IEC/TR 80001-2-4

Edition 1.0 2012-11

TECHNICAL REPORT

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

IEC/TR 80001-2-4:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 80001-2-4

Edition 1.0 2012-11

TECHNICAL REPORT

Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE T

ICS 11.040.01; 35.240.80

ISBN 978-2-83220-525-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD..3
INTRODUCTION..5
1 Scope..7
1.1 Purpose..7
1.2 HEALTHCARE DELIVERY ORGANIZATION..7
1.3 Field of application..7
1.4 Prerequisites..7
2 Normative references..8
3 Terms and definitions..8
4 RESPONSIBLE ORGANIZATION..12
4.1 TOP MANAGEMENT responsibilities..12
4.2 Small RESPONSIBLE ORGANIZATION – points to consider..13
4.3 Large RESPONSIBLE ORGANIZATION – points to consider..14
5 RISK MANAGEMENT implementation steps..14
5.1 Overview..14
5.2 Determine the clinical context within which the healthcare provision is made..14
5.3 Establish underlying RISK framework..14
5.4 Determining and understanding a MEDICAL IT-NETWORK..15
5.4.1 Performing a RISK ASSESSMENT..15
5.4.2 MEDICAL IT-NETWORK configuration..16
5.4.3 Development status of MEDICAL IT-NETWORK..18
5.4.4 Manufacturer identification..18
5.4.5 External IT and bio-medical engineering support..19
6 RESPONSIBILITY AGREEMENTS..19
Annex A (informative) MEDICAL IT-NETWORK configuration examples..20
Bibliography..24

Figure A.1 – Standalone MEDICAL IT-NETWORK outside the scope of IEC 80001-1..21
Figure A.2 – Standalone MEDICAL IT-NETWORK..22
Figure A.3 – Collaborative MEDICAL IT-NETWORK..22
Figure A.4 – Centralized MEDICAL IT-NETWORK..23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international 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.

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

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

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
62A/818/DTR	62A/835/RVC

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

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

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

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

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC 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.

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

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

INTRODUCTION

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

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

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

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

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

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

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

- a small organization could be a doctor's practice with:
  - a few clinicians, or
  - with many clinicians, a consolidated IT function and a highly centralised governance structure
- a large organization could be:
  - a multi-hospital conglomerate, or
  - an organisation with distributed clinics and a mixture of in-house and outsourced clinical and IT governance.

Small organisations may also find the guidance identified under large organisation relevant.

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

– including the RISK MANAGEMENT PROCESSES in the existing management PROCESSES, for example the organization's Quality Management System;

– ensuring that the internal audit schedule includes the RISK MANAGEMENT PROCESSES;

– making sure RISK MANAGEMENT training is included on induction of new staff and provided to existing staff; and

– ensuring RISK MANAGEMENT is undertaken for both new work and changes to existing MEDICAL IT-NETWORKS.

Having established a RISK MANAGEMENT framework, the RESPONSIBLE ORGANIZATION will be ready to undertake a detailed RISK ASSESSMENT (see IEC/TR 80001-2-1 [1]).

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

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

1 Scope

1.1 Purpose

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

1.2 HEALTHCARE DELIVERY ORGANIZATION

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

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

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

1.3 Field of application

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

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

1.4 Prerequisites

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

- RISK MANAGEMENT policy and PROCESSES are in place;
- probability, severity, and RISK acceptability scales are specified; and
- MEDICAL IT-NETWORKS are well defined.

2 Normative references

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

IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities.*

3 Terms and definitions

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

3.1
ACCOMPANYING DOCUMENT
a document accompanying a MEDICAL DEVICE or an accessory and containing information for the RESPONSIBLE ORGANIZATION or OPERATOR, particularly regarding SAFETY

Note 1 to entry: Adapted from IEC 60601-1:2005, definition 3.4.

[SOURCE: IEC 80001-1:2010, 2.1]

3.2
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 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclauses 9.2 (change management) and 10.1 (release management).

[SOURCE: IEC 80001-1:2010, 2.2]

3.3
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 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclause 9.1.

[SOURCE: IEC 80001-1:2010, 2.4]

3.4
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 to entry: Security, when mentioned in this technical report, should be taken to include DATA AND SYSTEMS SECURITY.

Note 2 to entry: 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.

[SOURCE: IEC 80001-1:2010, 2.5]

3.5
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, 2.6]

3.6
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 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclauses 8.2 (incident management) and 8.3 (problem management).

[SOURCE: IEC 80001-1:2010, 2.7]

3.7
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 1 to entry: Adapted from ISO 14971:2007, definition 2.2.

[SOURCE: IEC 80001-1:2010, 2.8]

3.8
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, 2.9]

3.9
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD(s)

[SOURCE ISO 14971:2007, 2.4]

3.10
HEALTHCARE DELIVERY ORGANIZATION
one or more **RESPONSIBLE ORGANISATIONS**

Note 1 to entry: Within this technical report, HEALTHCARE DELIVERY ORGANIZATIONS are considered to be professional health organisations including hospitals, doctors' offices, community care homes and clinics.

3.11
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 to entry: Adapted from IEC 61907:2009, definition 3.1.1.

Note 2 to entry: 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.

[SOURCE: IEC 80001-1:2010, 2.12]

3.12
KEY PROPERTIES
three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, 2.13]

3.13
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 to entry: 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 to entry: 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 to entry);
- 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 to entry: 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 to entry: 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’.

[SOURCE: IEC 80001-1:2010, 2.14]

3.14
MEDICAL IT-NETWORK
an IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, 2.16]

3.15
MEDICAL IT-NETWORK RISK MANAGER
person accountable for RISK MANAGEMENT of a MEDICAL IT-NETWORK

[SOURCE: IEC 80001-1:2010, 2.17]

3.16
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, 2.18]

3.17
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

Note 1 to entry: The term "activities" covers use of resources.

[SOURCE: IEC 80001-1:2010, 2.19]

3.18
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

Note 1 to entry: This agreement can be a legal document, e.g. a contract.

[SOURCE: IEC 80001-1:2010, 2.21]

3.19
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry: The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

Note 2 to entry: Adapted from IEC 60601-1:2005 definition 3.101.

[SOURCE: IEC 80001-1:2010, 2.22]

3.20
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, 2.23]

3.21
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, 2.24]

3.22
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, 2.25]

3.23
RISK CONTROL

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

[SOURCE: IEC 80001-1:2010, 2.26]

3.24
RISK EVALUATION

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

[SOURCE: IEC 80001-1:2010, 2.27]

3.25
RISK MANAGEMENT

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

[SOURCE: IEC 80001-1:2010, 2.28]

3.26
RISK MANAGEMENT FILE

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

[SOURCE: IEC 80001-1:2010, 2.29]

3.27
SAFETY

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

Note 1 to entry: Adapted from ISO 14971:2007, definition 2.24.

[SOURCE: IEC 80001-1:2010, 2.30]

3.28
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 1 to entry: Adapted from ISO 9000:2005, definition 3.2.7.

[SOURCE: IEC 80001-1:2010, 2.31]

4 RESPONSIBLE ORGANIZATION

4.1 TOP MANAGEMENT responsibilities

This subclause refers to the duties which are placed by IEC 80001-1 on the organization's TOP MANAGEMENT and covers the need for explicit policies setting out IEC 80001-1 compliance.

It is good practice for the TOP MANAGEMENT to appoint a sufficiently independent function to oversee the effective operation of RISK MANAGEMENT practices in the organization. The steps described in this report will generally be executed by a team of individuals within the RESPONSIBLE ORGANIZATION. It is recommended to have representation from multiple departments, including IT, biomedical engineering, clinical, and RISK MANAGEMENT. The makeup of the team should align with existing structures within the organization. This can include consideration of patient SAFETY and network security. Senior clinicians should be included in the creation of this function and thereafter advise on the clinical impact of IT-NETWORK related HAZARDS as part of a RISK ASSESSMENT. Suitable links to the organization's teams responsible for clinical governance or clinical accountability should also be put in place.

TOP MANAGEMENT needs to ensure the following functions are done:

- define and document the organization's RISK MANAGEMENT policy. This policy will need to address the KEY PROPERTIES;
- create and disseminate suitable RISK MANAGEMENT PROCESSES. These PROCESSES can be linked to the RESPONSIBLE ORGANIZATION's clinical SAFETY management system, its quality management system or its enterprise RISK MANAGEMENT system, where these exist;
- establish RISK acceptability criteria to determine which RISKS are tolerable to the organization. The criteria will take into account relevant:
  - regulations (e.g. EU Directives);
  - international standards;
  - national standards;
  - regional standards; and
  - professional (e.g. clinical) guidelines
- ensure that a staged approach is taken to the deployment and use of MEDICAL IT-NETWORKS such that the RISK MANAGEMENT PROCESSES can be efficiently and effectively applied, consistent with the complexity of the MEDICAL IT-NETWORK being deployed. This approach should require TOP MANAGEMENT to sign off each stage; and
- review the suitability of the RISK MANAGEMENT PROCESSES at planned, regular intervals to ensure the continuing EFFECTIVENESS of the RISK MANAGEMENT PROCESSES and document any decisions and actions taken.

Both large and small organizations should commence their IEC 80001-1 implementation by opening a MEDICAL IT-NETWORK RISK MANAGEMENT FILE which should act as a focus for all of the organization's activities in this area. The MEDICAL IT-NETWORK RISK MANAGEMENT FILE can be used as a means to demonstrate the organization's compliance with the requirements of IEC 80001-1 as part of an audit activity.

4.2 Small RESPONSIBLE ORGANIZATION – points to consider

When evaluating TOP MANAGEMENT functions, a small organization should consider the following points:

- Do we have any systems which interface with MEDICAL DEVICES? Is IEC 80001-1 applicable to us at this moment in time? Do we have future plans for integrating MEDICAL DEVICES into our IT infrastructure?
- Can we safely phase our compliance plans over a longer period of time, thereby reducing the immediate burden on resources?
- Are there any similar RESPONSIBLE ORGANIZATIONS in the area with whom we could share resources and jointly establish IEC 80001-1 compliance? Do we know of similar RESPONSIBLE ORGANIZATIONS who are already compliant and would share their experiences?
- How do we establish an accurate inventory for IT operations? Do we have a proper design for our IT-NETWORKS and any exiting MEDICAL IT-NETWORKS? Where does the boundary exist between MEDICAL IT-NETWORK and our routine IT systems?
- Do we have a formal PROCESS to make these compliance decisions? Do we have a suitable repository, for example a quality management system, in which we can incorporate the RISK MANAGEMENT PROCESSES? How are we going to prepare such PROCESSES?

- Have we an existing staff member (manager or administrator) who can assume the additional responsibilities of MEDICAL IT-NETWORK RISK MANAGER? How do we get our staff suitably trained in RISK MANAGEMENT?

4.3 Large RESPONSIBLE ORGANIZATION – points to consider

When evaluating TOP MANAGEMENT functions, a large organization should consider the following points in addition to the points identified for a small organization above:

- Where does RISK MANAGEMENT responsibility sit within our organization? Who should own the RISK MANAGEMENT policy? How is clinical governance related?
- How do the RISK MANAGEMENT PROCESSES fit into the organization's quality management system? Where will the RISK MANAGEMENT PROCESSES and policy sit?
- How can RISK MANAGEMENT PROCESS be divided into manageable sub-PROCESSES and how should these sub-PROCESSES be co-ordinated?
- Do we need a specific IEC 80001-1 compliance project? Do we need to appoint a project manager and establish a project team?
- What are our IT support arrangements? Which suppliers are impacted by these requirements? Have we communicated supplier responsibilities properly?

5 RISK MANAGEMENT implementation steps

5.1 Overview

This subclause looks at the RISK MANAGEMENT framework and prerequisite work to be undertaken by the RESPONSIBLE ORGANIZATION before it embarks on the detailed RISK ASSESSMENT of a new or changing MEDICAL IT-NETWORK.

The three steps proposed in this document to implement IEC 80001-1, are:

- determine the clinical context within which the healthcare provision is made (see 5.2);
- establish an underlying RISK MANAGEMENT framework (see 5.3); and
- determine and understand existing MEDICAL IT-NETWORK(S) (see 5.4).

These three steps are explored in greater detail in the following subclauses.

5.2 Determine the clinical context within which the healthcare provision is made

The RESPONSIBLE ORGANIZATION must establish a clear understanding of the purpose of the organization from a clinical perspective.

In deriving this understanding the RESPONSIBLE ORGANIZATION could consider the following:

- the clinical needs of patients the organization provides services for;
- the nature of the clinical services provided by the organization and the PROCESSES involved with each of those clinical services; and
- clinical staffing and competencies.

5.3 Establish underlying RISK framework

There is a requirement for the RESPONSIBLE ORGANIZATION to define a RISK MANAGEMENT framework and to put PROCESSES in place before commencing a detailed RISK ASSESSMENT.

A RESPONSIBLE ORGANIZATION should consider what PROCESSES are needed to support the RISK MANAGEMENT activities. For example, these PROCESSES need to be commensurate with the size of organization, the clinical context and the level of IT operations.

In determining the extent of the PROCESSES to be developed, or existing PROCESSES to be updated, the organization should ensure that the areas identified in IEC 80001-1 are addressed as a minimum. These areas include:

- RISK MANAGEMENT (IEC 80001-1:2010, subclauses 4.2.2 and 4.4);
- CHANGE-RELEASE MANAGEMENT (IEC 80001-1:2010, subclause 4.5.1);
- CONFIGURATION MANAGEMENT (IEC 80001-1:2010, subclause 4.5.1);
- RISK MANAGEMENT planning (IEC 80001-1, subclauses 4.3.5 and 4.5.2.3);
- go-live (IEC 80001-1:2010, subclause 4.5.3);
- monitoring (IEC 80001-1:2010, subclause 4.6.1); and
- EVENT MANAGEMENT (IEC 80001-1:2010, subclause 4.6.2).

In formulating the PROCESSES that govern the RISK MANAGEMENT work there are some principles which will help to guide and keep a clear focus on the needs of the RESPONSIBLE ORGANIZATION including:

- **Free from additional RISK**: The work should not itself introduce additional RISK, for example by disrupting clinicians and over burdening them whilst they are responsible for delivering care to patients.
- **Light touch**: The RISK MANAGEMENT controls should avoid overly bureaucratic PROCESSES and be commensurate to the level of RISK identified as part of a subsequent RISK ASSESSMENT.
- **Ownership**: Has the RESPONSIBLE ORGANIZATION assigned suitable personnel to assess and own the RISKS? For example, clinicians own the clinical PROCESSES and are therefore well placed to assess the severity of HARM. They should be consulted regularly to ratify the RISK ASSESSMENT decisions and conclusions.
- **Consistent**: RISK MANAGEMENT activities should sit comfortably alongside clinical governance measures in the RESPONSIBLE ORGANIZATION and align with relevant national professional clinical standards and regulatory/legal requirements.
- **Net RISK**: The introduction of a new MEDICAL IT-NETWORK will be a trade-off between RISKS; it will help remove or mitigate and the inherent RISKS that the new technology brings. In some circumstances, for example capital investment, it might be incumbent on the RESPONSIBLE ORGANIZATION to demonstrate that the introduction of a new system will have a net reduction in RISK to the patient and the organization. This demonstration will require the RESPONSIBLE ORGANIZATION to assess both the old and the new systems in accordance with the RISK MANAGEMENT framework.

5.4 Determining and understanding a MEDICAL IT-NETWORK

5.4.1 Performing a RISK ASSESSMENT

Performing a RISK ASSESSMENT requires a detailed understanding of the way in which the MEDICAL IT-NETWORK delivers its services. The RESPONSIBLE ORGANIZATION must form a clear understanding of each MEDICAL IT-NETWORK, its boundary, its interfaces, what data flows across and within them and how that information is used.

Within the context of this document, a MEDICAL IT-NETWORK can consist of:

- an individual, discrete MEDICAL DEVICE connected directly to the RESPONSIBLE ORGANIZATION'S IT-NETWORK;
- several discrete MEDICAL DEVICES connected directly to the RESPONSIBLE ORGANIZATION'S IT-NETWORK; or
- a self-contained MEDICAL IT-NETWORK which is connected in its entirety to the RESPONSIBLE ORGANIZATION'S IT-NETWORK.

In reviewing each MEDICAL IT-NETWORK the following aspects should be considered:

- the configuration of the MEDICAL IT-NETWORK including a clear definition of the equipment constituting the network and the functions they provide, the machine and human interfaces and what data is exchanged across these interfaces (described in 5.4.2);
- the development status of the MEDICAL IT-NETWORK (described in 5.4.3);
- who provides the equipment (described in 5.4.4); and
- what level of support is available (described in 5.4.5).

When undertaking the above, a large RESPONSIBLE ORGANIZATION should consider the following points:

- **Is there a logical candidate pilot?** Establishing a large and complex MEDICAL IT-NETWORK is quite difficult for any organization. A useful technique is the use of a pilot project to prove the new PROCESSES.
- **How do we identify the correct people to gather the information?** This question should be considered before gathering the information. Establishing a multi-disciplined team to answer the technical and clinical questions that will arise is best done from the outset. Contact arrangements can be put in place and agreements with line managers made, thereby preventing a loss of impetus later in the PROCESS.

5.4.2 MEDICAL IT-NETWORK configuration

5.4.2.1 Understanding of the components of the MEDICAL IT-NETWORK

A RESPONSIBLE ORGANIZATION will need to form a good understanding of the components of the MEDICAL IT-NETWORK and their interaction. For example, the actual MEDICAL DEVICE, all of the connected systems, the nature of their connectivity and interrelationship and the broader network services such as backup. Note that subclause 4.3.2 of IEC 80001-1:2010 requires an organization to establish a list of assets.

The effort required to gather the information will be proportionate to the complexity of the MEDICAL IT-NETWORK and how well it has been documented to date. The type of network can also require the RESPONSIBLE ORGANIZATION to work closely with other organizations.

In determining the configuration of a MEDICAL IT-NETWORK, the following views could be constructed; additional views may also be assembled as required:

- **Physical view**: a diagram including the MEDICAL DEVICE(S), other systems and key interfaces (both human and machine). This view should clearly show the boundary of the MEDICAL IT-NETWORK.
- **Data view**: a diagram showing the flow of clinical data around the MEDICAL IT-NETWORK, for example a data flow diagram.
- **PROCESS view**: This could be a list of services, provided by the MEDICAL IT-NETWORK and its associated MEDICAL DEVICES. A service could be a pathology result. It is important to understand the associated roles and tasks for the services provided.

The MEDICAL IT-NETWORK being considered, from the physical view, will fall into one of the following categories:

a) **Standalone**: the classic single-system/small number of users, small dedicated MEDICAL IT-NETWORK which a small RESPONSIBLE ORGANIZATION would typically use. This category would also apply to the type of small specialist MEDICAL IT-NETWORK found in highly specialist departments in a large RESPONSIBLE ORGANIZATION, which are segregated from the main site network (for example, in the pathology laboratory).

b) **Collaborative**: where two or more RESPONSIBLE ORGANIZATIONS link their relatively simple and discrete standalone systems within a broader interoperable context. It is recommended that the details of the collaborations are recorded in addition to the details for the simple standalone systems.

c) **Centralised**: a typical centralised MEDICAL IT-NETWORK would exist in a large hospital, where a central IT department manages the network and services associated with a number of clinical specialities. The specialities themselves have dedicated network services from this central provision and are given access to applications which support the administrative and potentially clinical areas of care delivery. These networks will invariably interface with MEDICAL DEVICES to some degree. The level of complexity of the MEDICAL IT-NETWORK is an order of magnitude greater than would be seen in a small RESPONSIBLE ORGANIZATION. Care should be taken to be clear about the separation between clinical domains as in the centralised context some common MEDICAL IT-NETWORK components will be shared across different MEDICAL IT-NETWORKS.

Examples for these configurations are presented in Annex A.

The purpose of establishing the physical view in terms of the above configurations is to ensure that an accurate model of the MEDICAL IT NETWORK is derived for the RISK ASSESSMENT, especially in terms of connected systems and associated interfaces. Whilst the nature of the configuration does not change the basic RISK ASSESSMENT PROCESS it will be helpful in determining the potential HAZARDS and HAZARDOUS SITUATIONS.

5.4.2.2 Small RESPONSIBLE ORGANIZATION – points to consider

For a small organization, the biggest threat here is becoming overwhelmed by the quantity of information being collated. It is therefore important to avoid over complication at this stage. There are a few simple questions which will help a small organization to understand the MEDICAL IT-NETWORK:

- **Do we have an asset register? How accurate is it?** The asset register is a useful starting point for identifying the equipment within a MEDICAL IT-NETWORK. It does, however, need to be accurate. If it is not, then there is a good chance that a portion of the MEDICAL IT-NETWORK will fall out of scope of the RISK ASSESSMENT and therefore compromise the SAFETY of the whole MEDICAL IT-NETWORK.
- **Can we supplement the asset register with markers to show MEDICAL DEVICES?** If possible, you should try to mark the asset register with an indicator for those MEDICAL DEVICES which make up part of the MEDICAL IT-NETWORK. This will make things easier to maintain and give considerable help when assessing the impact of changes to the MEDICAL IT-NETWORK.
- **What MEDICAL DEVICES do we have in our RESPONSIBLE ORGANIZATION?** MEDICAL DEVICES are labelled as such and should come with a Certificate of Conformance from the manufacturer together with an ACCOMPANYING DOCUMENT; do you have these? If you have issues in this area, suppliers' websites can carry this documentation. In addition, Regulatory Agencies provide useful databases covering current systems approvals.
- **What interfaces exist between the MEDICAL DEVICE and our broader system(s)?** Before you can progress to a RISK ASSESSMENT, you need a clear understanding of the clinical information passing to and from any MEDICAL DEVICE. Clearly, the starting point for this piece of work is an understanding of what is, or is not, a MEDICAL DEVICE.

5.4.2.3 Large RESPONSIBLE ORGANIZATION – points to consider

It is important before commencing this exercise in a large organization to differentiate between a regulated standalone MEDICAL DEVICE and a regulated MEDICAL DEVICE which interfaces with other systems via a network. It is important to remember that the focus of IEC 80001-1 is the MEDICAL IT-NETWORK, and whilst good practice would dictate that a RESPONSIBLE ORGANIZATION has good PROCESSES and inventory around controlling standalone MEDICAL DEVICES, the subject of this document is how to implement IEC 80001-1.

Establishing the configuration in a large organization will be a complex undertaking and the following points, in addition to those specified above for a small organization, should be considered:

- **What help can the specialist clinical function offer in establishing an accurate picture?** A good place to find out information on MEDICAL DEVICES in radiology is to ask the radiologists and associated clinical staff who use the systems on a daily basis. Specialist clinical users should be consulted within each MEDICAL IT-NETWORK domain to properly capture the regulatory picture and their knowledge of working practices and the equipment.

- **What help can the technical functions (IT and biomed) offer?** Many failure modes of a MEDICAL IT-NETWORK are technical in nature and require the expertise of technical functions to both identify failure modes as well as to evaluate the likelihood of the failure.
- **What help can the RISK MANAGEMENT function offer?** Although the interpretation of RISK is slightly different with respect to the quantification of HAZARDS and that generally used by project managers, those conversant with a RISK approach will be able to assist in ensuring RISKS are defined, documented and controlled.
- **What help can the RESPONSIBLE ORGANIZATION's clinical governance team provide?** A RESPONSIBLE ORGANIZATION should have a clinical governance and compliance team who will have a good perspective on the regulatory environment in the RESPONSIBLE ORGANIZATION.
- **Can we break up the MEDICAL DEVICES we have into associated clinical domains?** It is important to ensure that the organization captures the correct clinical context within which the MEDICAL DEVICE is operating. The MEDICAL IT-NETWORK configuration views benefit from simplification if the MEDICAL IT-NETWORKS can be separated into clustered interrelated clinical domains.
- **Do we have any common MEDICAL DEVICES which interact across the organization?** When gathering the configuration information, MEDICAL DEVICES which are operating across several clinical settings should be identified. The analysis of the MEDICAL DEVICES within an IT-NETWORK can be of use in the assessment of other IT-NETWORKS containing the same MEDICAL DEVICE.

5.4.3 Development status of MEDICAL IT-NETWORK

It is important that a RISK ASSESSMENT uses information which correctly reflects the current status of the MEDICAL IT-NETWORK, as this will significantly influence the approach taken to mitigate the RISKS. In defining the development status of a MEDICAL IT-NETWORK the following classifications should be considered:

- **Existing**: stable and unchanged baselined MEDICAL IT-NETWORK. The purpose of the RISK ASSESSMENT is to identify any inherent RISKS and establish the EFFECTIVENESS of any prevailing controls or mitigations associated with the deployed and operation of the MEDICAL IT-NETWORK.
- **Modification**: stable baselined MEDICAL IT-NETWORK onto which one or more changes are being introduced. The purpose of the assessment is to identify the impact of the changes and to examine their impact on existing RISK CONTROL measures.
- **Under development**: new or existing MEDICAL IT-NETWORK where components are substantially new. The purpose of the assessment is to identify any potential RISKS associated with the MEDICAL IT-NETWORK under development and to ensure that adequate controls or mitigations are implemented to ensure the RISKS are within the agreed acceptability criteria.

The RESPONSIBLE ORGANIZATION needs to consider the development status of a MEDICAL IT-NETWORK and make a reasoned judgement as to which status is relevant, along with a corresponding consideration of the RISK ASSESSMENT approach.

5.4.4 Manufacturer identification

Once the RESPONSIBLE ORGANIZATION has quantified its MEDICAL IT-NETWORKS, it is necessary to identify the manufacturers of the various components. Completion of this activity will ensure that all component manufacturers have been identified.

The responsibilities of manufacturers and providers are defined in subclauses 3.5 and 3.6 of IEC 80001-1:2010, respectively.

Points to consider for any size of organization:

- Is the manufacturer the same as the supplier?
- Do our procurement PROCESSES ensure the RESPONSIBLE ORGANIZATION gets access to any supporting information? This could be from the manufacturer or from the supplier if these are different organizations.
- Who can request information from a manufacturer / supplier?
- Who can commission (or compel if necessary) a manufacturer / supplier to take action to mitigate a RISK?
- What is the complexity of the supply chain, for example, the use of sub-contractors?

5.4.5 External IT and bio-medical engineering support

It is important that the RESPONSIBLE ORGANIZATION ensures proper RESPONSIBILITY AGREEMENTS are in place with external support organisations in order to ensure adequate support and mitigation of any identified RISKS associated with components of the MEDICAL IT-NETWORK (see Clause 6). In this section IT is related to the basic network components rather than the MEDICAL DEVICE.

In order to clarify the support model it is useful to consider how the service is operated and maintained. To do this a RESPONSIBLE ORGANIZATION will need to consider the following questions:

- Which organizations are responsible for providing support?
- Do we have support contracts in place with each of these organizations?
- Are we clear which services are delivered in support of the network and its components (for example, the range of basic support tasks like resetting forgotten passwords to provision of new desktop computers) under each contract?
- Is the support adequate for our current and potential future needs?

6 RESPONSIBILITY AGREEMENTS

IEC 80001-1:2010, subclause 3.2 states that "The overall responsibility for RISK MANAGEMENT for a MEDICAL IT-NETWORK shall stay within the RESPONSIBLE ORGANIZATION”. To fulfil this responsibility, the RESPONSIBLE ORGANIZATION will need the timely input of information from its manufacturers. Ensuring the availability of this material can be achieved through RESPONSIBILITY AGREEMENTS.

Annex A
(informative)

MEDICAL IT-NETWORK configuration examples

A.1 General

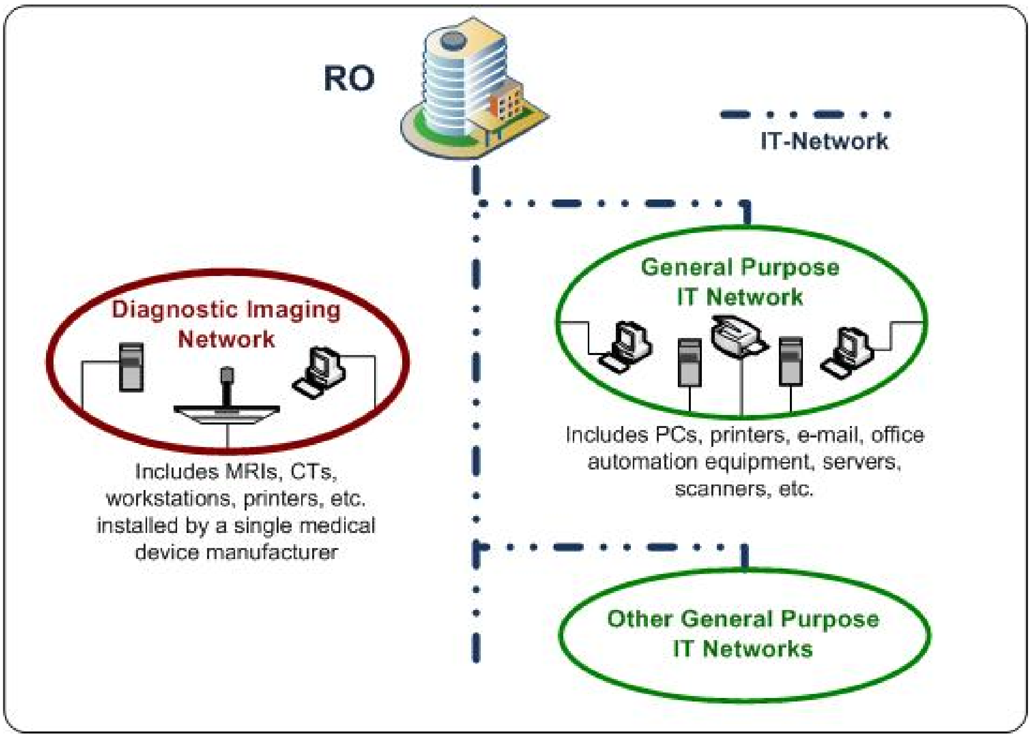
This annex presents four examples of MEDICAL IT-NETWORK configurations to support the text presented in 5.4.2. The first example (A.2) represents the system configurations 1a and 1b from Table C.1 of IEC 80001-1. The subsequent three examples (A.3 to A.5) are variations of system configuration 2b, from Table C.1 of IEC 80001-1:2010, with increasing complexity.

Within the following diagrams the MEDICAL DEVICE being connected to the general purpose IT NETWORK is shown as a collection of equipment on its own specific network. Equally the MEDICAL IT-NETWORK could consist of a one or more discrete MEDICAL DEVICES connected directly to the general purpose IT NETWORK.

A.2 Isolated network configuration

The example presented in Figure A.1 is comparable to system configuration 1 described in Table C.1 of IEC 80001-1:2010. As this example is not explicit as to whether the equipment is sourced from one or more MEDICAL DEVICE manufacturers, the interpretation is equally applicable to system configurations 1a and 1b.

The RESPONSIBLE ORGANIZATION is a provider of radiological services for a small community. The RESPONSIBLE ORGANIZATION is a single facility and is not associated with any other RESPONSIBLE ORGANIZATION. The RESPONSIBLE ORGANIZATION has two segregated networks operating within the facility. The first is a general purpose IT network that is used for the day-to-day business applications. The second is a MEDICAL DEVICE network comprising diagnostic imaging equipment that was installed by a single MEDICAL DEVICE manufacturer. As these networks are independent from one another, this configuration is outside the scope of IEC 80001-1.


RO
IT-Network
Diagnostic Imaging Network
Includes MRIs, CTs, workstations, printers, etc. installed by a single medical device manufacturer
General Purpose IT Network
Includes PCs, printers, e-mail, office automation equipment, servers, scanners, etc.
Other General Purpose IT Networks

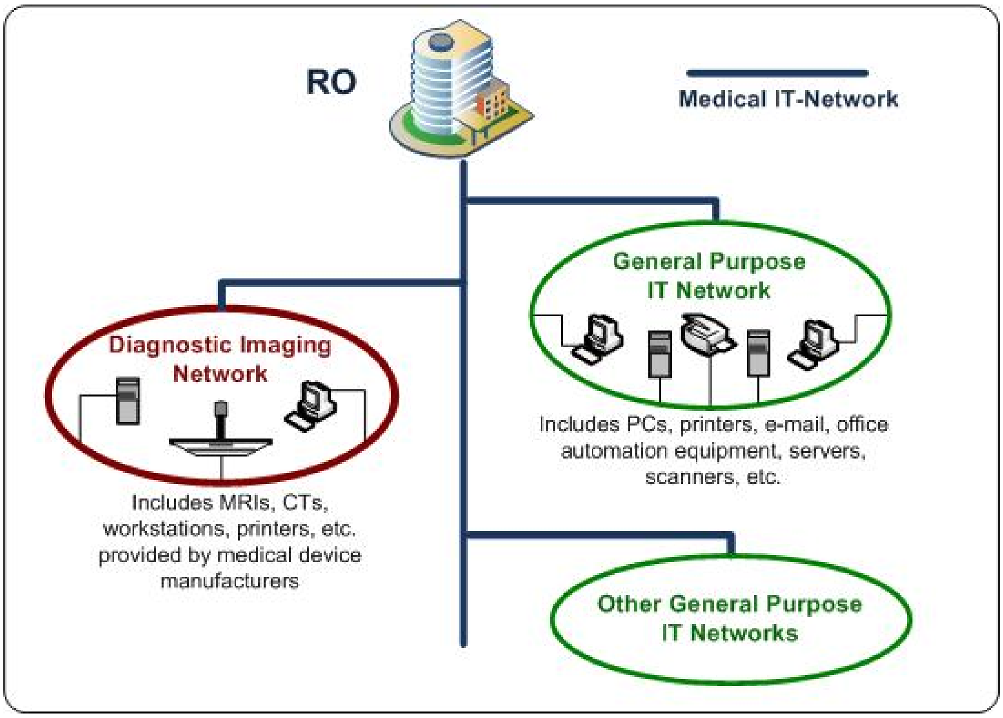
IEC 2306/12

Figure A.1 – Standalone MEDICAL IT-NETWORK outside the scope of IEC 80001-1

A.3 Standalone MEDICAL IT-NETWORK

The example presented in Figure A.2 is comparable to the system configuration 2b described in Table C.1 of IEC 80001-1:2010.

The RESPONSIBLE ORGANIZATION is a provider of radiological services for a small community. The RESPONSIBLE ORGANIZATION is a single facility and is not associated with any other RESPONSIBLE ORGANIZATION. The RESPONSIBLE ORGANIZATION has two networks operating within the facility. The first is a general purpose IT network that is used for the day-to-day business applications. The second is a MEDICAL DEVICE network comprising diagnostic imaging equipment that was purchased from MEDICAL DEVICE manufacturers. These two networks have been connected together to form a MEDICAL IT-NETWORK. The MEDICAL IT-NETWORK is used to store radiological images onto a server that was provided by the RESPONSIBLE ORGANIZATION. The radiological images that are stored can be retrieved and distributed via the general purpose IT network.


RO
Medical IT-Network
General Purpose IT Network
Includes PCs, printers, e-mail, office automation equipment, servers, scanners, etc.
Diagnostic Imaging Network
Includes MRIs, CTs, workstations, printers, etc. provided by medical device manufacturers
Other General Purpose IT Networks

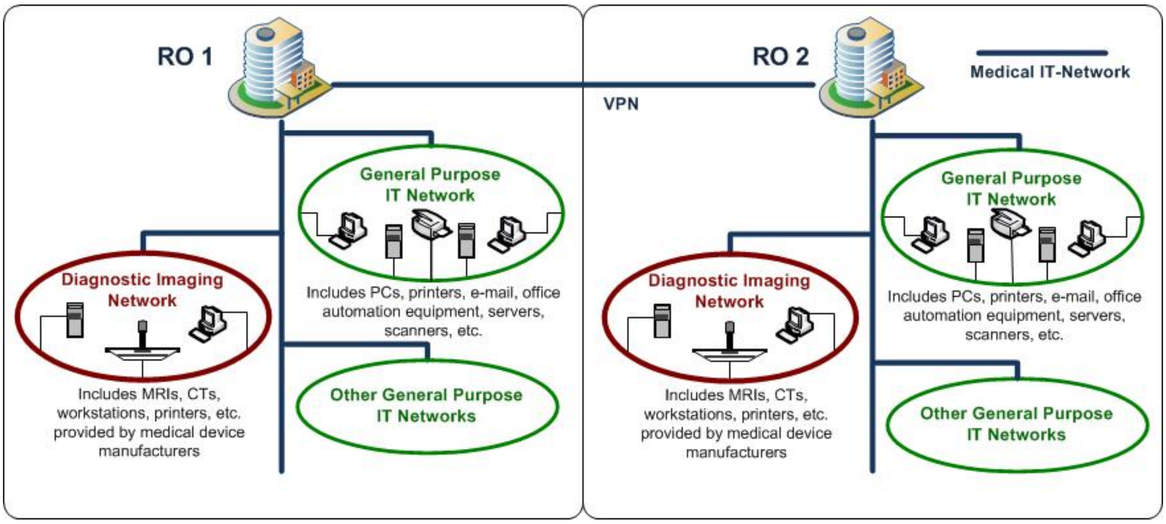
IEC 2307/12

Figure A.2 – Standalone MEDICAL IT-NETWORK

A.4 Collaborative MEDICAL IT- NETWORK

The example presented in Figure A.3 is extension to the system configuration 2b described in Table C.1 of IEC 80001-1:2010 and involves the interconnection of MEDICAL IT-NETWORKS across two facilities.

The RESPONSIBLE ORGANIZATION is a provider of radiological services for a small community, comprising two separate facilities. Each facility has a MEDICAL IT-NETWORK, as per the configuration defined in A.3, with the two connected together, in this example, via a Virtual Private Network (VPN).


RO 1
RO 2
VPN
Medical IT-Network
General Purpose IT Network
Includes PCs, printers, e-mail, office automation equipment, servers, scanners, etc.
Diagnostic Imaging Network
Includes MRIs, CTs, workstations, printers, etc. provided by medical device manufacturers
Other General Purpose IT Networks
General Purpose IT Network
Includes PCs, printers, e-mail, office automation equipment, servers, scanners, etc.
Diagnostic Imaging Network
Includes MRIs, CTs, workstations, printers, etc. provided by medical device manufacturers
Other General Purpose IT Networks

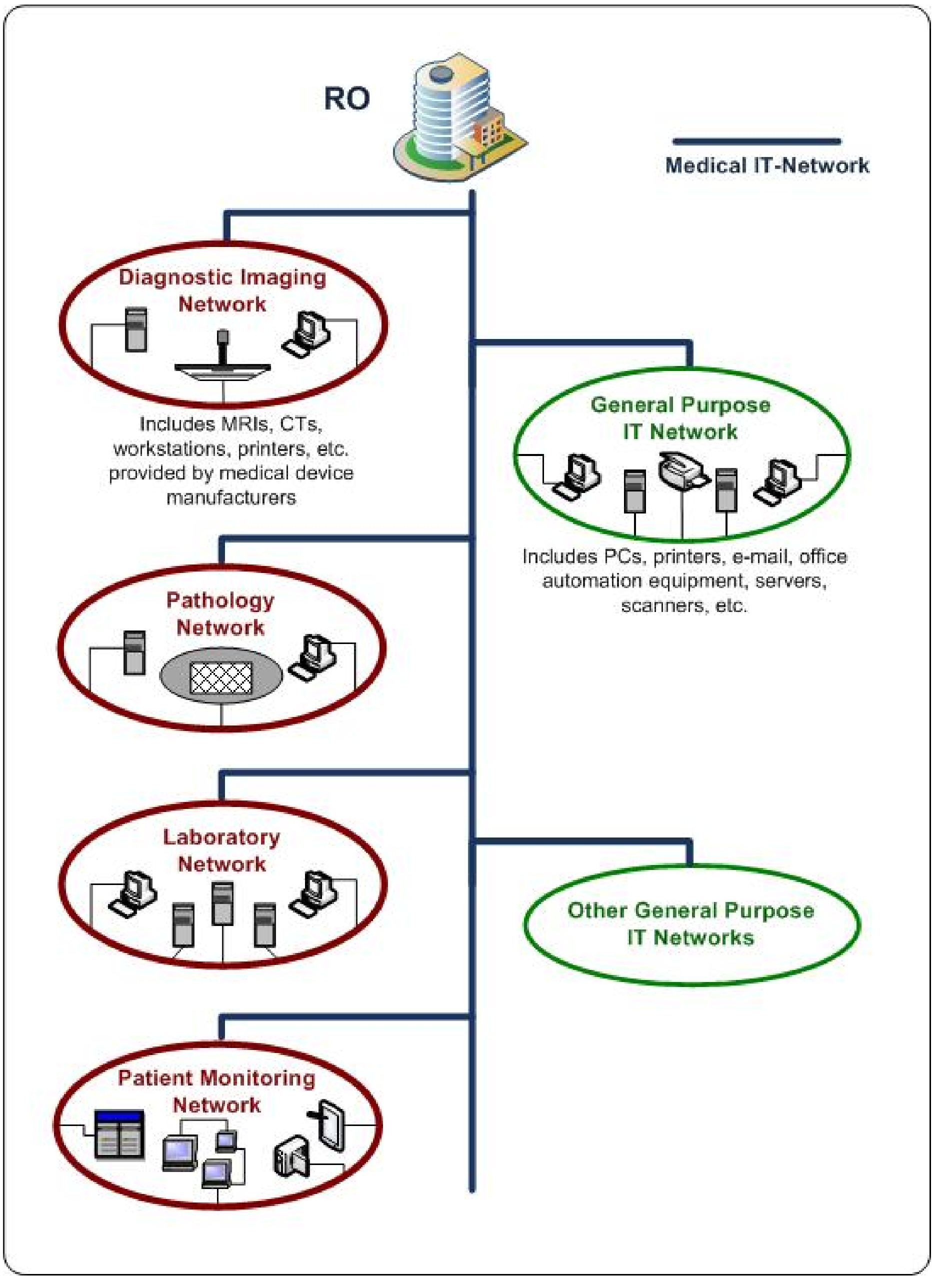
IEC 2308/12

Figure A.3 – Collaborative MEDICAL IT-NETWORK

A.5 Centralized MEDICAL IT-NETWORK

The example presented in Figure A.4 is an extension to the system configuration 2b described in Table C.1 of IEC 80001-1:2010 and involves the interconnection of multiple MEDICAL DEVICE networks within a single RESPONSIBLE ORGANIZATION.

The RESPONSIBLE ORGANIZATION is an acute care hospital serving a large community with a variety of services, for example, diagnostic imaging and pathology. The RESPONSIBLE ORGANIZATION has many MEDICAL DEVICES operating on segregated networks that were purchased and installed by the individual MEDICAL DEVICE manufacturers. However, these networks are connected to a single MEDICAL IT-NETWORK within the RESPONSIBLE ORGANIZATION.


RO
Medical IT-Network
Diagnostic Imaging Network
Includes MRIs, CTs, workstations, printers, etc. provided by medical device manufacturers
General Purpose IT Network
Includes PCs, printers, e-mail, office automation equipment, servers, scanners, etc.
Pathology Network
Laboratory Network
Other General Purpose IT Networks
Patient Monitoring Network

IEC 2309/12

Figure A.4 – Centralized MEDICAL IT-NETWORK

Bibliography

[1] IEC 80001-2-1:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples*

____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch