPONSIBLE ORGANIZATION is required by this standard to establish policy, provide resources,

assign qualified people and review the results of RISK MANAGEMENT activities. It is important that someone be assigned the responsibility for the execution of the RISK MANAGEMENT PROCESS for the MEDICAL IT-NETWORK. A primary responsibility of TOP MANAGEMENT is appointing a MEDICAL IT-NETWORK RISK MANAGER and ensuring that others in the RESPONSIBLE ORGANIZATION co-operate with the MEDICAL IT-NETWORK RISK MANAGER to manage the RISK of incorporating MEDICAL DEVICES into IT-NETWORKS.

Because the concept of RISK depends on the clinical impact of the failure as well as the probability of failure, the responsibilities of the MEDICAL DEVICE manufacturers are different than those of providers of other information technology. MEDICAL DEVICE manufacturers have an understanding of the clinical impact of a network failure which is based on the INTENDED USE of the MEDICAL DEVICE, whereas IT providers can only offer information on failure modes, probabilities, etc., of the IT equipment. For these reasons, these two roles are addressed independently.

The MEDICAL DEVICE manufacturer is required to have ACCOMPANYING DOCUMENTS available. These ACCOMPANYING DOCUMENTS have to be made available to the RESPONSIBLE ORGANIZATION as the content of these documents is essential for the RESPONSIBLE ORGANIZATION'S RISK MANAGEMENT activities during incorporating MEDICAL DEVICES into an IT-NETWORK. It is noted that there can be different understandings in the content and the extent of the ACCOMPANYING DOCUMENTS. For that reason, the requirements 3.5 a) through 3.5 f) define the minimal content of such ACCOMPANYING DOCUMENTS as there are MEDICAL DEVICES which are not required to demonstrate compliance with IEC 60601-1 (e.g. IVD medical devices). However, application of subclause 14.13 of IEC 60601-1:2005 [1] to satisfy these requirements for MEDICAL DEVICE manufacturers is strongly encouraged.

Network failure modes and probabilities also depend on items outside the control of either the MEDICAL DEVICE manufacturers or the providers of other information technology such as the system design, configuration, topology, IT processes and procedures, actual use (vs. intended) of the MEDICAL DEVICE, etc. Therefore, only the RESPONSIBLE ORGANIZATION has ultimate visibility of the RISKS of the MEDICAL IT-NETWORK and has the primary responsibility for the RISK MANAGEMENT of the MEDICAL IT-NETWORK.

A.3 Clause 4 – Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS

A basic premise of this standard is that RISK must be considered for all changes before they are made to a MEDICAL IT-NETWORK. This standard requires RISK MANAGEMENT to be performed on MEDICAL IT-NETWORKS. There can be multiple MEDICAL IT-NETWORKS per RESPONSIBLE ORGANIZATION. The RISK MANAGEMENT activities required in this document are based largely on those of ISO 14971 [4] but go beyond SAFETY as defined in ISO 14971 to include managing RISK to EFFECTIVENESS and RISK to DATA AND SYSTEM SECURITY. This requires some changes to defined terms from ISO 14971. For this standard, HARM is extended to include reduction in EFFECTIVENESS and breach of security. This requires SAFETY to specify what type of HARM is included in the RISK. So the definition of SAFETY becomes freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment. With these changes, the RISK MANAGEMENT activities of ISO 14971 can be applied for this standard. Because they are being applied to the life cycle management of a MEDICAL IT-NETWORK, they are described in the context of an operational MEDICAL IT-NETWORK. Clause 4 is divided into sub-clauses that describe the RISK MANAGEMENT activities during the change of a MEDICAL IT-NETWORK or during the operation of a MEDICAL IT-NETWORK. Table A.1 shows the relationship of the RISK MANAGEMENT activities of ISO 14971 to those in this standard.

Subclause 4.2 – RESPONSIBLE ORGANIZATION RISK MANAGEMENT

Subclause 4.2 describes activities and deliverables that are required at the level of the RESPONSIBLE ORGANIZATION. These deliverables apply to all MEDICAL IT-NETWORKS within the RESPONSIBLE ORGANIZATION.

Subclause 4.3 – MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation

Subclause 4.3 describes activities and deliverables needed on a per MEDICAL IT-NETWORK basis that are required for RISK MANAGEMENT activities to commence.

Table A.1 – Relationship between ISO 14971 and IEC 80001-1

ISO 14971:2007 section		IEC 80001-1 section	
4	**RISK ANALYSIS**		
4.1	RISK ANALYSIS PROCESS	n/a	
4.2	INTENDED USE and identification of characteristics related to SAFETY		
4.3	Identification of HAZARDS	4.4.2	**RISK ANALYSIS**
4.4	Estimation of the RISK(S) for each hazardous situation – "Reasonably foreseeable sequences or combinations of events that can result in a hazardous situation shall be considered and the resulting hazardous situation(s) shall be recorded" – "For each identified hazardous situation, the associated RISK(S) shall be estimated"	4.4.2	"For each identified HAZARD, the RESPONSIBLE ORGANIZATION shall estimate the associated RISKS…"
5	**RISK EVALUATION**	4.4.3	**RISK EVALUATION**
6	**RISK CONTROL**	4.4.4	**RISK CONTROL**
6.1	RISK reduction	n/a	
6.2	RISK CONTROL option analysis	4.4.4.1	RISK CONTROL option analysis
		4.4.4.2	RISK CONTROl measures
6.3	Implementation of RISK CONTROL measures	4.4.4.3	Implementation of RISK CONTROL measures
		4.4.4.4	VERIFICATION of RISK CONTROL measures
6.4	RESIDUAL RISK evaluation		(addressed in 4.4.4.1)
6.5	RISK/benefit analysis		(addressed in both 4.4.4.1 and 4.4.5)
6.6	RISKS arising from RISK CONTROL measures	4.4.4.5	New RISKS arising from RISK CONTROL
7	**Evaluation of overall RESIDUAL RISK acceptability**	4.4.5	**RESIDUAL RISK evaluation and reporting**

Subclause 4.5 – CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT

Subclause 4.5 describes RISK MANAGEMENT activities that are required when changing a MEDICAL IT-NETWORK before it enters the live environment phase. This includes changing an existing MEDICAL IT-NETWORK as well as initially building a MEDICAL IT-NETWORK or turning a non-MEDICAL IT-NETWORK into a MEDICAL IT-NETWORK. In this stage, the traditional RISK MANAGEMENT activities

occur in the context of a project. The MEDICAL IT-NETWORK RISK MANAGER is responsible for consolidating all project RISK MANAGEMENT activities into a single RISK MANAGEMENT FILE for the MEDICAL IT-NETWORK.

Some RISK CONTROL measures defined for the MEDICAL IT-NETWORK can include activities during the live environment phase, such as clinical procedures to mitigate network outage.

For activities that are performed frequently, it is desirable to avoid unnecessary repetition of RISK MANAGEMENT. This standard mentions CHANGE PERMITS as one way to do this. If RISK MANAGEMENT demonstrates that a routine change, for example adding a user, can be performed with acceptable RISK, subject to specified constraints (for example a limit on the type and number of users), then the RESPONSIBLE ORGANISATION can define a CHANGE PERMIT which allows such routine changes and specifies the constraints.

Subclause 4.6 – Live Network RISK MANAGEMENT

Subclause 4.6 describes RISK MANAGEMENT activities needed after the MEDICAL IT-NETWORK is put into use (live environment).

Monitoring is the ongoing review of all RISK MANAGEMENT activities and RISK CONTROLS that were put in place to achieve acceptable RISK in the use (live environment) of MEDICAL IT-NETWORK(S). It delivers the evidence that overall RISK to KEY PROPERTIES in the MEDICAL IT-NETWORK(S) is acceptable.

EVENT MANAGEMENT specifies those actions required when a real or potential negative event occurs during use of a MEDICAL IT-NETWORK in the live environment.

Annex B
(informative)

Overview of RISK MANAGEMENT relationships

Figure B.1 provides an overview of the various roles and relationships involved in carrying out a RISK MANAGEMENT effort that involves incorporation of MEDICAL DEVICES on IT-NETWORKS.

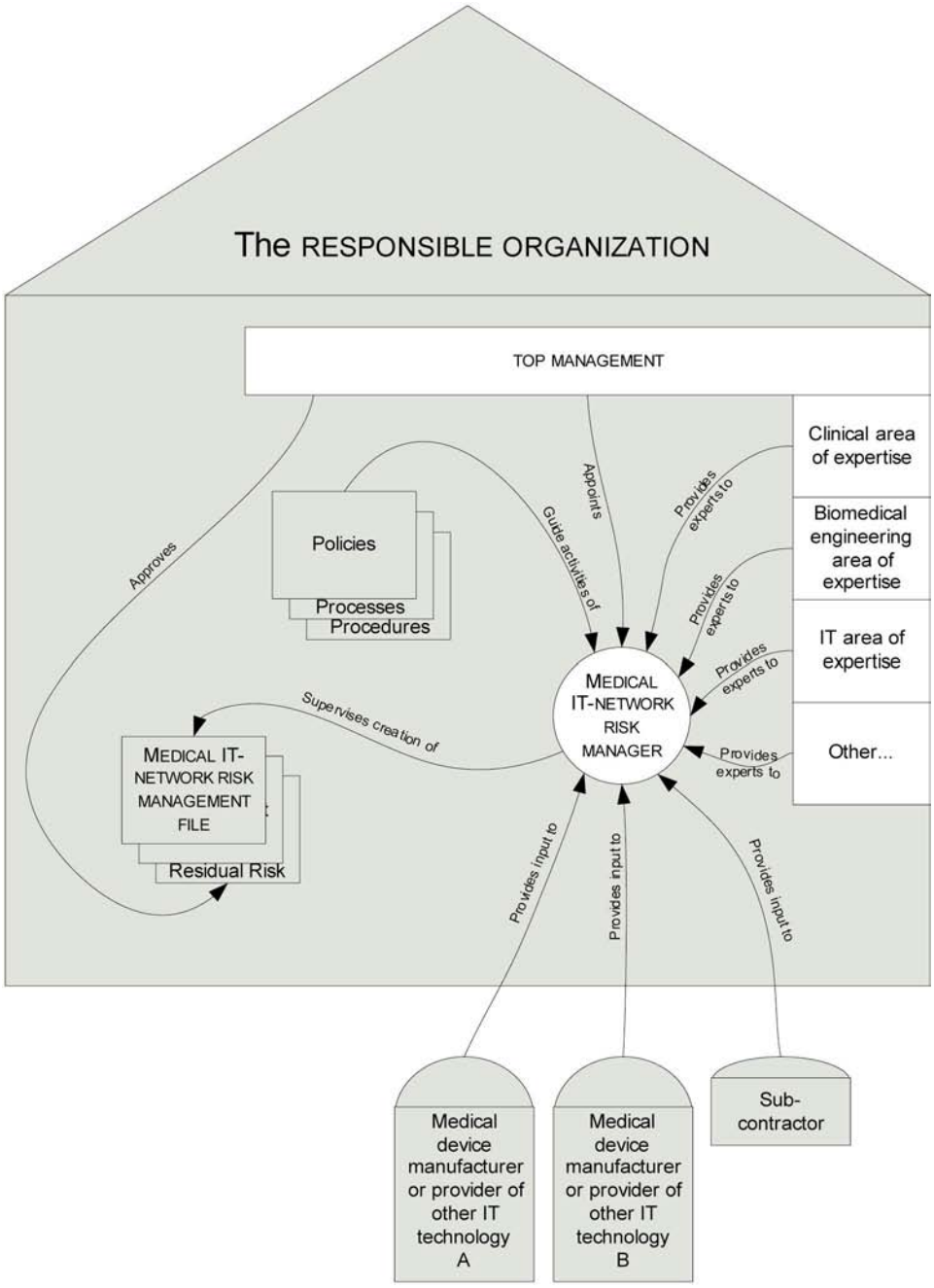


Figure B.1 – Overview of roles and relationships

IEC 2390/10

Annex C
(informative)

Guidance on field of application

C.1 Overview

The field of application statement for IEC 80001-1 provides a starting point which describes which IT-NETWORKS are in the scope of the standard. This document provides additional guidance including examples of IT-NETWORKS that are in scope as well as out of scope.

C.2 When to apply this standard

Table C.1 provides guidance concerning various IT-NETWORK scenarios that may be encountered in a clinical environment and whether to apply IEC 80001-1 PROCESSES to them.

Table C.1 – IT-NETWORK scenarios that can be encountered in a clinical environment

System config-uration	Scenario description		Network components	Network	Network responsibility	Standard
1	a	MEDICAL DEVICES from one MEDICAL DEVICE manufacturer and non-MEDICAL DEVICES incorporated by the same MEDICAL DEVICE manufacturer and installed as required by that MEDICAL DEVICE manufacturer on an isolated IT-NETWORK.	MEDICAL and non-MEDICAL DEVICE(S) from single MEDICAL DEVICE manufacturer	Physically isolated	MEDICAL DEVICE manufacturer	14971
	b	MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and installed as required by that MEDICAL DEVICE manufacturer on an isolated IT-NETWORK	MEDICAL DEVICES and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers	Physically isolated	MEDICAL DEVICE manufacturer	14971
2	a	MEDICAL and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and MEDICAL and non-MEDICAL DEVICES incorporated by other MEDICAL DEVICE manufacturers interconnected on the same IT-NETWORK by a 3rd party (such as a hospital).	Medical and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	80001-1
	b	MEDICAL and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and MEDICAL and non-MEDICAL DEVICES incorporated by other MEDICAL DEVICE manufacturers as well as non-MEDICAL DEVICES and applications interconnected on a shared IT-NETWORK by a 3rd party.	MEDICAL and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers plus multiple non-MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	80001-1
3		Installations with non-MEDICAL DEVICES from multiple manufacturers using the IT-NETWORK for transmission of electronic Protected Health Information (ePHI).	Multiple non-MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	Out of 80001-1 scope [a]

[a] Local national regulations on medical data security apply, however, the RESPONSIBLE ORGANIZATION can also choose to apply IEC 80001-1.

Some examples can assist in understanding the various network types listed in Table C.1:

- Configuration 1a – Patient monitoring devices on their own isolated network or the same devices with a gateway to hospital IT-NETWORK for non-MEDICAL DEVICE uses.
- Configuration 1b – Patient monitoring devices from vendor A combined with network attached infusion devices from vendor B provided as an integrated controlled solution by a single vendor (A, B or C).
- Configuration 2a – Multiple MEDICAL DEVICES from different MEDICAL DEVICE manufacturers placed on a common IT-NETWORK by a hospital.
- Configuration 2b – Network attached infusion devices on shared IT-NETWORK with other hospital applications, and/or patient monitoring devices on an isolated network with a gateway to the hospital IT-NETWORK for MEDICAL DEVICE uses such as alarm reporting.
- Configuration 3 – Hospital systems communicating patient demographics and related electronic Protected Health Information (ePHI).

Annex D
(informative)

Relationship with ISO/IEC 20000-2:2005, *Information technology – Service management – Part 2: Code of practice*

D.1 General

IEC 80001-1 applies the concept of life cycle RISK MANAGEMENT to an IT-NETWORK incorporating MEDICAL DEVICES. As with general IT-NETWORKS, MEDICAL IT-NETWORKS can be highly complex, highly dynamic systems where monitoring often leads to the need for change. Implementing these changes requires careful preparation. In most cases, because of their regulation under law for quality systems and validation, MEDICAL DEVICE manufacturers are less able to rapidly change their MEDICAL DEVICES. Per regulation, changes and maintenance require strictly formal strategies and procedures that often require the direct involvement of the MEDICAL DEVICE manufacturer. For MEDICAL IT-NETWORKS, both the RESPONSIBLE ORGANIZATION and MEDICAL DEVICE manufacturer need to recognize these inherently different constraints on service management. In addition, the incorporation of MEDICAL DEVICES can lead to co-dependency of the MEDICAL IT-NETWORK and MEDICAL DEVICES, so that change to one leads to the need for change of the other.

Life cycle RISK MANAGEMENT in a MEDICAL IT-NETWORK needs to be done in the context of the specific operating conditions required to support effective healthcare delivery. For this reason, the concepts of IT-service management as described in ISO/IEC 20000-2 [10] have been reviewed for their ability to meet the requirements of IEC 80001-1. This annex provides a simple overview of the relationship between IEC 80001-1 and ISO/IEC 20000-2 to aid in the investigation of service strategies that could address the service needs of a MEDICAL IT-NETWORK. This information also aims to assist in the communication between the parties responsible for IT-NETWORKS and MEDICAL DEVICES (i.e. RESPONSIBLE ORGANIZATION, MEDICAL DEVICE manufacturer, and providers of other IT technology).

Compliance with ISO/IEC 20000-2 [10] is not equivalent to compliance with IEC 80001-1.

D.2 Terminology and definitions

Where MEDICAL DEVICES require maintenance, repair or modifications and eventually replacement, IT-NETWORKS have incidents and problems that must be handled and (major) changes that require careful implementation. There are many similarities in the service to both MEDICAL DEVICE(S) and IT-NETWORK(S). For reference, Figure D.1, taken from ISO/IEC 20000-1:2005 [10] indicates the relationship between service processes for IT-NETWORKS.

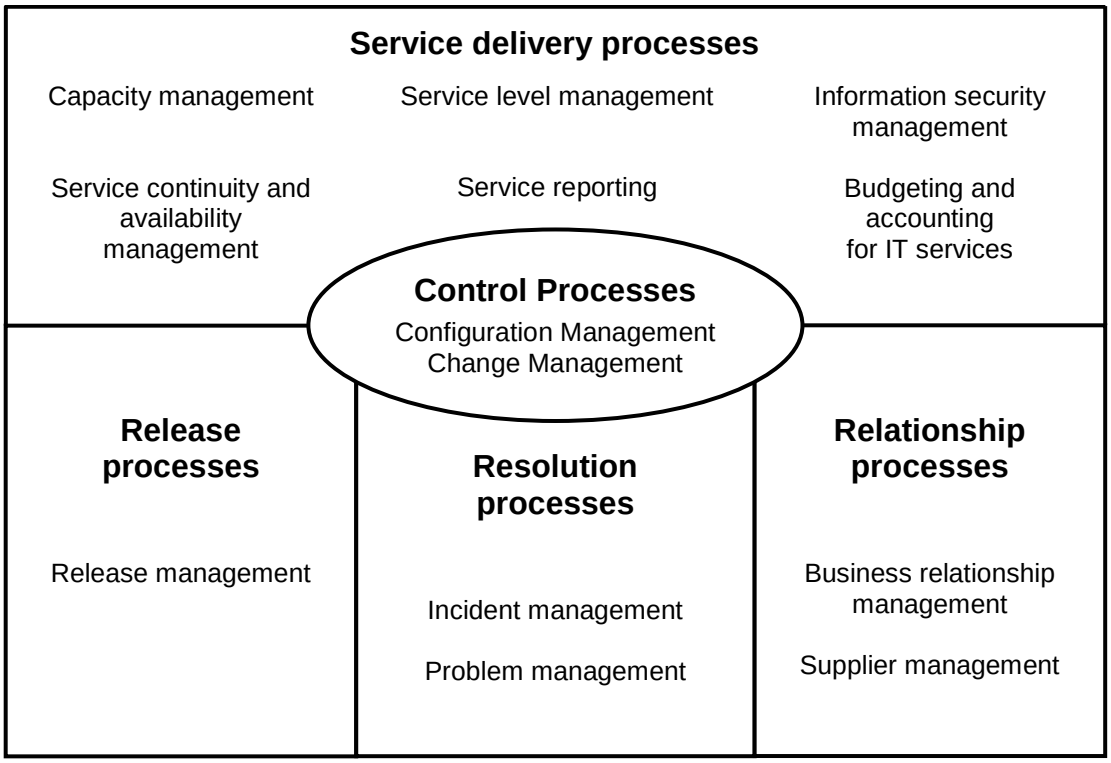


Figure D.1 – Service management processes
(ISO/IEC 20000-1:2005, Figure 1)

Table D.1 relates terminology and sections of IEC 80001-1 to those in ISO/IEC 20000-1 and ISO/IEC 20000-2. The numbers indicate the section in the subsequent standards.

Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005

IEC 80001-1	ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005
2.4 CONFIGURATION MANAGEMENT In IEC 80001-1, CONFIGURATION MANAGEMENT is a PROCESS that stores in the CMDB.	**2.5 configuration management database** The CMDB is the database used for configuration management. [ISO/IEC 20000-1:2005]
2.7 EVENT MANAGEMENT The nature of events is not defined in 80001-1. They relate to both the IT-NETWORK and the MEDICAL DEVICE	**2.7 incident** Incident and problem both relate to events that are managed by EVENT MANAGEMENT in IEC 80001-1. [ISO/IEC 20000-1:2005]
2.21 RESPONSIBILITY AGREEMENT An agreement between e.g. suppliers, manufacturers, service provider, system integrator and the RESPONSIBLE ORGANIZATION	**2.13 service level agreement (SLA);** **2.14 service management** Defines the relation between owner of an IT network and the service provider. [ISO/IEC 20000-1:2005]
2.22 RESPONSIBLE ORGANIZATION	**2.15 service provider** The RESPONSIBLE ORGANIZATION shall certify the IT-NETWORK service provider as part of its policy. [ISO/IEC 20000-1:2005]
2.29 RISK MANAGEMENT FILE	**2.9 record; 2.3 change record; 2.11 request for change** element(s) of the RISK MANAGEMENT FILE **2.5 configuration management database (CMDB)** element of the RISK MANAGEMENT FILE (asset description). NOTE The RISK MANAGEMENT FILE can be stored in a database that includes the CMDB. [ISO/IEC 20000-1:2005]
3.3 TOP MANAGEMENT responsibilities	**3.1 Management responsibility** Both standards address senior management responsibilities. ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005 leave more organizational freedom.
3.4 MEDICAL IT-NETWORK RISK MANAGER The RISK manager is responsible for the RISK MANAGEMENT PROCESS.	**3.1 Management responsibility** RISK MANAGEMENT is not specifically assigned as a task for management. **6.6.7 Documents and records** Records should be analyzed. In IEC 80001-1, this is the responsibility of the MEDICAL IT-NETWORK RISK MANAGER. [ISO/IEC 20000-2:2005]
3.5 MEDICAL DEVICE manufacturer(s); **3.6 Providers of other Information Technology** These sections specify information to be provided via the suppliers to the RESPONSIBLE ORGANIZATION	**7.1 Relationship process – general** **6.6.5 Security and availability of information** [ISO/IEC 20000-2:2005] **7.3 Supplier management** Both standards require relationships to be formalized via contract. Sections 6.6.5 and 7.3 relate to suppliers of components of the MEDICAL IT-NETWORK.
4.2.1 Policy for RISK MANAGEMENT for incorporating MEDICAL DEVICES	**3.1 Management responsibility**
4.2.2 RISK MANAGEMENT PROCESS Covers SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY	**6.6.3 security risk assessment practices** [ISO/IEC 20000-2:2005] Security is a subset of the KEY PROPERTIES of a MEDICAL IT-NETWORK. IEC 80001-1 provides the general RISK MANAGEMENT PROCESS for the IT-NETWORK.

Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005 *(continued)*

IEC 80001-1	ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005
4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation	**4.1 Plan service management (Plan);** **4.4.2 Management of improvements;** **5.1 Topics for consideration** ISO/IEC 20000 can include RISK MANAGEMENT. IEC 80001-1 defines the requirements to service management for MEDICAL IT-NETWORKS.
4.3.2 RISK-relevant asset description	**6.6.2 Identifying and classifying information assets** The scope should include all KEY PROPERTIES
4.3.3 MEDICAL IT-NETWORK documentation This section specifies information relating to the RISK MANAGEMENT PROCESS.	**4.1.1 Scope of service management; 6.6.2 Identifying and classifying information asset** The content of the information has overlap with 4.3.3 of IEC 80001-1.
4.3.4 RESPONSIBILITY AGREEMENT	**7.3 Supplier management (1st paragraph)** Both sections aim to clarify the intentions of collaboration to all relevant stakeholders.
4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK	**6.6.3 Security risk assessment practices** Security is a subset of the KEY PROPERTIES of a MEDICAL IT-NETWORK. IEC 80001-1 provides the general RISK MANAGEMENT PROCESS for the IT-NETWORK.
4.4.4 RISK CONTROL	**9.1.5 Configuration verification and audit; 9.2.1 Planning and implementation** ISO/IEC 20000 covers a broad scope of items that require VERIFICATION. VERIFICATION of RISK CONTROL measures is elaborated in IEC 80001-1.
4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT	**9 Control processes; 10 Release process** Change and configuration management as well as release and go-live are covered in Clauses 9 and 10. Clause 4 of IEC 80001-1 describes the RISK MANAGEMENT activities as included in these PROCESSES.
4.5.2.3 MEDICAL IT-NETWORK projects Major changes need a project to assess RISK prior to implementing change.	**9.2.1 Planning and implementation** ISO/IEC 20000 indicates all changes to be planned before implementation. IEC 80001-1 requires all changes to be risk managed which includes planning.
4.5.3 Go-live	**9.2.1 Planning and implementation; 10.1.6 Release verification and acceptance** IEC 80001-1 assigns the responsibility for sign-off to the MEDICAL IT-NETWORK RISK MANAGER.
4.6.1 Monitoring	**10.1.8 Roll-out, distribution and installation; 10.1.9 Post release and roll-out** Monitoring can relate to both organizational or technical RISK CONTROL measures.
5.1 Document control procedure	**3.2 Documentation requirements**
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE	**5.2 Change records; 6.6.7 Documents and records; 10.1.7 Documentation**

Bibliography

[1] IEC 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*

[2] IEC 61907:2009, *Communication network dependability engineering*

[3] IEC 62304:2006, *Medical device software – Software life-cycle processes*

[4] ISO 14971:2007, *Medical devices – Application of risk management to medical devices*

[5] ISO/IEC 15026-2: —[2)], *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*

[6] ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT security*

[7] ISO 16484-2:2004, *Building automation and control systems (BACS) – Part 2: Hardware*

[8] ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

[9] ISO/IEC 20000-1:2005, *Information technology – Service management – Part 1: Specification*

[10] ISO/IEC 20000-2:2005, *Information technology – Service management – Part 2: Code of practice*

[11] ISO 31000:2009, *Risk management – Principles and guidelines*

[12] GHTF/SG1/N29R16:2005, *Information Document Concerning the. Definition of the Term "Medical Device"*. Global Harmonization Task Force (GHTF) – Study Group 1 (SG1)

_____

2) To be published.