BS EN 80001-1:2011

BSI Standards Publication

Application of risk management for IT-networks incorporating medical devices

Part 1: Roles, responsibilities and activities

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 80001-1:2011. It is identical to IEC 80001-1:2010.

The UK participation in its preparation was entrusted by Technical Committee CH/62, Electrical Equipment in Medical Practice, to Subcommittee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice, with contribution from IST/35, Health Informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 57854 0

ICS 11.040.01; 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2011.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 80001-1

March 2011

ICS 11.040.01; 35.240.80

English version

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

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux - Partie 1: Fonctions, responsabilités et activités

(CEI 80001-1:2010)

Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten -

Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten

(IEC 80001-1:2010)

This European Standard was approved by CENELEC on 2011-02-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization

Comité Européen de Normalisation Electrotechnique

Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2011 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 80001-1:2011 E

Foreword

The text of document 62A/703/FDIS, future edition 1 of IEC 80001-1, prepared by SC 62A, Common aspects of electrical equipment used in medical practice, of IEC TC 62, Electrical equipment in medical practice, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 80001-1 on 2011-02-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-11-01

– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2014-02-01

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.

Endorsement notice

The text of the International Standard IEC 80001-1:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[1] IEC 60601-1:2005	NOTE	Harmonized as EN 60601-1:2006 (not modified).
[2] IEC 61907:2009	NOTE	Harmonized as EN 61907:2010 (not modified).
[3] IEC 62304:2006	NOTE	Harmonized as EN 62304:2006 (not modified).
[4] ISO 14971:2007	NOTE	Harmonized as EN ISO 14971:2009 (not modified).
[7] ISO 16484-2:2004	NOTE	Harmonized as EN ISO 16484-2:2004 (not modified).
[8] ISO 9000:2005	NOTE	Harmonized as EN ISO 9000:2005 (not modified).

CONTENTS

INTRODUCTION. 6
1 Scope 9
2 Terms and definitions 9
3 Roles and responsibilities 14
3.1 General 14
3.2 RESPONSIBLE ORGANIZATION 14
3.3 TOP MANAGEMENT responsibilities 15
3.4 MEDICAL IT-NETWORK RISK MANAGER 16
3.5 MEDICAL DEVICE manufacturer(s) 17
3.6 Providers of other information technology 18
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19
4.1 Overview 19
4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 20
4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20
4.2.2 RISK MANAGEMENT PROCESS 21
4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21
4.3.1 Overview 21
4.3.2 RISK-relevant asset description 22
4.3.3 MEDICAL IT-NETWORK documentation 22
4.3.4 RESPONSIBILITY AGREEMENT 22
4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK 24
4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24
4.4.1 Overview 24
4.4.2 RISK ANALYSIS 24
4.4.3 RISK EVALUATION 25
4.4.4 RISK CONTROL 25
4.4.5 RESIDUAL RISK evaluation and reporting 26
4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT 27
4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27
4.5.2 Decision on how to apply RISK MANAGEMENT 27
4.5.3 Go-live 29
4.6 Live network RISK MANAGEMENT 29
4.6.1 Monitoring 29
4.6.2 EVENT MANAGEMENT 29
5 Document control 30
5.1 Document control procedure 30
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30
Annex A (informative) Rationale 31
Annex B (informative) Overview of RISK MANAGEMENT relationships 35
Annex C (informative) Guidance on field of application 36
Annex D (informative) Relationship with ISO/IEC 20000-2:2005 *Information technology – Service management – Part 2: Code of practice* 38
Bibliography 42

Figure 1 – Illustration of TOP MANAGEMENT responsibilities. 16
Figure 2 – Overview of life cycle of MEDICAL IT-NETWORKS including RISK MANAGEMENT 20
Figure B.1 – Overview of roles and relationships 35
Figure D.1 – Service management processes 39

Table A.1 – Relationship between ISO 14971 and IEC 80001-1 33
Table C.1 – IT-NETWORK scenarios that can be encountered in a clinical environment. 36
Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005. 40

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.

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

---

1) Numbers in square brackets refer to the Bibliography.

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 3.6shall 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.

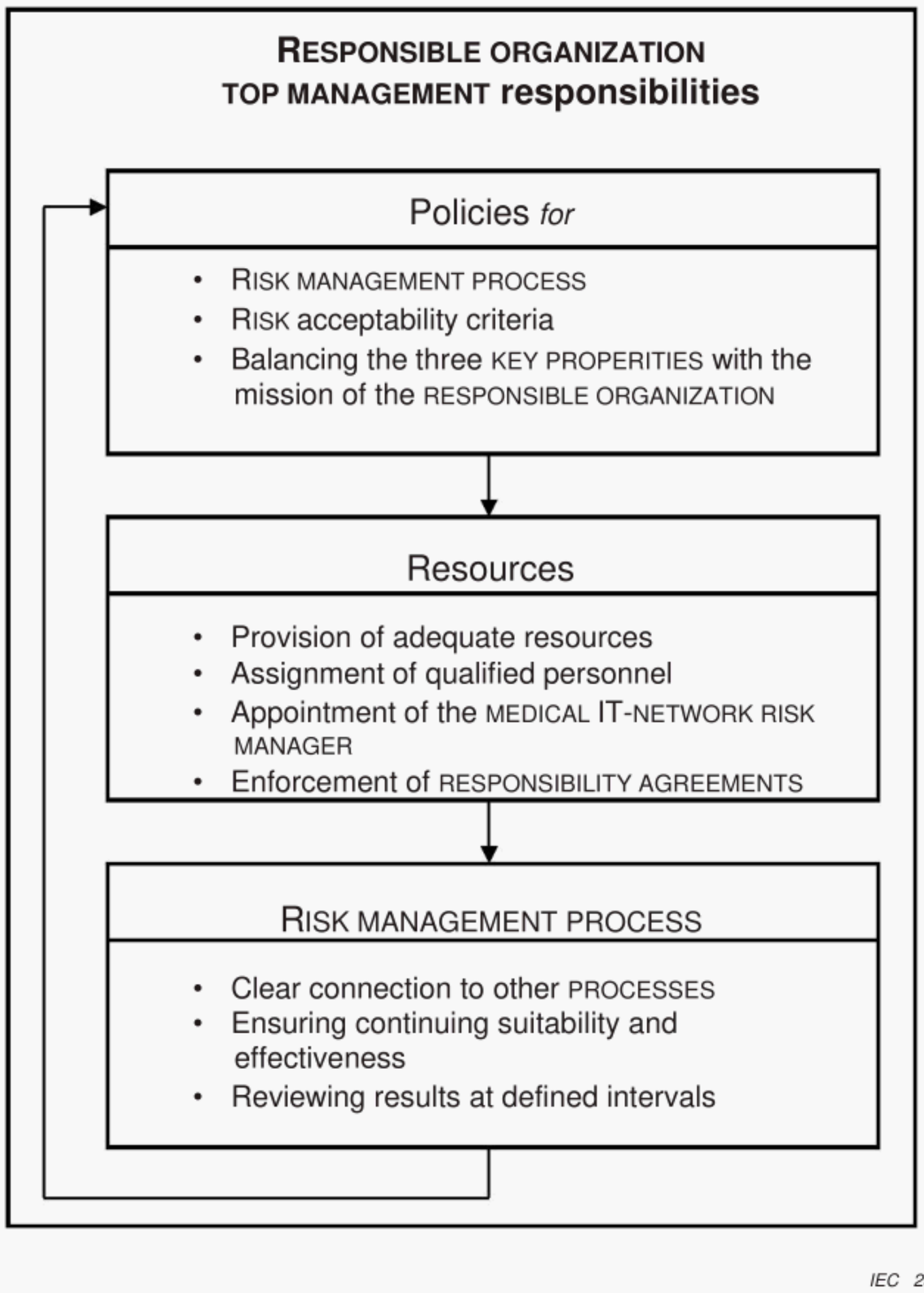


Figure 1 – Illustration of TOP MANAGEMENT responsibilities

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.

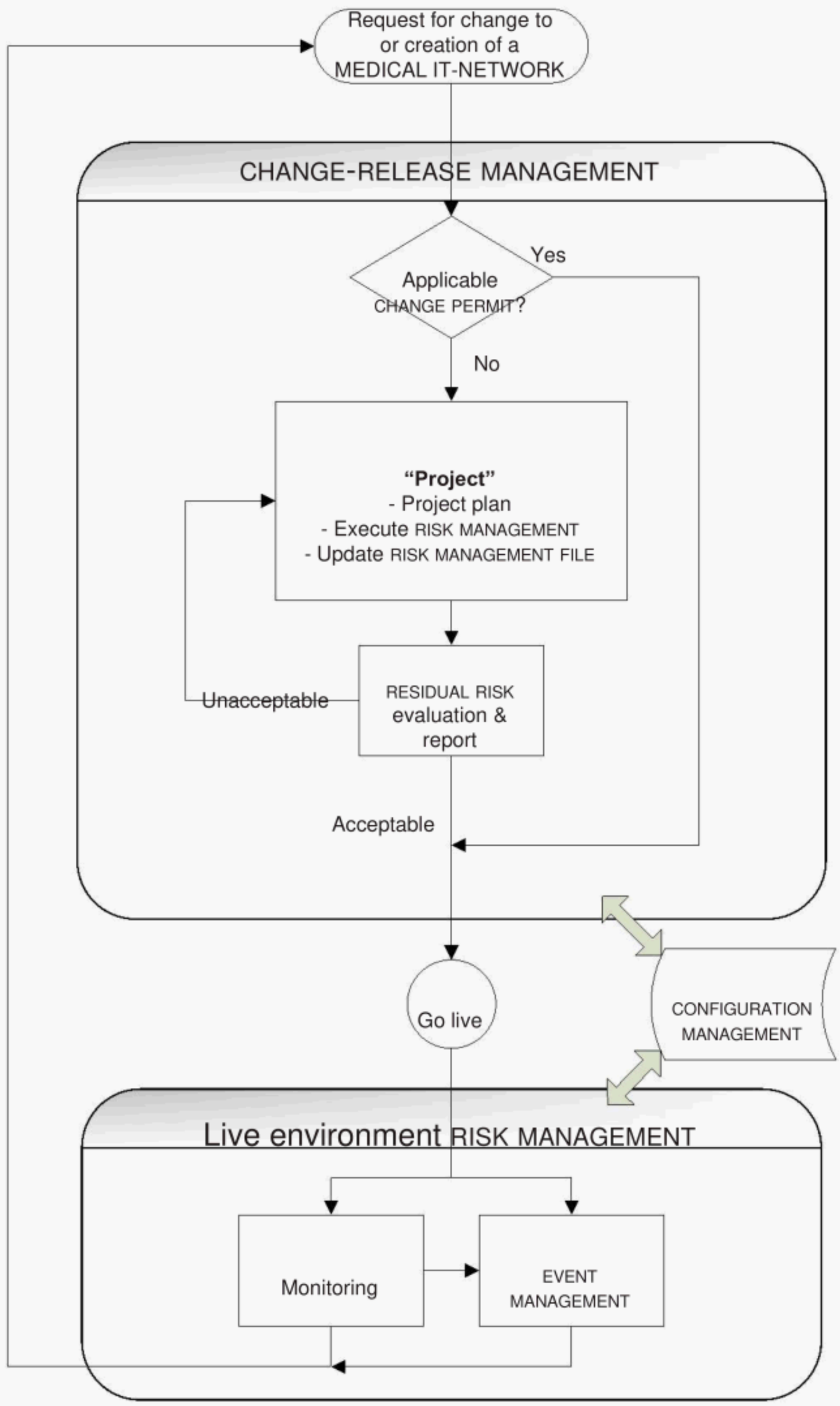
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS

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 4.3.2for 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.

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

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.

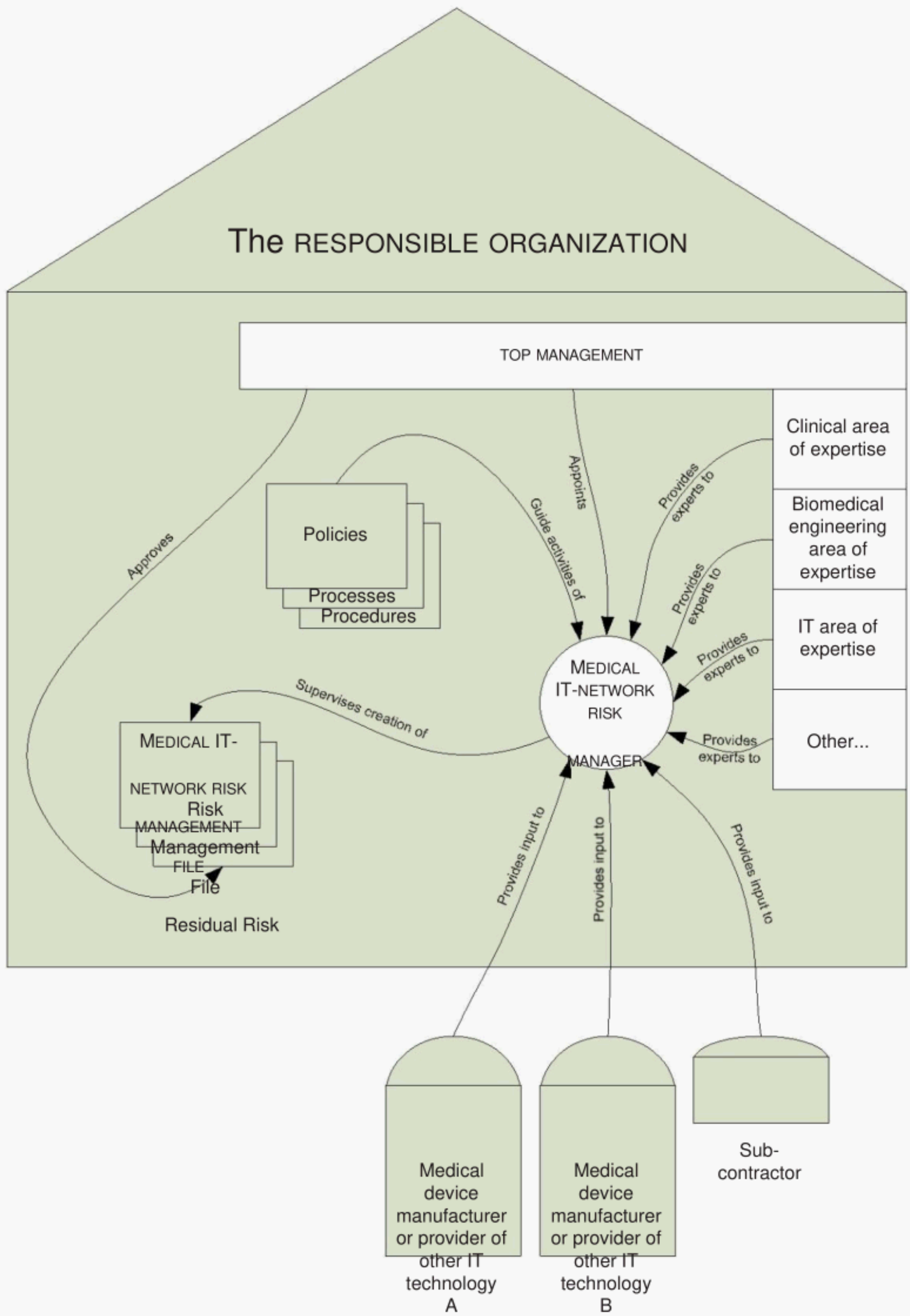


Figure B.1 – Overview of roles and relationships

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.

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.

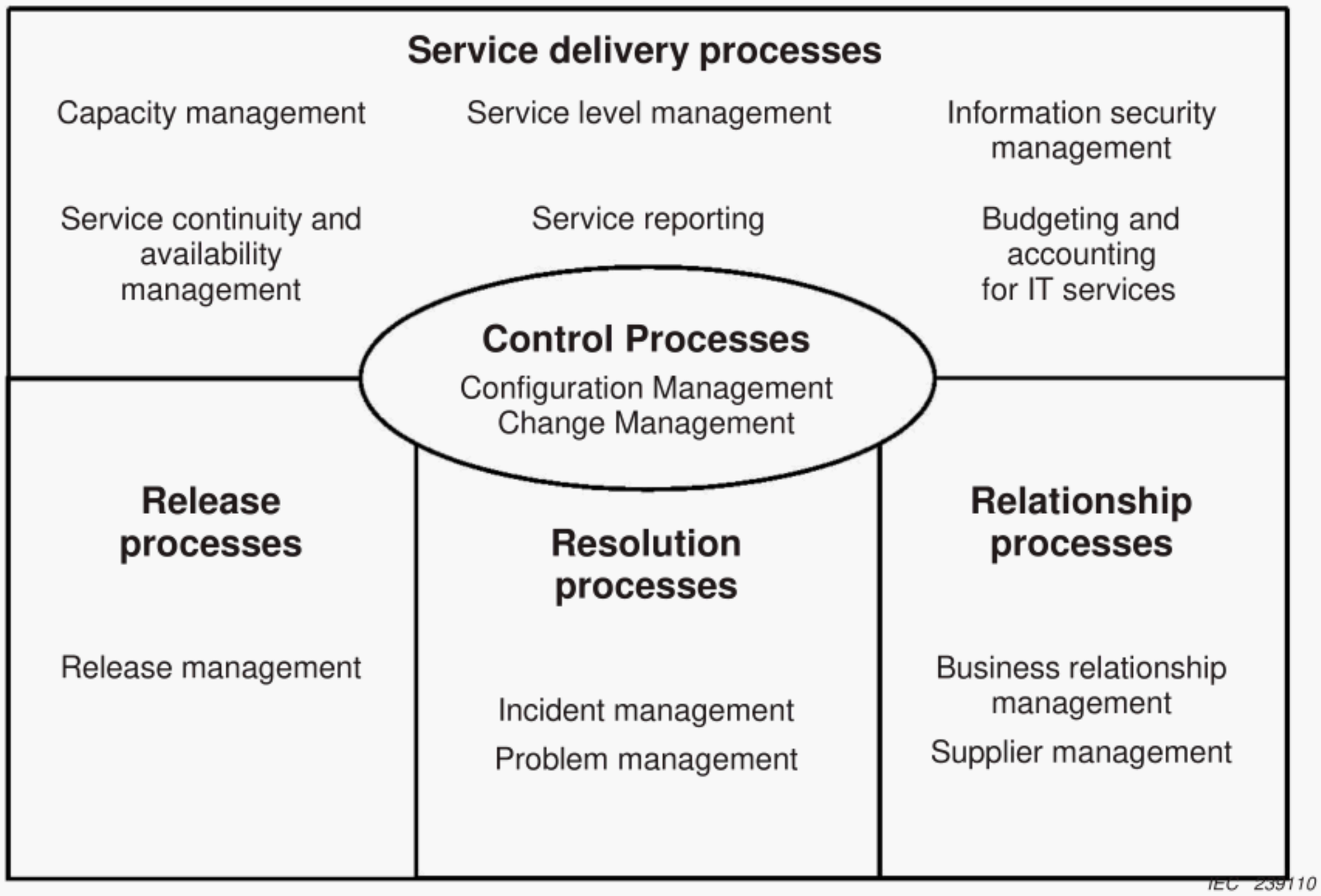


Figure D.1 – Service management processes
(ISO/IEC 20000-1:2005, Figure 1)

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.

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.

This page deliberately left blank

This page deliberately left blank

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With British Standards Online (BSOL) you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a BSI Subscribing Member.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a Multi-User Network Licence (MUNL) you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person
or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs
and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™