IEC 80001-1

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 80001-1

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 11.040.01; 35.240.80

ISBN 978-2-88912-221-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Roles, responsibilities and activities

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 80001-1 has been prepared by a joint working group of subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62*:* Electrical equipment in medical practice and ISO technical committee 215: Health informatics.

It is published as a double logo standard.

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

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

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

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

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

For the purposes of this standard:

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

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

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The '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

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 3.6 shall be defined.

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

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

NOTE The CONFIGURATION MANAGEMENT information can be included in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE either through explicit documentation or by reference, for example, to a live database.

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

3.2 RESPONSIBLE ORGANIZATION

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

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

Compliance is checked by assessment of the RESPONSIBLE ORGANIZATION.

3.3 TOP MANAGEMENT responsibilities

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

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

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

c) ensuring the provision of adequate resources;

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

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

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

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

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

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

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

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

i) maintenance of MEDICAL IT-NETWORKS; and

j) choice of and procurement of MEDICAL DEVICES.

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

k) MEDICAL IT-NETWORKS;

l) general IT activities;

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

EXAMPLE biomedical engineering, radiological engineering

n) the use of MEDICAL DEVICES; and

EXAMPLE experienced users from clinical departments

o) maintenance and technical support for MEDICAL DEVICES.

EXAMPLE biomedical engineering department

TOP MANAGEMENT shall ensure:

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

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

NOTE The TOP MANAGEMENT responsibilities are illustrated in Figure 1.

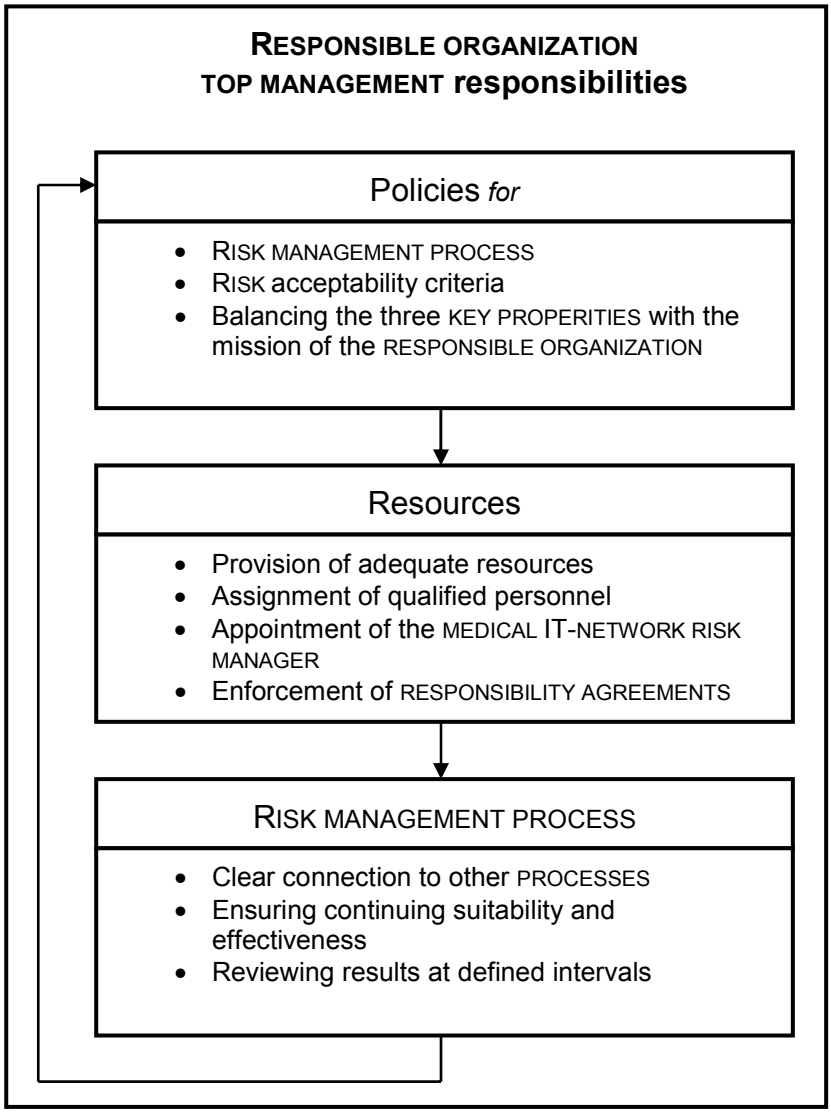


Figure 1 – Illustration of TOP MANAGEMENT responsibilities

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

3.4 MEDICAL IT-NETWORK RISK MANAGER

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

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

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

a) Overall management of the RISK MANAGEMENT PROCESS;

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

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

   1) MEDICAL DEVICE manufacturers;

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

   3) internal IT function and other facilities management functions;

   4) clinical users; and

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

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

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

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

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

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

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

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

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

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

Compliance is checked by assessment of the RESPONSIBLE ORGANIZATION.

3.5 MEDICAL DEVICE manufacturer(s)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.6 Providers of other information technology

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

a) infrastructure components;

b) infrastructure services;

c) client devices not being MEDICAL DEVICES;

d) servers;

e) application software; or

f) middleware.

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

g) technical descriptions and technical manuals;

h) required IT-NETWORK characteristics;

i) recommended product configurations;

j) known incompatibilities and restrictions;

k) operating requirements;

l) product corrective actions and recalls; and

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

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

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

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

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

Examples of supplementary information are:

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

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

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

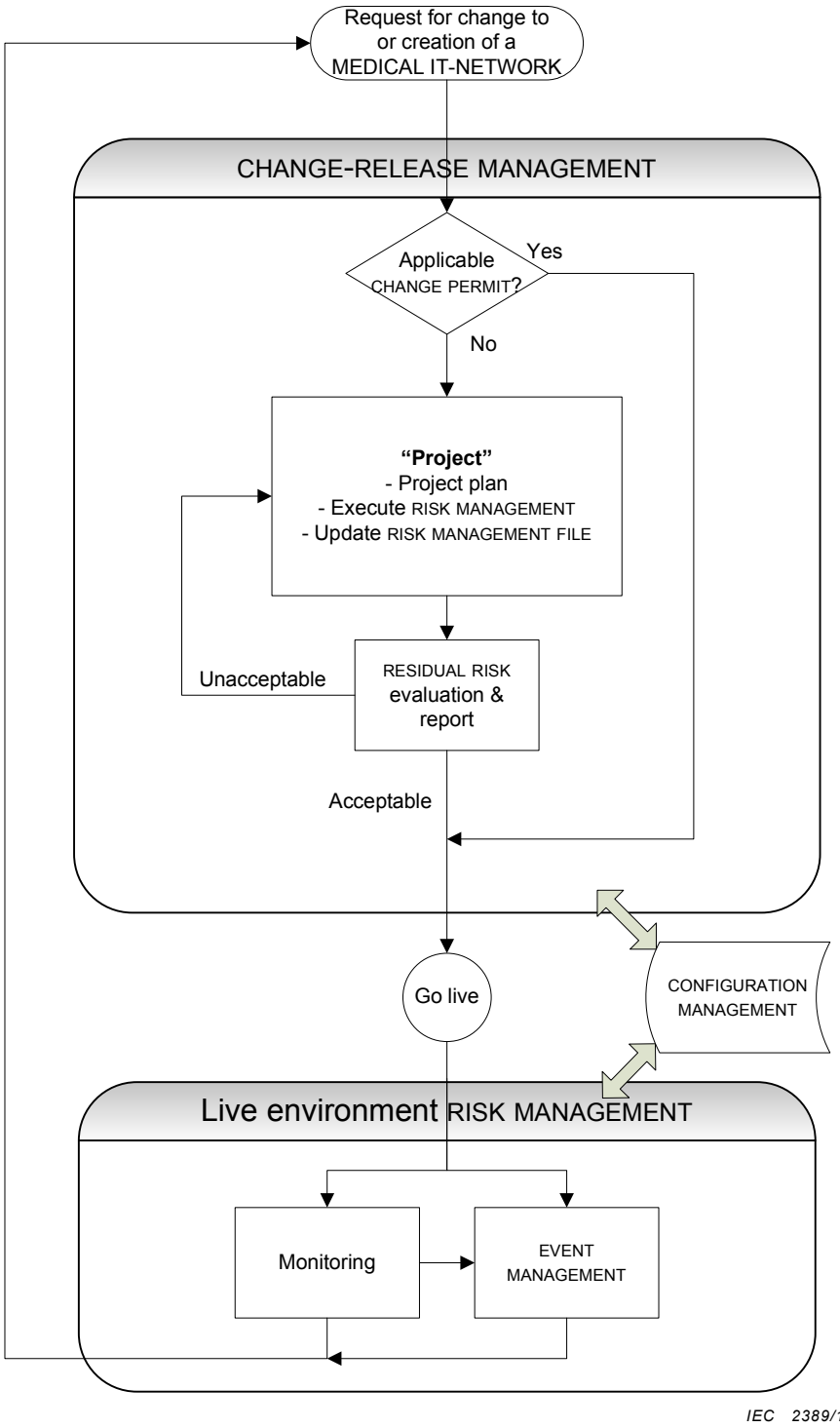
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS

4.1 Overview

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

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

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



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

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

4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT

4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES

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

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

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

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

   1) EVENT MANAGEMENT,

   2) CHANGE-RELEASE MANAGEMENT,

   3) CONFIGURATION MANAGEMENT, and

   4) monitoring.

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

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

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

4.2.2 RISK MANAGEMENT PROCESS

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

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

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

4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation

4.3.1 Overview

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

a) RISK-relevant asset description,

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

b) IT-NETWORK documentation, and

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

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

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

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

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

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

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

4.3.2 RISK-relevant asset description

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

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

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

c) CONFIGURATION MANAGEMENT information;

d) medical application software;

e) data about configuration of hardware and software;

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

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

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

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

4.3.3 MEDICAL IT-NETWORK documentation

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

a) physical and logical network configuration;

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

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

b) applied standards and conformance statements;

c) physical and logical client / server structure;

d) network security, reliability and data integrity;

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

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

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

4.3.4 RESPONSIBILITY AGREEMENT

Whenever a MEDICAL DEVICE is incorporated into an IT-NETWORK, or the configuration of such a connection is changed, the RESPONSIBLE ORGANIZATION shall determine the need for one or

more documented RESPONSIBILITY AGREEMENTS that define (e.g. by contract) the responsibilities of all relevant stakeholders.

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

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

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

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

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

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

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

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

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

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

NOTE 1 The manufacturer of a MEDICAL DEVICE is responsible for making available technical documentation on how to use the MEDICAL DEVICE'S interfaces to connect to an IT-NETWORK, provided that such a connection is intended by the manufacturer. There is no such obligation on the supplier of other equipment, and it might be necessary to make a specific arrangement to gain access to such technical documentation.

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

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

h) state:

- who is responsible for requesting such co-operation;
- who is responsible for responding to such requests; and
- what criteria will be used to judge the adequacy of such response.

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

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

4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK

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

a) a description of the MEDICAL IT-NETWORK, including:
   1) identified stakeholders within the RESPONSIBLE ORGANIZATION that shall be informed about HAZARDS to ensure their RISK awareness;
   2) the defined use and expected benefits of the MEDICAL IT-NETWORK;
   3) the reason for each MEDICAL DEVICE incorporation; and
   4) the use of each MEDICAL DEVICE, due to its incorporation into the MEDICAL IT-NETWORK that is not included in the manufacturer's INTENDED USE.

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

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

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

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

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

4.4 MEDICAL IT-NETWORK RISK MANAGEMENT

4.4.1 Overview

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

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

NOTE There is a single set of RISK MANAGEMENT documents per MEDICAL IT-NETWORK, because RISK CONTROL measures for any given project or change must not conflict with existing RISK CONTROL measures for the MEDICAL IT-NETWORK or with RISK CONTROL measures proposed by a concurrent project.

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

4.4.2 RISK ANALYSIS

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

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

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

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

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

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

4.4.3 RISK EVALUATION

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

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

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

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

4.4.4 RISK CONTROL

4.4.4.1 RISK CONTROL option analysis

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

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

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

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

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

NOTE 1 RISK CONTROL measures can include for example:

– instructions and constraints documented as a CHANGE PERMIT (see 2.3 and 4.5.2.2);

– network components;

– change of network configuration;

– organizational considerations; or

– changes to the incorporated MEDICAL DEVICES.

NOTE 2 For each RISK, the design should carefully consider where to best implement the control to ensure sustainability – for example, by changes to the MEDICAL IT-NETWORK or manufacturer-authorized changes to the MEDICAL DEVICE.

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

If, during RISK CONTROL option analysis, the RESPONSIBLE ORGANIZATION determines that required RISK reduction is not practicable, the RESPONSIBLE ORGANIZATION shall conduct and document a RISK/benefit analysis of the RESIDUAL RISK (see 4.4.5).

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

4.4.4.2 RISK CONTROL measures

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

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

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

4.4.4.3 Implementation of RISK CONTROL measures

The selected RISK CONTROL measures shall be implemented.

RISK CONTROL measures within the MEDICAL DEVICE should only be implemented by the MEDICAL DEVICE manufacturer or by the RESPONSIBLE ORGANIZATION following the instructions for use or with the documented permission of the MEDICAL DEVICE manufacturer.

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

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

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

4.4.4.4 VERIFICATION of RISK CONTROL measures

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

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

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

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

4.4.4.5 New RISKS arising from RISK CONTROL

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

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

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

4.4.5 RESIDUAL RISK evaluation and reporting

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

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

NOTE See 4.4.3 for RISK EVALUATION.

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

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

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

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

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

4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT

4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS

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

The MEDICAL IT-NETWORK RISK MANAGER shall ensure that a CHANGE-RELEASE MANAGEMENT PROCESS exists for the MEDICAL IT-NETWORK and that the PROCESS includes RISK MANAGEMENT.

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

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

A CONFIGURATION MANAGEMENT PROCESS shall be documented and applied to control the versions of the MEDICAL IT-NETWORK across all RISK MANAGEMENT PROCESSES during MEDICAL IT-NETWORK CHANGE-RELEASE MANAGEMENT.

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

4.5.2 Decision on how to apply RISK MANAGEMENT

4.5.2.1 Overview

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

The RESPONSIBLE ORGANIZATION shall consider the nature of the change to decide whether the requirements are met by an applicable CHANGE PERMIT. Where no applicable CHANGE PERMIT exists, a MEDICAL IT-NETWORK project shall be initiated.

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

4.5.2.2 CHANGE PERMITS

If the RESPONSIBLE ORGANISATION decides, as a result of RISK MANAGEMENT activities, that a specified type of routine change may be performed with acceptable RISK, subject to specified constraints, then the RESPONSIBLE ORGANISATION may define a CHANGE PERMIT which allows such routine changes and specifies the constraints.

NOTE 1 For example, a CHANGE PERMIT might allow varying the number of MEDICAL DEVICES of a specified type in a MEDICAL IT-NETWORK within a specified range.

NOTE 2 Provided that the changes performed always conform to the CHANGE PERMIT and its limitations, no CHANGE-RELEASE MANAGEMENT or RISK MANAGEMENT is needed each time the CHANGE PERMIT is used.

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

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

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

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

4.5.2.3 MEDICAL IT-NETWORK projects

The RESPONSIBLE ORGANIZATION shall establish and maintain a project plan for the incorporation of a new type of MEDICAL DEVICE into an IT-NETWORK, for change to the MEDICAL IT-NETWORK, for change to the MEDICAL DEVICES incorporated in the MEDICAL IT-NETWORK, for decommissioning of a MEDICAL DEVICE or MEDICAL IT-NETWORK, or any other activity that has the potential to introduce new RISK. The typical first project plan would be for development of a new MEDICAL IT-NETWORK. The project plan shall provide:

a) requirements for RISK MANAGEMENT activities including:
   1) activities to establish or update any RISK MANAGEMENT FILE documents needed as a result of this project, such as the RISK MANAGEMENT plan or other RISK MANAGEMENT documents;
   2) a plan to meet the requirements stated in the RISK MANAGEMENT plan for the affected MEDICAL IT-NETWORK(S); and
   3) activities for VERIFICATION of RISK CONTROL measures.

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

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

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

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

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

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

4.5.3 Go-live

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

The MEDICAL IT-NETWORK RISK MANAGER shall examine all project or change RESIDUAL RISK summaries to determine acceptability of RISK associated with interactions with recent or pending projects or changes (e.g., the incorporation of the MEDICAL DEVICE into an operational, evolving IT-NETWORK).

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

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

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

4.6 Live network RISK MANAGEMENT

4.6.1 Monitoring

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

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

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

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

c) information about the incorporated components;

d) information about similar MEDICAL IT-NETWORKS;

e) reported events; and

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

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

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

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

4.6.2 EVENT MANAGEMENT

The RESPONSIBLE ORGANIZATION shall establish EVENT MANAGEMENT to:

a) capture and document negative events;

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

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

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

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

5 Document control

5.1 Document control procedure

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

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

5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE

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

a) the RISK ANALYSIS;

b) the RISK EVALUATION;

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

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

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

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

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

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

Annex A
(informative)

Rationale

A.1 General

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

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

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

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

A.2 Clause 3 – Roles and responsibilities

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

The healthcare delivery organization that owns and utilizes the MEDICAL IT-NETWORK has overall responsibility for its functioning. It is the RESPONSIBLE ORGANIZATION. To ensure that RISK MANAGEMENT is properly addressed for the MEDICAL IT-NETWORK, the TOP MANAGEMENT of the RESPONSIBLE ORGANIZATION is required by this standard to establish policy, provide resources, assign qualified people and review the results of RISK MANAGEMENT activities. It is important that someone be assigned the responsibility for the execution of the RISK MANAGEMENT PROCESS for the MEDICAL IT-NETWORK. A primary responsibility of TOP MANAGEMENT is appointing a MEDICAL IT-NETWORK RISK MANAGER and ensuring that others in

the RESPONSIBLE ORGANIZATION co-operate with the MEDICAL IT-NETWORK RISK MANAGER to manage the RISK of incorporating MEDICAL DEVICES into IT-NETWORKS.

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

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

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

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

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

Subclause 4.2 – RESPONSIBLE ORGANIZATION RISK MANAGEMENT

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

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

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

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

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

Subclause 4.5 – CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT

Subclause 4.5 describes RISK MANAGEMENT activities that are required when changing a MEDICAL IT-NETWORK before it enters the live environment phase. This includes changing an existing MEDICAL IT-NETWORK as well as initially building a MEDICAL IT-NETWORK or turning a non-MEDICAL IT-NETWORK into a MEDICAL IT-NETWORK. In this stage, the traditional RISK MANAGEMENT activities occur in the context of a project. The MEDICAL IT-NETWORK RISK MANAGER is responsible for consolidating all project RISK MANAGEMENT activities into a single RISK MANAGEMENT FILE for the MEDICAL IT-NETWORK.

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

For activities that are performed frequently, it is desirable to avoid unnecessary repetition of RISK MANAGEMENT. This standard mentions CHANGE PERMITS as one way to do this. If RISK MANAGEMENT demonstrates that a routine change, for example adding a user, can be performed with acceptable RISK, subject to specified constraints (for example a limit on the

type and number of users), then the RESPONSIBLE ORGANISATION can define a CHANGE PERMIT which allows such routine changes and specifies the constraints.

Subclause 4.6 – Live Network RISK MANAGEMENT

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

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

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

Annex B
(informative)

Overview of RISK MANAGEMENT relationships

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

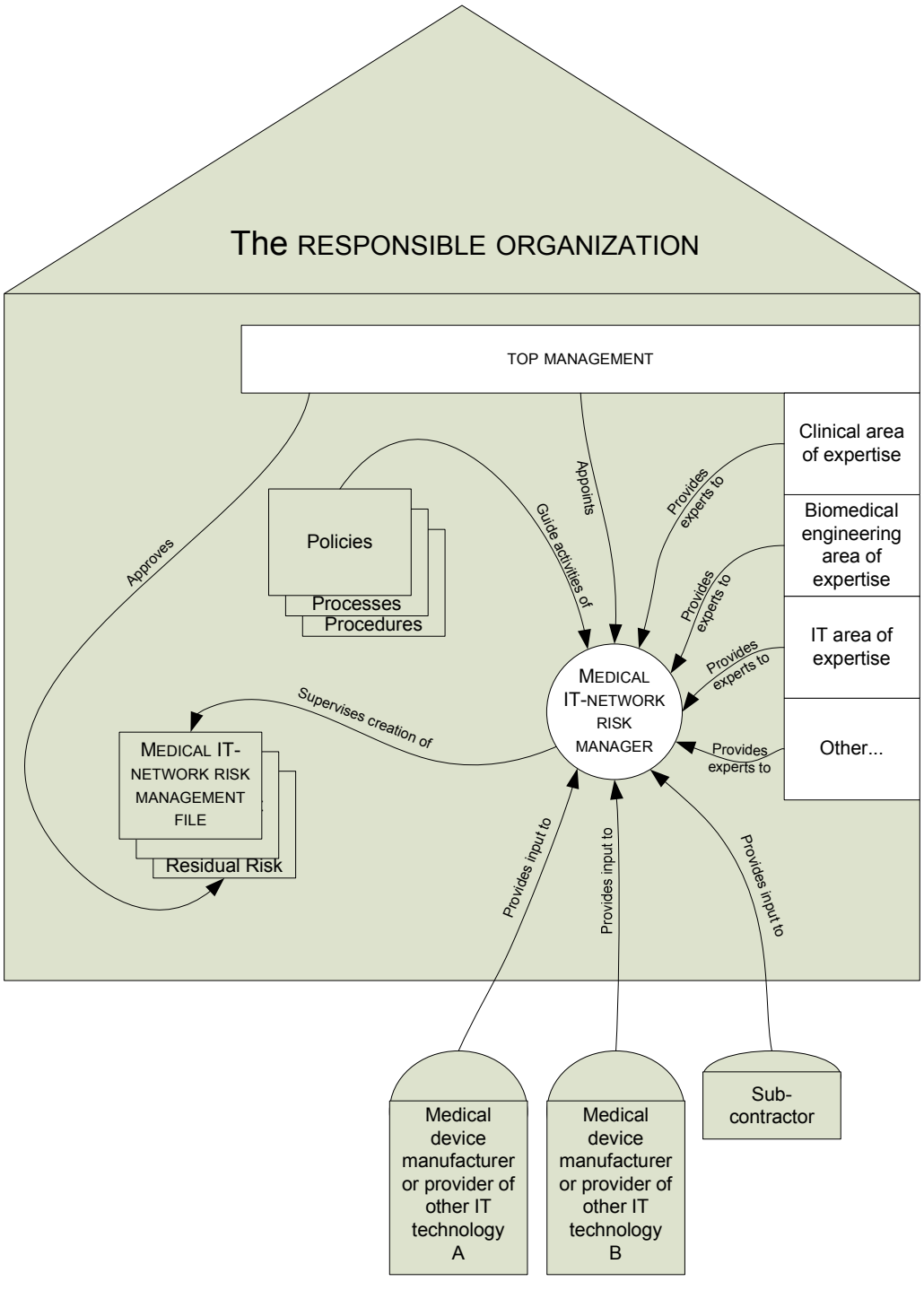


Figure B.1 – Overview of roles and relationships

Annex C
(informative)

Guidance on field of application

C.1 Overview

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

C.2 When to apply this standard

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

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

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

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

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

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

Annex D
(informative)

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

D.1 General

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

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

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

D.2 Terminology and definitions

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

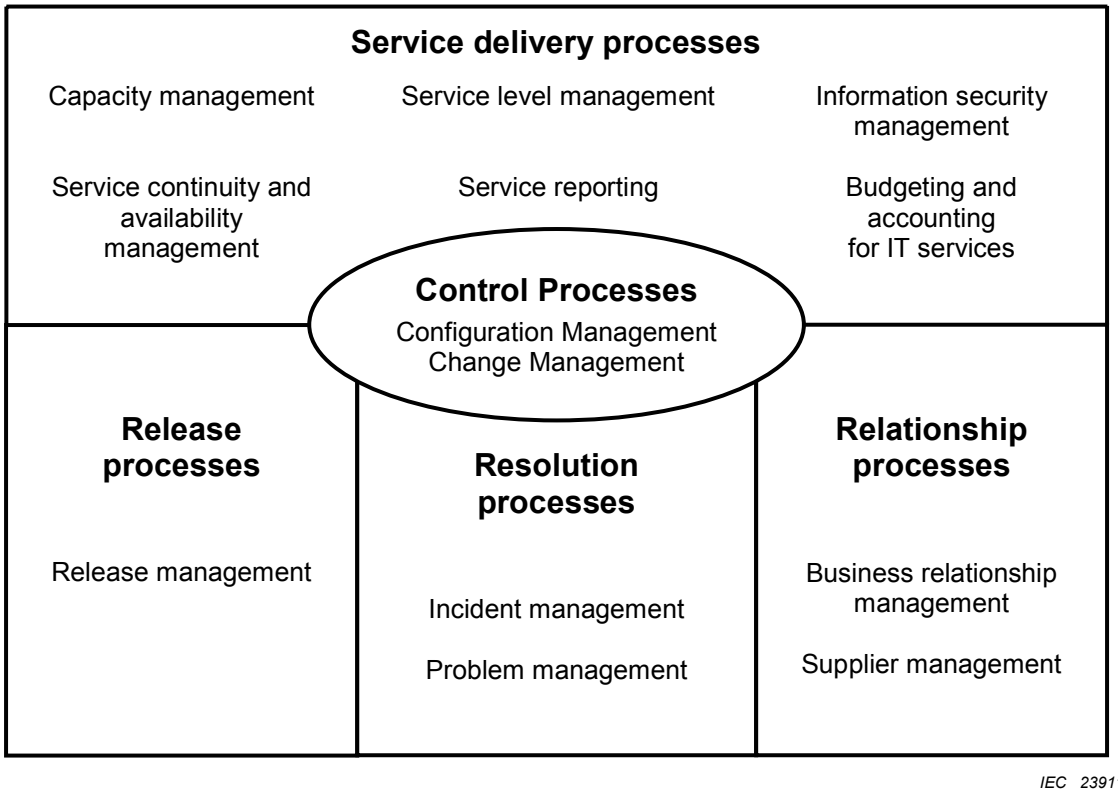


Figure D.1 – Service management processes
(ISO/IEC 20000-1:2005, Figure 1)

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

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

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

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

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

Bibliography

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

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

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

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

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

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

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

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

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

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

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

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

_____

2) To be published.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATION DE LA GESTION DES RISQUES AUX RÉSEAUX DES TECHNOLOGIES DE L'INFORMATION CONTENANT DES DISPOSITIFS MÉDICAUX –

Partie 1: Fonctions, responsabilités et activités

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 80001-1 a été établie par un groupe de travail mixte du sous-comité 62A: *Aspects généraux des équipements électriques utilisés en pratique médicale*, du comité d'études 62 de la CEI: Equipements électriques dans la pratique médicale, et du comité technique 215 de l'ISO: Informatique médicale.

La présente publication est une norme double logo.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
62A/703/FDIS	62A/718/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme. A l'ISO, la norme a été approuvée par 17 membres P sur 18 ayant voté.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Les termes définis à l'Article 2 de la présente norme sont imprimés en PETITES MAJUSCULES.

Pour les besoins de la présente norme:

- "devoir" mis au présent de l'indicatif signifie que la satisfaction à une exigence est obligatoire pour la conformité à la présente norme;
- "il convient/il est recommandé" signifie que la satisfaction à une exigence est recommandée mais n'est pas obligatoire pour la conformité à la présente norme;
- "pouvoir" mis au présent de l'indicatif est utilisé pour décrire un moyen admissible pour satisfaire à une exigence; et.
- "établir" signifie définir, documenter et mettre en application.

Une liste de toutes les parties de la série CEI 80001, publiées sous le titre général *Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

De plus en plus de DISPOSITIFS MÉDICAUX sont conçus afin d'échanger des informations électroniquement avec d'autres appareils de l'environnement utilisateur, y compris d'autres DISPOSITIFS MÉDICAUX. Ces informations sont fréquemment échangées par l'intermédiaire d'un réseau de technologies de l'information (RÉSEAU TI) également capable de transférer des données de nature plus générale.

Parallèlement, les RÉSEAUX TI se révèlent de plus en plus vitaux pour l'environnement clinique et doivent désormais supporter des trafics de plus en plus diversifiés, allant des données essentielles à la vie du PATIENT nécessitant une livraison et une réaction immédiates à des données générales relatives aux actions d'entreprise et aux courriels dont le contenu est potentiellement malveillant (ex. les virus).

Pour de nombreuses collectivités publiques, la conception et la production des DISPOSITIFS MÉDICAUX sont soumises à des réglementations et à des normes reconnues par les autorités de réglementation. En général, les autorités de réglementation accordent leur attention aux fabricants de DISPOSITIFS MÉDICAUX, en exigeant des caractéristiques de conception ainsi qu'un PROCÉSSUS documenté pour la conception et la fabrication. Les DISPOSITIFS MÉDICAUX ne peuvent pas être mis sur le marché de ces collectivités publiques s'il n'a pas été clairement établi que ces exigences ont été remplies.

L'utilisation des DISPOSITIFS MÉDICAUX par le personnel médical est également soumise à des réglementations. Les membres du personnel médical doivent être correctement formés et qualifiés, et sont de plus en plus sujets à des PROCESSUS spécifiques, conçus afin de protéger les PATIENTS d'un RISQUE inacceptable.

Par contre, l'incorporation des DISPOSITIFS MÉDICAUX au sein de RÉSEAUX TI dans l'environnement clinique est beaucoup moins réglementée. Il est stipulé dans la CEI 60601-1:2005 [1][1)] que les fabricants de DISPOSITIFS MÉDICAUX doivent fournir certaines informations dans les DOCUMENTS D'ACCOMPAGNEMENT si le DISPOSITIF MÉDICAL est destiné à être connecté à un RÉSEAU TI. Il existe également des normes relatives aux activités associées aux technologies de l'information telles que la planification, la conception ainsi que la maintenance des RÉSEAUX TI. C'est le cas par exemple de l'ISO 20000-1:2005 [9]. Cependant, avant la publication de la présente norme, il n'existait aucune norme indiquant la manière dont les DISPOSITIFS MÉDICAUX peuvent être connectés aux RÉSEAUX TI, y compris aux RÉSEAUX TI généraux, afin d'obtenir l'INTEROPÉRABILITÉ sans compromettre l'organisation et la délivrance des soins en termes de SÉCURITÉ, EFFICACITÉ, et de SÉCURITÉ DES DONNÉES ET DES SYSTÈMES.

Il subsiste un certain nombre de problèmes potentiels liés à l'incorporation des DISPOSITIFS MÉDICAUX au sein des RÉSEAUX TI, tels que:

– l'absence de prise en considération du RISQUE engendré par l'utilisation de réseaux TI durant l'évaluation du RISQUE clinique;
– l'absence de soutien des fabricants de DISPOSITIFS MÉDICAUX dans l'incorporation de leurs produits au sein des RÉSEAUX TI, (ex. l'indisponibilité ou l'inadéquation des informations fournies par le fabricant à l'OPERATEUR du RÉSEAU TI);
– le fonctionnement incorrect ou les performances altérées (ex. incompatibilité ou configuration incorrecte) résultant de l'association de DISPOSITIFS MÉDICAUX et d'autres appareils sur le même RÉSEAU TI;
– le fonctionnement incorrect résultant de l'association de LOGICIELS DE DISPOSITIFS MÉDICAUX et d'autres applications logicielles (ex. systèmes ouverts de messagerie électronique ou jeux sur ordinateur) au sein du même RÉSEAU TI;

---

1) Les chiffres entre crochets se réfèrent à la Bibliographie.

– l'absence de contrôles de sécurité sur de nombreux DISPOSITIFS MÉDICAUX; et
– le conflit entre le besoin de contrôle strict des modifications apportées aux DISPOSITIFS MÉDICAUX et le besoin d'une réaction rapide face à la menace des cyberattaques.

Lorsque ces problèmes se manifestent, des conséquences indésirables surviennent fréquemment.

La présente norme s'adresse aux ORGANISMES RESPONSABLES, aux fabricants de DISPOSITIFS MÉDICAUX, ainsi qu'aux fournisseurs en technologies de l'information.

La présente norme adopte les principes suivants en tant que base pour les sections normatives et informatives:

– L'incorporation ou la suppression d'un DISPOSITIF MÉDICAL ou autres composants dans un RÉSEAU TI est une tâche nécessitant la conception de l'action; ceci pourrait se révéler hors de contrôle du fabricant du DISPOSITIF MÉDICAL.
– Il est recommandé que la GESTION DES RISQUES soit utilisée avant qu'un DISPOSITIF MÉDICAL ne soit incorporé au sein d'un RÉSEAU TI, et pour toute modification durant le cycle de vie entier du RÉSEAU TI contenant le DISPOSITIF MÉDICAL, afin d'éviter les RISQUES inacceptables, y compris le RISQUE pouvant affecter les PATIENTS, résultant de l'incorporation du DISPOSITIF MÉDICAL au sein du RÉSEAU TI. Plusieurs critères rentrent en ligne de compte lors d'une décision relative au RISQUE comme la fiabilité, le coût ou l'impact sur la mission. Il convient qu'ils soient pris en compte lors de la détermination des RISQUES acceptables tout comme les exigences décrites dans la présente norme.
– Il convient que les aspects relatifs à la suppression, à la maintenance, au changement ou à la modification des appareils, des éléments ou des composants soient correctement abordés en plus de l'incorporation des DISPOSITIFS MÉDICAUX.
– Le fabricant d'un DISPOSITIF MÉDICAL est responsable de la GESTION DES RISQUES de ce DISPOSITIF MÉDICAL lors de sa conception, de son implémentation et de sa fabrication. La présente norme ne couvre pas le PROCESSUS DE GESTION DES RISQUES pour le DISPOSITIF MÉDICAL.
– Le fabricant d'un DISPOSITIF MÉDICAL destiné à être incorporé au sein d'un RÉSEAU TI pourrait être amené à fournir des informations relatives au DISPOSITIF MÉDICAL, informations se révélant nécessaires afin de permettre à l'ORGANISME RESPONSABLE de contrôler les RISQUES conformément à la présente norme. Ces informations peuvent inclure, dans les DOCUMENTS D'ACCOMPAGNEMENT, les instructions s'adressant spécifiquement à la personne incorporant un DISPOSITIF MÉDICAL dans un RÉSEAU TI.
– Il convient que ces DOCUMENTS D'ACCOMPAGNEMENT communiquent les instructions à suivre lors de l'incorporation du DISPOSITIF MÉDICAL au sein du RÉSEAU TI, ainsi que la manière dont le DISPOSITIF MÉDICAL transfère les informations sur le RÉSEAU TI, et fassent état des caractéristiques minimales du RÉSEAU TI nécessaires afin d'assurer l'EMPLOI PRÉVU du DISPOSITIF MÉDICAL lorsque ce dernier est incorporé au sein du RÉSEAU TI. Il convient que les DOCUMENTS D'ACCOMPAGNEMENT avertissent des situations dangereuses possibles associées à la défaillance ou aux interruptions du RÉSEAU TI et à la mauvaise utilisation de la connexion au RÉSEAU TI ou des informations qui sont transférées sur le RÉSEAU TI.
– Des ACCORDS DE RESPONSABILITÉ peuvent établir les fonctions et responsabilités des acteurs impliqués dans l'incorporation d'un DISPOSITIF MÉDICAL au sein d'un RÉSEAU TI, tous les aspects du cycle de vie du RÉSEAU TI MÉDICAL qui en résulte ainsi que toutes les activités faisant partie de ce cycle de vie.
– L'ORGANISME RESPONSABLE doit affecter les personnes à certaines fonctions définies dans la présente norme. La présente norme définit les responsabilités inhérentes à ces fonctions. La plus importante de ces fonctions est celle de GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL. Cette fonction peut être attribuée à une personne de l'ORGANISME RESPONSABLE ou à un fournisseur externe.

– Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL est chargé de s'assurer que la GESTION DES RISQUES est incluse au cours des PROCESSUS suivants:

  - la planification et la conception des nouvelles incorporations de DISPOSITIFS MÉDICAUX ou les modifications apportées à ces incorporations;
  - la mise en service du RÉSEAU TI MÉDICAL et son utilisation; et
  - la GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et la gestion des modifications du RÉSEAU TI durant le cycle de vie entier du RÉSEAU TI.

– Il convient que la GESTION DES RISQUES s'applique afin d'aborder les PROPRIÉTÉS CLÉS suivantes appropriées au RÉSEAU TI comportant un DISPOSITIF MÉDICAL:

  - SÉCURITÉ (absence de RISQUE inacceptable d'une blessure physique ou d'une atteinte à la santé des personnes ou de dommages sur les biens ou l'environnement);
  - EFFICACITÉ (capacité à obtenir le résultat prévu pour le patient et l'ORGANISME RESPONSABLE);
  - SÉCURITÉ DES DONNÉES ET DU SYSTÈME (un état de fonctionnement d'un RÉSEAU TI MÉDICAL dans lequel les éléments d'actif informationnel (données et systèmes) sont suffisamment protégés de l'altération en matière de confidentialité, d'intégrité et de disponibilité).

APPLICATION DE LA GESTION DES RISQUES AUX RÉSEAUX DES TECHNOLOGIES DE L'INFORMATION CONTENANT DES DISPOSITIFS MÉDICAUX –

Partie 1: Fonctions, responsabilités et activités

1 Domaine d'application

Etant donné que les DISPOSITIFS MÉDICAUX sont incorporés dans des RÉSEAUX TI afin d'en tirer des bénéfices (par exemple, l'INTEROPÉRABILITÉ), la présente norme internationale définit les fonctions, responsabilités et activités nécessaires à la GESTION DES RISQUES des RÉSEAUX TI comportant des DISPOSITIFS MÉDICAUX afin de traiter la SÉCURITÉ, L'EFFICACITÉ et la SÉCURITÉ DES DONNÉES ET DU SYSTÈME (les PROPRIÉTÉS CLÉS). La présente norme internationale ne spécifie pas les niveaux de RISQUES acceptables.

NOTE 1 Les activités de GESTION DES RISQUES décrites dans la présente norme sont tirées de celles de l'ISO 14971 [4]. La relation entre l'ISO 14971 et la présente norme est décrite à l'Annexe A.

La présente norme s'applique dès lors qu'un DISPOSITIF MÉDICAL a été acquis par un ORGANISME RESPONSABLE et qu'il est envisagé de l'incorporer dans un RÉSEAU IT.

NOTE 2 La présente norme ne couvre pas la GESTION DES RISQUES avant mise sur le marché.

La présente norme s'applique tout au long du cycle de vie des RÉSEAUX TI comportant des DISPOSITIFS MÉDICAUX.

NOTE 3 Les activités de gestion du cycle de vie décrites dans la présente norme sont très proches de celles de l'ISO/CEI 20000-2 [10]. La relation entre l'ISO/CEI 20000-2 et la présente norme est décrite à l'Annexe D.

La présente norme s'applique lorsqu'il n'existe aucun fabricant de DISPOSITIFS MÉDICAUX se portant responsable de la définition des PROPRIÉTÉS CLÉS du RÉSEAU TI comportant un DISPOSITIF MÉDICAL.

NOTE 4 Si un fabricant individuel décrit un DISPOSITIF MÉDICAL complet comportant un réseau, l'installation ou l'assemblage du DISPOSITIF MÉDICAL conformément aux DOCUMENTS D'ACCOMPAGNEMENT du fabricant n'est pas soumis aux spécifications de la présente norme quelle que soit la personne installant ou assemblant le DISPOSITIF MÉDICAL.

NOTE 5 Si un fabricant individuel décrit un DISPOSITIF MÉDICAL complet comportant un réseau, les ajouts effectués à ce DISPOSITIF MÉDICAL ou les modifications apportées à la configuration de ce DISPOSITIF MÉDICAL, autres que ceux décrits par le fabricant, sont soumis aux spécifications de la présente norme.

La présente norme s'applique aux ORGANISMES RESPONSABLES, aux fabricants de DISPOSITIFS MÉDICAUX et aux fournisseurs d'autres technologies de l'information pour les besoins de la GESTION DES RISQUES d'un RÉSEAU IT incorporant des DISPOSITIFS MÉDICAUX tels que spécifiés par l'ORGANISME RESPONSABLE.

La présente norme ne s'applique pas aux applications d'utilisation personnelle où le PATIENT, l'OPERATEUR et l'ORGANISME RESPONSABLE ne désignent qu'une seule et même personne.

NOTE 6 Lorsqu'un DISPOSITIF MÉDICAL est utilisé à domicile sous la surveillance et/ou dans le respect des instructions du fournisseur, ce fournisseur est considéré comme L'ORGANISME RESPONSABLE. L'utilisation à titre personnel où le patient acquiert et utilise un DISPOSITIF MÉDICAL sans la surveillance ou les instructions d'un fournisseur ne relève pas du domaine d'application de la présente norme.

La présente norme ne couvre pas les exigences réglementaires ou légales.

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent:

2.1
DOCUMENT D'ACCOMPAGNEMENT
document accompagnant un DISPOSITIF MÉDICAL ou un accessoire et contenant des informations pour l'ORGANISME RESPONSABLE ou l'OPERATEUR, en particulier en matière de SÉCURITÉ

NOTE Adapté de la CEI 60601-1:2005, définition 3.4.

2.2
GESTION DU DÉCLENCHEMENT DES MODIFICATIONS
PROCESSUS garantissant que toutes les modifications apportées au RÉSEAU TI sont évaluées, approuvées, implémentées et revues de manière contrôlée et que toutes les modifications sont effectuées, réparties et suivies, le résultat étant un déclenchement de la modification de manière contrôlée avec des éléments d'entrée et de sortie appropriés à la GESTION DE LA CONFIGURATION

NOTE Adapté de l'ISO/CEI 20000-1:2005, Paragraphes 9.2 (gestion des modifications) et 10.1 (gestion du déclenchement).

2.3
AUTORISATION DE MODIFICATIONS
résultat du PROCESSUS DE GESTION DES RISQUES se présentant sous la forme d'un document autorisant une modification spécifique ou un type de modification sans activités ultérieures de GESTION DES RISQUES soumises à des contraintes précises

2.4
GESTION DE LA CONFIGURATION
PROCESSUS garantissant que les informations relatives à la configuration des composants et du RÉSEAU TI sont définies et conservées de manière précise et contrôlée et qui fournit un mécanisme pour identifier, contrôler et assurer la traçabilité des versions d'un RÉSEAU IT

NOTE Adapté de l'ISO/CEI 20000-1:2005, Paragraphe 9.1.

2.5
SÉCURITÉ DES DONNÉES ET DES SYSTÈMES
état de fonctionnement d'un RÉSEAU TI MÉDICAL dans lequel les éléments d'actifs informationnels (données et systèmes) sont suffisamment protégés de l'altération en matière de confidentialité, d'intégrité et de disponibilité

NOTE 1 Il convient que la sécurité, lorsqu'elle est mentionnée dans la présente norme, inclue la SÉCURITÉ DES DONNÉES ET DES SYSTÈMES.

NOTE 2 LA SÉCURITÉ DES DONNÉES ET DES SYSTÈMES est garantie par un système de politiques, de directives, d'infrastructures et de services conçu afin de protéger les éléments d'actifs informationnels et les systèmes qui obtiennent, transmettent, stockent et utilisent des informations dans le cadre de la mission de l'organisme.

2.6
EFFICACITÉ
capacité à obtenir le résultat prévu pour le patient et l'ORGANISME RESPONSABLE

2.7
GESTION DES ÉVÈNEMENTS
PROCESSUS garantissant que tous les événements pouvant ou susceptibles d'influencer négativement le fonctionnement du RÉSEAU TI sont saisis, évalués et gérés de manière contrôlée

NOTE Adapté de l'ISO/CEI 20000-1:2005, Paragraphes 8.2 (gestion des incidents) et 8.3 (gestion des problèmes).

2.8
DOMMAGE
blessure physique ou atteinte à la santé des personnes ou dommage touchant les biens ou l'environnement ou réduction de L'EFFICACITÉ ou brèche dans la SÉCURITÉ DES DONNÉES ET DES SYSTÈMES

NOTE Adapté de la CEI 14971:2007, définition 2.2.

2.9
PHÉNOMÈNE DANGEREUX
source potentielle de DOMMAGE

[ISO 14971:2007, définition 2.3]

2.10
EMPLOI PRÉVU
DESTINATION PRÉVUE
utilisation à laquelle un produit, un PROCESSUS ou un service est destiné conformément aux spécifications, aux instructions et aux informations fournies par le fabricant

[ISO 14971: 2007, définition 2.5]

2.11
INTEROPÉRABILITÉ
propriété permettant à divers systèmes ou composants de fonctionner ensemble dans un but précis

2.12
RÉSEAU TI (RÉSEAU DE TECHNOLOGIES DE L'INFORMATION)
un ou plusieurs systèmes composés de nœuds de communication et de liaisons de transmission afin de garantir une transmission à liaison physique ou sans fil entre au moins deux nœuds de communication précis

NOTE 1 Adapté de la CEI 61907:2009, définition 3.1.1.

NOTE 2 Le domaine d'application du RÉSEAU TI MÉDICAL de la présente norme est défini par l'ORGANISME RESPONSABLE en s'appuyant sur l'emplacement des DISPOSITIFS MÉDICAUX dans le RÉSEAU TI MÉDICAL et sur l'utilisation définie du réseau. Il peut comporter des contextes d'infrastructures informatiques, de soins à domicile ainsi que des contextes non cliniques. Voir également 4.3.3.

2.13
PROPRIÉTÉS CLÉS
trois caractéristiques faisant l'objet d'une gestion des risques (SÉCURITÉ, EFFICACITÉ et SÉCURITÉ DES DONNÉES ET DES SYSTEMES) des RÉSEAUX TI MÉDICAUX

2.14
DISPOSITIF MÉDICAL
désigne tout instrument, appareil, équipement, machine, dispositif, implant, réactif *in vitro* ou calibreur, logiciel, matériau ou tout autre article similaire ou associé:

a) destiné par son fabricant à être utilisé, seul ou en association, au profit de personnes pour un ou plusieurs des besoin(s) spécifique(s) suivant(s):
   - diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie,
   - diagnostic, contrôle, traitement, atténuation ou compensation d'une blessure,
   - étude, remplacement, modification ou support en liaison avec l'anatomie ou d'un processus physiologique,
   - assistance ou maintien de la vie,

– maîtrise de la conception,désinfection des dispositifs médicaux,communication d'informations à des fins de traitement ou de diagnostic par un examen *in vitro* de prélèvements provenant du corps humain; et

b) et dont l'action principale voulue dans ou sur le corps humain, n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme mais dont la fonction prévue peut être assistée par de tels moyens.

NOTE 1 La définition d'un dispositif pour un examen *in vitro* inclut, par exemple, les réactifs, les calibreurs, les dispositifs pour la collecte et le stockage des échantillons, les matériaux de contrôle ainsi que les instruments ou appareils associés. Les informations fournies par un tel dispositif de diagnostic *in vitro* peuvent être pour des besoins de diagnostic, de surveillance ou de compatibilité. Dans certaines collectivités publiques, des dispositifs de diagnostic *in vitro*, y compris les réactifs et dispositifs similaires, peuvent être couverts par des réglementations séparées.

NOTE 2 Les produits suivants peuvent être considérés comme des dispositifs médicaux dans certaines collectivités publiques mais il n'existe pas encore d'approche harmonisée les concernant:

– aides pour les personnes invalides/handicapées;
– dispositifs pour le traitement/diagnostic des maladies et des blessures chez les animaux;
– accessoires pour les dispositifs médicaux (voir Note 3);
– substances désinfectantes;
– dispositifs incorporant des tissus animaux et humains pouvant satisfaire aux exigences de la définition ci-dessus mais soumis à des contrôles différents.

NOTE 3 Il convient que les accessoires spécifiquement prévus par les fabricants pour être utilisés en association avec un dispositif médical "parent" afin que ce dispositif médical atteigne sa destination prévue soient soumis aux mêmes procédures GHTF que celles qui s'appliquent au dispositif médical lui même. Par exemple, un accessoire sera classé comme s'il était un dispositif médical de plein droit. Ceci peut entraîner une classification différente pour l'accessoire et le dispositif 'parent'.

NOTE 4 Les composants des dispositifs médicaux sont généralement contrôlés par le système de gestion de la qualité du fabricant et les procédures d'évaluation de la conformité pour ce dispositif. Dans certaines collectivités publiques, les composants sont inclus dans la définition d'un 'dispositif médical'.

[GHTF SG1/N29R16:2005]

2.15
LOGICIEL DE DISPOSITIFS MÉDICAUX
système logiciel qui a été développé pour être incorporé dans le DISPOSITIF MÉDICAL ou qui est destiné à être utilisé comme un DISPOSITIF MÉDICAL à part entière

[CEI 62304:2006, définition 3.12, modifiée]

2.16
réseau TI médical
RÉSEAU TI incorporant au moins un DISPOSITIF MÉDICAL

2.17
GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL
personne responsable de la GESTION DES RISQUES D'UN RÉSEAU TI MÉDICAL

2.18
OPÉRATEUR
personne manipulant un appareil

[CEI 60601-1:2005, définition 3.73]

2.19
PROCESSUS
ensemble d'activités corrélées ou interactives liées qui transforme des éléments d'entrée en éléments de sortie

[ISO 14971:2007, définition 2.13]

NOTE Le terme “activités” couvre l'utilisation des ressources.

2.20
RISQUE RÉSIDUEL
RISQUE subsistant après que des mesures de MAÎTRISE DU RISQUE ont été prises

[ISO 14971:2007, définition 2.15]

2.21
ACCORD DE RESPONSABILITÉ
un ou plusieurs documents définissant entièrement les responsabilités de tous les intervenants concernés

NOTE Cet accord peut être un document légal, ex. un contrat.

2.22
ORGANISME RESPONSABLE
entité responsable de l'utilisation et de la maintenance d'un RÉSEAU TI MÉDICAL

NOTE 1 L'entité responsable peut être par exemple un hôpital, un médecin à titre individuel ou un organisme de télésanté.

NOTE 2 Adapté de la CEI 60601-1:2005, définition 3.101.

2.23
RISQUE
combinaison de la probabilité d'un DOMMAGE et de sa gravité

[ISO 14971:2007, définition 2.16]

2.24
ANALYSE DU RISQUE
utilisation des informations disponibles pour identifier les PHÉNOMÈNES DANGEREUX et estimer le RISQUE

[ISO 14971:2007, définition 2.17]

2.25
APPRÉCIATION DU RISQUE
PROCESSUS englobant une ANALYSE DU RISQUE et une ÉVALUATION DU RISQUE

[ISO/CEI Guide 51:1999, définition 3.12]

2.26
MAÎTRISE DU RISQUE
PROCESSUS au cours duquel les décisions sont prises et les mesures visant à réduire les RISQUES ou à les maintenir dans les limites spécifiques sont mises en place

[ISO 14971:2007, définition 2.19]

2.27
ÉVALUATION DU RISQUE
PROCESSUS de comparaison des RISQUES estimés avec les critères de RISQUE donnés afin de déterminer l'acceptabilité du RISQUE

[ISO 14971:2007, définition 2.21]

2.28
GESTION DES RISQUES
application systématique des politiques de gestion, des procédures et des pratiques à des tâches d'analyse, d'évaluation, de contrôle et de maîtrise des RISQUES

[ISO 14971:2007, définition 2.22]

2.29
DOSSIER DE GESTION DES RISQUES
ensemble des enregistrements et d'autres documents produits par la GESTION DES RISQUES

[ISO 14971:2007, définition 2.23]

2.30
SÉCURITÉ
absence de RISQUE inacceptable d'une blessure physique ou d'une atteinte à la santé des personnes ou de dommages sur les biens ou l'environnement

NOTE Adapté de l'ISO 14971:2007, définition 2.24.

2.31
DIRECTION
personne ou groupe de personnes dirigeant et contrôlant l'ORGANISME RESPONSABLE chargé du RÉSEAU TI MÉDICAL au plus haut niveau

NOTE Adapté de la CEI 9000:2005, définition 3.2.7.

2.32
VÉRIFICATION
confirmation par des preuves tangibles que les exigences spécifiées ont été satisfaites

NOTE 1 Le terme "vérifié" désigne l'état correspondant.

NOTE 2 La confirmation peut couvrir des activités telles que:

– la réalisation d'autres calculs,
– la comparaison d'une spécification de conception nouvelle avec une spécification de conception similaire éprouvée,
– la réalisation d'essais et de démonstrations, et
– la revue de documents avant diffusion.

[ISO 14971:2007, définition 2.28]

NOTE 3 Lors de la conception et du développement, la VÉRIFICATION concerne le PROCESSUS d'examen du résultat d'une activité donnée en vue de déterminer sa conformité aux exigences fixées pour ladite activité.

3 Fonctions et responsabilités

3.1 Généralités

L'incorporation et la modification des appareils ou des logiciels d'un RÉSEAU TI MÉDICAL doivent être effectuées selon un ensemble de responsabilités clairement définies. Au minimum, les parties, responsabilités et exigences identifiées de 3.2 à 3.6 doivent être définies.

L'ORGANISME RESPONSABLE doit établir et maintenir un DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL pour le RÉSEAU TI MÉDICAL considéré.

Toute la documentation associée aux exigences de la présente norme pour les ORGANISMES RESPONSABLES ainsi que la documentation d'aide doivent être conservées dans un DOSSIER DE

GESTION DES RISQUES DU RÉSEAU TI MÉDICAL. Ce dossier doit contenir les informations relatives à la GESTION DE LA CONFIGURATION actuelle du RÉSEAU TI MÉDICAL.

NOTE Les informations relatives à la GESTION DE LA CONFIGURATION peuvent être incluses dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL sous la forme d'une documentation explicite ou sous forme de références, par exemple, à une base de données existante.

La conformité est vérifiée par inspection du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

3.2 ORGANISME RESPONSABLE

La responsabilité globale de LA GESTION DES RISQUES pour un RÉSEAU TI MÉDICAL doit rester au sein de l'ORGANISME RESPONSABLE.

L'ORGANISME RESPONSABLE doit être le propriétaire du PROCESSUS DE GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL, comprenant la planification, la conception, l'installation, la connexion du dispositif, la configuration, l'utilisation/le fonctionnement, la maintenance et la mise hors service du dispositif.

La conformité est vérifiée par l'évaluation de l'ORGANISME RESPONSABLE.

3.3 Responsabilités de la DIRECTION

En ce qui concerne la GESTION DES RISQUES des RÉSEAUX TI MÉDICAUX, LA DIRECTION doit être responsable pour:

a) mettre en place une politique pour la GESTION DES RISQUES pour incorporer des DISPOSITIFS MÉDICAUX;

b) définir la politique pour déterminer les RISQUES acceptables, en prenant en compte les normes internationales ainsi que les réglementations nationales ou régionales en vigueur;

c) garantir la fourniture de ressources appropriées;

d) garantir l'attribution de personnel qualifié pour la gestion, les performances de travail et les activités d'évaluation; et

e) revoir les résultats des activités liées à la GESTION DES RISQUES, y compris la GESTION DES ÉVÉNEMENTS (voir 4.6.2) à intervalle défini afin de garantir la conformité continue et l'efficacité du PROCESSUS DE GESTION DES RISQUES.

Les informations ci-dessus doivent être documentées dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

LA DIRECTION GÉNÉRALE doit désigner un GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL, suffisamment qualifié, et possédant les connaissances et compétences nécessaires à la GESTION DES RISQUES appliquée aux RÉSEAUX TI MÉDICAUX (voir 3.4).

LA DIRECTION doit identifier les personnes responsables des tâches suivantes et s'assurer qu'elles coopèrent avec le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL:

f) collecte, analyse, évaluation et stockage des informations requises pour la GESTION DES RISQUES;

g) gestion du cycle de vie des DISPOSITIFS MÉDICAUX incorporés dans les RÉSEAUX TI;

h) révision et acceptation du RISQUE RÉSIDUEL au nom de la DIRECTION;

i) maintenance des RÉSEAUX TI MÉDICAUX; et

j) choix et achat des DISPOSITIFS MÉDICAUX.

LA DIRECTION doit garantir que la participation au PROCESSUS DE GESTION DES RISQUES pour LES RÉSEAUX TI MÉDICAUX inclut la gestion responsable:

k) des RÉSEAUX TI MÉDICAUX;

l) des activités TI générales;

m) de la gestion du cycle de vie des DISPOSITIFS MÉDICAUX connectés aux RÉSEAUX TI;

EXEMPLE ingénierie biomédicale, ingénierie radiologique

n) l'utilisation de DISPOSITIFS MÉDICAUX; et

EXEMPLE utilisateurs expérimentés provenant de services cliniques

o) maintenance et support technique pour les DISPOSITIFS MÉDICAUX

EXEMPLE département d'ingénierie biomédicale

LA DIRECTION doit garantir:

p) que la surveillance, le fonctionnement, l'installation et la maintenance du(es) RÉSEAU(X) TI MÉDICAUX pendant leur cycle de vie soient effectués conformément au plan de GESTION DES RISQUES et selon les résultats du PROCESSUS DE GESTION DES RISQUES DU RÉSEAU TI, quelle que soit la personne en charge de ces tâches;

q) que toutes les équipes chargées de la surveillance, du fonctionnement, de l'installation, de l'entretien, du dépannage et de la maintenance du(es) RÉSEAU(X) TI MÉDICAL(AUX) sont correctement informées de leur responsabilité conformément à la présente norme, y compris de leur responsabilité pour maintenir l'efficacité des CONTRÔLES DES RISQUES.

NOTE Les responsabilités de la DIRECTION sont illustrées à la Figure 1.

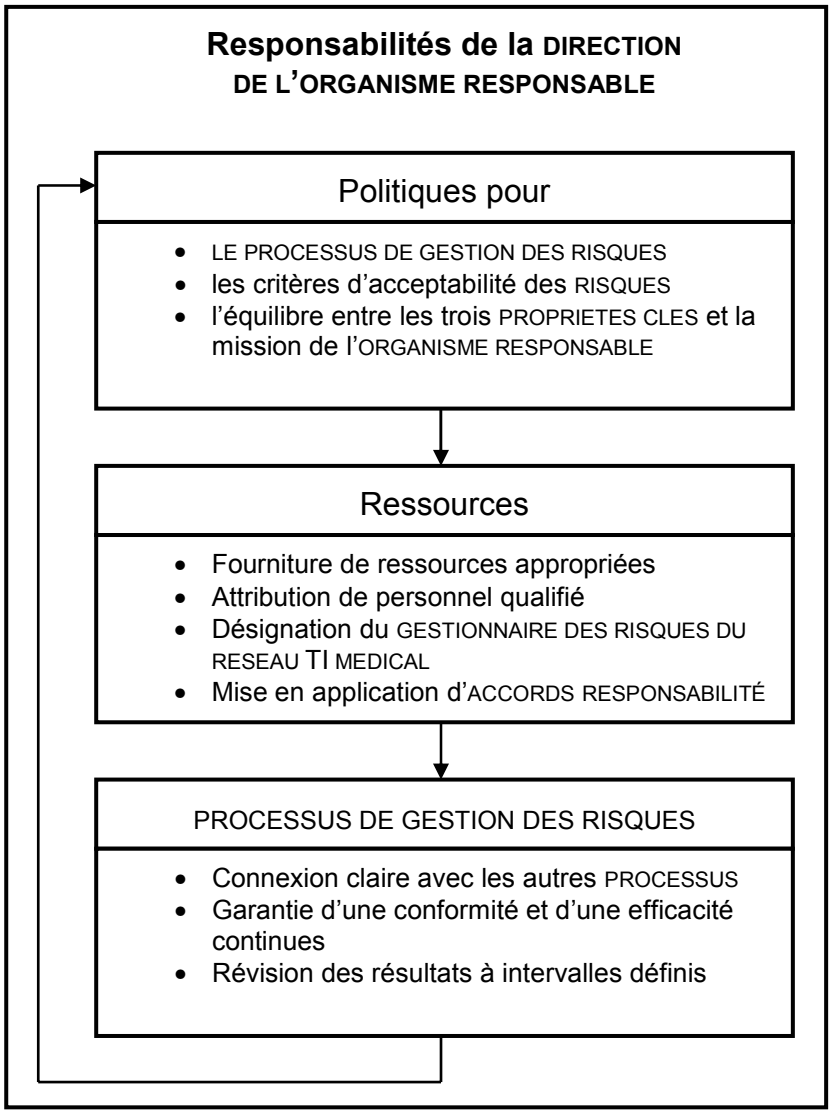


Figure 1 – Illustration des responsabilités de la direction

La conformité est vérifiée par inspection du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

3.4 GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI doit être responsable de la gestion du PROCESSUS DE GESTION DES RISQUES.

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit superviser l'exécution du PROCESSUS DE GESTION DES RISQUES afin de maintenir les PROPRIÉTÉS CLÉS du RÉSEAU TI MÉDICAL.

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit être responsable des aspects suivants relatifs à la GESTION DES RISQUES des RÉSEAUX TI incorporant des DISPOSITIFS MÉDICAUX:

a) Gestion globale du PROCESSUS DE GESTION DES RISQUES;

b) compte-rendu du PROCESSUS DE GESTION DES RISQUES à la DIRECTION; et

c) gestion de la communication nécessaire entre les participants internes et externes à la GESTION DES RISQUES. Parmi ces participants, il peut y avoir selon ce qui est approprié:

   1) les fabricants de DISPOSITIFS MÉDICAUX;
   2) les autres fournisseurs d'appareils informatiques, de logiciels et de services;
   3) la fonction informatique interne et les autres fonctions de gestion des installations;
   4) les utilisateurs cliniques; et
   5) la fonction de support technique responsable des DISPOSITIFS MÉDICAUX (par exemple le service de bioingénierie).

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI doit être responsable des performances du PROCESSUS DE GESTION DES RISQUES. Ceci comprend mais ne se limite pas à la responsabilité concernant:

d) la collecte de toutes les informations concernant les RISQUES relatives aux DISPOSITIFS MÉDICAUX;

e) la planification de l'incorporation des DISPOSITIFS MÉDICAUX conformément aux instructions fournies par les différents fabricants de DISPOSITIFS MÉDICAUX et les politiques de l'ORGANISME RESPONSABLE;

f) les performances du PROCESSUS DE GESTION DES RISQUES lorsqu'un DISPOSITIF MÉDICAL est ajouté à un RÉSEAU TI;

g) les performances du PROCESSUS DE GESTION DES RISQUES lorsqu'une modification est apportée au DISPOSITIF MÉDICAL incorporé ou au RÉSEAU TI MÉDICAL;

h) l'autorisation de procéder à la mise en service à la suite d'une modification sur un RÉSEAU TI MÉDICAL;

i) informer l'ORGANISME RESPONSABLE des RISQUES inacceptables liés au RÉSEAU TI MÉDICAL ainsi que des PHÉNOMÈNES DANGEREUX associés émanant des modifications dans la configuration; et

j) surveiller tous les projets de RÉSEAU TI MÉDICAL ou les modifications des RÉSEAUX TI MÉDICAUX dont le GESTIONNAIRE DES RISQUES DU RÉSEAU TI est responsable.

Ces tâches peuvent être déléguées, cependant c'est le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL qui demeure responsable de la garantie des performances appropriées.

La conformité est vérifiée par l'évaluation de l'ORGANISME RESPONSABLE.

3.5 Fabricant(s) de DISPOSITIFS MÉDICAUX

Conformément aux réglementations applicables et aux normes pertinentes, chaque fabricant de DISPOSITIFS MÉDICAUX doit fournir des DOCUMENTS D'ACCOMPAGNEMENT à l'ORGANISME RESPONSABLE décrivant l'EMPLOI PRÉVU et comportant des instructions à suivre pour une utilisation sûre et efficace du DISPOSITIF MÉDICAL.

Pour un DISPOSITIF MÉDICAL qui peut être connecté à un RÉSEAU TI, le fabricant de DISPOSITIFS MÉDICAUX doit fournir des instructions pour la mise en œuvre d'une telle connexion, comprenant mais ne se limitant pas à:

a) l'objet de la connexion du DISPOSITIF MÉDICAL à un RÉSEAU TI;

b) les caractéristiques requises pour le RÉSEAU TI incorporant le DISPOSITIF MÉDICAL;

c) la configuration requise pour le RÉSEAU TI incorporant le DISPOSITIF MÉDICAL;

d) les spécifications techniques de la connexion réseau du DISPOSITIF MÉDICAL comprenant les spécifications relatives à la sécurité;

e) le flux d'informations voulu entre le DISPOSITIF MÉDICAL, le RÉSEAU TI MÉDICAL et les autres dispositifs sur le RÉSEAU TI MÉDICAL, et si cela concerne les PROPRIÉTÉS CLÉS, l'acheminement prévu au sein du RÉSEAU TI MÉDICAL; et

f) une liste des situations dangereuses lorsque le RÉSEAU TI n'offre pas les caractéristiques requises pour satisfaire aux besoins de la connexion du DISPOSITIF MÉDICAL au RÉSEAU TI.

La conformité est vérifiée par la disponibilité des DOCUMENTS D'ACCOMPAGNEMENT du fabricant de DISPOSITIF MÉDICAL et d'autres instructions pour la mise en œuvre d'une telle connexion.

NOTE 1 Lorsque le contenu mis à disposition ne satisfait pas aux besoins de la GESTION DES RISQUES de l'ORGANISME RESPONSABLE, un contenu supplémentaire peut être mis à disposition dans le cadre d'un ACCORD DE RESPONSABILITÉ.

L'ORGANISME RESPONSABLE doit obtenir les DOCUMENTS D'ACCOMPAGNEMENT pour un DISPOSITIF MÉDICAL incorporé dans un RÉSEAU TI MÉDICAL. Le suivi de ces documents doit être assuré dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

L'ORGANISME RESPONSABLE doit obtenir des informations documentaires supplémentaires pour un DISPOSITIF MÉDICAL incorporé dans un RÉSEAU IT selon ce qui est nécessaire pour assurer la GESTION DES RISQUES pour un RÉSEAU IT MÉDICAL, incluant toute situation dangereuse connue qui doit être gérée par l'ORGANISME RESPONSABLE. Le suivi de ces documents doit être assuré dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

NOTE 2 Un ACCORD DE RESPONSABILITÉ peut être utilisé entre l'ORGANISME RESPONSABLE et un fabricant de DISPOSITIF MÉDICAL pour identifier et partager la documentation nécessaire.

La conformité est vérifiée par inspection du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

3.6 Fournisseurs d'autres équipements de technologies de l'information

Les fournisseurs d'autres équipements de technologies de l'information (autres que les DISPOSITIFS MÉDICAUX) peuvent fournir:

a) des composants d'infrastructure;

b) des services d'infrastructure;

c) des dispositifs de client n'étant pas considérés comme des DISPOSITIFS MÉDICAUX;

d) des serveurs;

e) des logiciels d'application; ou

f) des logiciels médiateurs.

Conformément aux réglementations applicables et aux normes pertinentes, chaque fournisseur d'autre technologie de l'information (appareil et/ou logiciel) doit mettre à disposition des informations documentaires applicables à la technologie fournie comme suit:

g) les descriptions et les manuels techniques;

h) les caractéristiques des RÉSEAUX TI MÉDICAUX;

i) les configurations recommandées des produits;

j) les incompatibilités et les restrictions connues;

k) les exigences relatives au fonctionnement;

l) les actions de correction et les rappels des produits; et

m) notices de cybersécurité (avertissements concernant les vulnérabilités de sécurité connues).

La conformité est vérifiée en s'assurant de la disponibilité des informations documentaires de tout fournisseur d'autres technologies de l'information.

NOTE 1 Lorsque le contenu mis à disposition ne satisfait pas aux besoins de la GESTION DES RISQUES de l'ORGANISME RESPONSABLE, un contenu supplémentaire peut être mis à disposition dans le cadre d'un ACCORD DE RESPONSABILITÉ.

L'ORGANISME RESPONSABLE doit obtenir les informations documentaires spécifiées ci-dessus pour toutes les technologies de l'information incorporées dans un RÉSEAU TI MÉDICAL. Ces informations documentaires doivent être maintenues dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

L'ORGANISME RESPONSABLE doit obtenir des informations documentaires supplémentaires pour les autres technologies de l'information selon ce qui est nécessaire pour encore plus alimenter les activités de GESTION DES RISQUES du RÉSEAU TI MÉDICAL. Ces informations documentaires supplémentaires doivent être maintenues dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

Exemples d'informations supplémentaires:

– les stratégies d'essai et les critères d'acceptation des essais;
– la révélation des modes de défaillances;
– les statistiques relatives à la fiabilité du système;
– les cas d'assurance de la sécurité; et
– les performances.

NOTE 2 Un ACCORD DE RESPONSABILITÉ peut être utilisé entre l'ORGANISME RESPONSABLE et un fournisseur d'autres technologies de l'information pour identifier et partager la documentation nécessaire.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

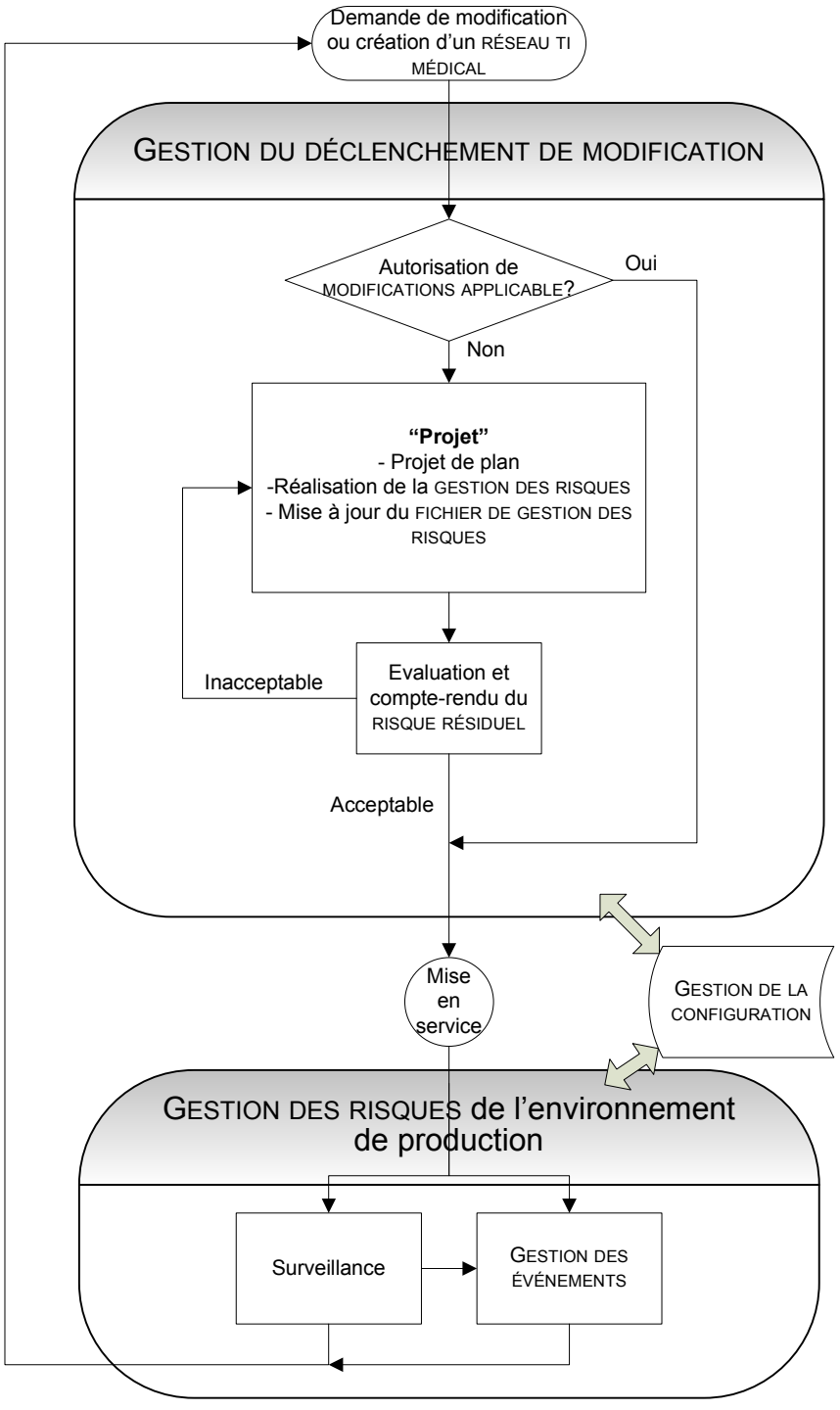
4 GESTION DES RISQUES du cycle de vie des RÉSEAUX TI MÉDICAUX

4.1 Vue d'ensemble

L'ORGANISME RESPONSABLE doit maintenir les PROPRIÉTÉS CLÉS du RÉSEAU TI MÉDICAL pendant le cycle de vie.

NOTE Le cycle de vie des RÉSEAUX TI MÉDICAUX y compris la GESTION DES RISQUES est illustré à la Figure 2.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.



NOTE Une demande de modification peut être une demande de mise hors service d'un DISPOSITIF MÉDICAL ou du réseau TI MÉDICAL. Cette mise hors service exige une planification et une gestion des RISQUES similaires à celles des autres modifications.

Figure 2 – Vue d'ensemble du cycle de vie des RÉSEAUX TI MÉDICAUX y compris la gestion des risques

4.2 GESTION DES RISQUES DE L'ORGANISME RESPONSABLE

4.2.1 POLITIQUE DE GESTION DES RISQUES pour l'incorporation des DISPOSITIFS MÉDICAUX

Afin de soutenir le cycle de vie du RÉSEAU TI MÉDICAL, la DIRECTION doit définir et documenter une politique de GESTION DES RISQUES pour l'incorporation des DISPOSITIFS MÉDICAUX dans un RÉSEAU TI. La politique de GESTION DES RISQUES doit comprendre

a) l'équilibre entre les trois PROPRIÉTÉS CLÉS et la mission de l'ORGANISME RESPONSABLE;

b) un moyen d'établir des critères d'acceptabilité des RISQUES pour chacune des PROPRIÉTÉS CLÉS, en prenant en compte les normes internationales et les réglementations nationales ou régionales applicables; et

c) une description ou une référence aux processus appliqués aux réseaux TI médicaux, comportant, au minimum,

   1) LA GESTION DES ÉVÈNEMENTS,

   2) LA GESTION DU DÉCLENCHEMENT DES MODIFICATIONS,

   3) LA GESTION DE LA CONFIGURATION, et

   4) la surveillance.

NOTE Les activités relatives au cycle de vie du RÉSEAU TI MÉDICAL peuvent être conservées dans le cadre d'une politique de gestion des services informatiques (par ex. conformément à l'ISO 20000) à condition qu'elles soient intimement liées à la politique de GESTION DES RISQUES.

La politique doit être exprimée dans des termes qui peuvent être interprétés tout au long des activités de GESTION DES RISQUES.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.2.2 PROCESSUS DE GESTION DES RISQUES

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit établir et entretenir un PROCESSUS afin d'identifier les PHÉNOMÈNES DANGEREUX, d'estimer et d'évaluer les RISQUES associés, contrôler ces RISQUES, et surveiller l'efficacité des CONTRÔLES DES RISQUES, en prenant en compte l'utilisation définie du RÉSEAU TI MÉDICAL.

NOTE Les modifications ultérieures apportées au RÉSEAU TI MÉDICAL pourraient introduire de nouveaux RISQUES et nécessiter des analyses supplémentaires.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.3 Planification et documentation de la GESTION DES RISQUES DU RÉSEAU TI MÉDICAL

4.3.1 Vue d'ensemble

L'ORGANISME RESPONSABLE doit planifier LA GESTION DES RISQUES du RÉSEAU TI MÉDICAL en fournissant

a) la description des avantages liés aux RISQUES,

   NOTE 1 Voir 4.3.2 pour trouver une description et des exemples d'avantages liés aux RISQUES.

b) la documentation relative au RÉSEAU TI, et

c) un plan de GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL.

NOTE 2 L'évaluation et la documentation de la structure du réseau sont essentielles afin de fournir les informations nécessaires à l'ANALYSE DU RISQUE et à l'ÉVALUATION DU RISQUE.

En raison de la nature des RÉSEAUX TI, l'état actuel du RÉSEAU TI et les modifications prévues doivent être pris en considération.

Le développement initial de nouveaux RÉSEAUX TI MÉDICAUX ainsi que les modifications apportées à des RÉSEAUX TI MÉDICAUX non prises en charge par des AUTORISATIONS DE MODIFICATIONS doivent être gérés par des projets.

NOTE 3 Un RÉSEAU TI MÉDICAL peut être doté de plusieurs projets simultanés ou séquentiels.

NOTE 4 Voir aussi 4.5.2.3 pour les projets de RÉSEAU TI MÉDICAL et 4.5.2.2 pour les AUTORISATIONS DE MODIFICATION.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.3.2 Description des avantages liés aux RISQUES

L'ORGANISME RESPONSABLE doit établir une liste des avantages des RÉSEAUX TI connectés aux DISPOSITIFS MÉDICAUX. Les avantages typiques incluent, mais ne se limitent pas au matériel, au logiciel et aux données essentiels à l'EMPLOI PRÉVU du DISPOSITIF MÉDICAL et à l'utilisation définie du RÉSEAU TI MÉDICAL. La liste des avantages peut comprendre par exemple:

a) les composants spécifiques du RÉSEAU TI MÉDICAL et tous les DISPOSITIFS MÉDICAUX incorporés ainsi que les autres appareils (ex. modalités de création d'images, composants du réseau) de l'infrastructure de technologie de l'information;

b) les caractéristiques relatives au fonctionnement de l'infrastructure TI du RÉSEAU TI MÉDICAL (ex. propriétés des performances telles que la longueur d'onde);

c) les informations relatives à la GESTION DE LA CONFIGURATION;

d) le logiciel d'application médicale;

e) les données relatives à la configuration du matériel et des logiciels;

f) la caractérisation des données patient identifiables sur le RÉSEAU TI MÉDICAL ou utilisées par le DISPOSITIF MÉDICAL incorporé y compris leur nature, leur volume et leur sensibilité;

g) les informations appuyant la procédure de santé, incluant l'historique d'utilisation ainsi que les détails OPERATEUR/utilisateur; et

h) une description de la sécurité et des autres matériels concernant les considérations de SÉCURITÉ du système dans son ensemble (dans ce cas, la protection est un aspect de la SÉCURITÉ).

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.3.3 Documentation relative au RÉSEAU TI MÉDICAL

L'ORGANISME RESPONSABLE doit rédiger et conserver la documentation relative au réseau nécessaire pour la GESTION DES RISQUES du RÉSEAU TI MÉDICAL pour les interfaces entre le(s) DISPOSITIF(S) MÉDICAL(AUX) et l'ensemble des composants du réseau (logiciels et matériels). Cette documentation doit comprendre mais ne pas se limiter:

a) à la configuration physique et logique du réseau;

NOTE 1 La configuration du réseau inclut la définition des limites du réseau.

NOTE 2 La documentation peut contenir les propriétés électriques du RÉSEAU TI qui pourraient avoir un impact sur les performances du RÉSEAU TI MÉDICAL et sur les dispositifs incorporés. On peut donner comme exemples, la liste n'étant pas exhaustive, la mise à la terre, le (dé)couplage galvanique, les courants parasites et la puissance transmise par le réseau Ethernet (PoE).

b) aux normes appliquées et aux déclarations de conformité;

c) à la structure physique et logique client / serveur;

d) à la sécurité, la fiabilité et l'intégrité des données du réseau;

e) aux exigences relatives à la communication avec le réseau pour chacun des DISPOSITIFS MÉDICAUX comme spécifié par le fabricant; et

f) aux prochaines modifications / mises à niveau / améliorations (prévues / relativement prévisibles).

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.3.4 ACCORD DE RESPONSABILITÉ

Lorsqu'un DISPOSITIF MÉDICAL est incorporé au sein d'un RÉSEAU TI, ou lorsque la configuration d'une telle connexion est modifiée, l'ORGANISME RESPONSABLE doit déterminer le besoin d'un ou de plusieurs ACCORDS DE RESPONSABILITÉ documentés définissant (ex. par contrat) les responsabilités des intervenants concernés.

Un ACCORD DE RESPONSABILITÉ peut s'appliquer à un ou plusieurs projets ou à la maintenance d'un ou de plusieurs RÉSEAUX TI MÉDICAUX, et doit identifier la responsabilité pour tous les aspects du cycle de vie du RÉSEAU TI MÉDICAL ainsi que toutes les activités faisant partie du cycle de vie.

NOTE Afin de prendre en charge l'incorporation des DISPOSITIFS MÉDICAUX au sein d'un RÉSEAU TI, les fabricants de DISPOSITIFS MÉDICAUX mettent des informations techniques appropriées à disposition afin d'élaborer la documentation relative à la GESTION DES RISQUES DE L'ORGANISME RESPONSABLE. Lorsque le PROCESSUS requiert des informations qu'un fabricant de DISPOSITIFS MÉDICAUX juge sensibles, la fourniture de ces informations sera déterminée par l'ACCORD DE RESPONSABILITÉ et peut être protégée par un accord de confidentialité.

Les ACCORDS DE RESPONSABILITÉ doivent comporter (ou se référer à des documents comportant) au minimum:

a) le nom de la personne responsable de la GESTION DES RISQUES pour les activités couvertes par l'ACCORD DE RESPONSABILITÉ;

b) le domaine d'application des activités couvertes par l'ACCORD DE RESPONSABILITÉ, y compris un résumé de et/ou des références aux exigences;

c) une liste des DISPOSITIFS MÉDICAUX et des autres appareils destinés à être incorporés dans le RÉSEAU TI ou modifiés, ainsi que les noms des fabricants de DISPOSITIFS MÉDICAUX ou des autres organismes chargés de fournir des informations techniques nécessaires à la réalisation du projet;

d) une liste des documents à fournir par les fabricants de DISPOSITIFS MÉDICAUX et par les autres fournisseurs d'appareils comportant des instructions pour la connexion à ou la déconnexion d'un RÉSEAU TI;

e) les informations techniques à fournir par les fabricants de DISPOSITIFS MÉDICAUX ou informatiques et par les autres fournisseurs d'appareils qui sont nécessaires afin d'effectuer l'ANALYSE DU RISQUE du RÉSEAU TI; ET

f) la définition des fonctions et des responsabilités dans la gestion des évènements potentiellement indésirables.

L'ORGANISME RESPONSABLE doit fournir un résumé des responsabilités selon ce qui est approprié.

NOTE 1 Le fabricant d'un DISPOSITIF MÉDICAL est chargé de mettre à disposition la documentation technique expliquant comment utiliser les interfaces du DISPOSITIF MÉDICAL pour la connexion à un RÉSEAU TI, à condition qu'une telle connexion soit prévue par le fabricant. Cette obligation ne s'applique pas au fournisseur d'un autre appareil, et il pourrait être nécessaire de conclure un arrangement spécifique afin d'accéder à une telle documentation technique.

Si la coopération des fabricants de DISPOSITIFS MÉDICAUX, des fournisseurs d'autres appareils ou d'autres organismes est nécessaire en plus des documents listés fournis par les fabricants ou organismes, un ACCORD DE RESPONSABILITÉ doit:

g) identifier la nature de la coopération requise; et

h) établir:

- la personne responsable de la demande d'une telle coopération;
- la personne en charge de répondre à de telles demandes; et
- quels critères seront utilisés afin de juger de l'adéquation d'une telle réponse.

NOTE 2 Dans la mesure où cette information peut changer au cours du cycle de vie d'un RÉSEAU TI MÉDICAL, il est recommandé qu'elle soit périodiquement mise à jour dans l'ACCORD DE RESPONSABILITÉ.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.3.5 Plan de GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL

L'ORGANISME RESPONSABLE doit élaborer et maintenir un plan de GESTION DES RISQUES pour chacun des RÉSEAUX TI MÉDICAUX. Le plan de GESTION DES RISQUES doit comprendre:

a) une description du RÉSEAU TI MÉDICAL, comportant:
   1) les intervenants identifiés au sein de l'ORGANISME RESPONSABLE qui doivent être informés des PHÉNOMÈNES DANGEREUX afin de s'assurer qu'ils sont conscients des RISQUES;
   2) l'utilisation définie et les bénéfices attendus du RÉSEAU TI MÉDICAL;
   3) la raison de chaque incorporation de DISPOSITIF MÉDICAL; et
   4) l'utilisation de chaque DISPOSITIF MÉDICAL due à son incorporation dans le RÉSEAU TI MÉDICAL lorsqu'elle n'est pas incluse dans l'EMPLOI PRÉVU par le fabricant.

b) une description des activités, des fonctions et des responsabilités de toutes les équipes impliquées dans le fonctionnement/la maintenance du RÉSEAU TI MÉDICAL, en ce qui concerne la GESTION DES RISQUES.

c) les exigences relatives à la surveillance du RÉSEAU TI MÉDICAL (se référer à 4.6.1).

d) les critères d'acceptabilité des RISQUES, basés sur la politique de l'ORGANISME RESPONSABLE pour déterminer les RISQUES acceptables, y compris les critères d'acceptabilité des RISQUES lorsque la probabilité de survenue d'un PHÉNOMÈNE DANGEREUX ne peut pas être estimée.

Lorsqu'un projet introduit des modifications d'un RÉSEAU TI MÉDICAL existant, le plan de GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL doit être mis à jour.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4 GESTION DES RISQUES DU RÉSEAU TI MÉDICAL

4.4.1 Vue d'ensemble

La présente section décrit les PROCESSUS DE GESTION DES RISQUES prenant en charge à la fois la réalisation d'un projet de RÉSEAU TI MÉDICAL et la décision d'effectuer une modification particulière.

Les activités de GESTION DES RISQUES nécessaires à l'ANALYSE DU RISQUE, à L'ÉVALUATION DU RISQUE, au MAÎTRISE DU RISQUE ainsi qu'à l'évaluation, au compte-rendu et à l'approbation des RISQUES RÉSIDUELS doivent être documentés. Cette documentation peut faire partie intégrante du plan DE GESTION DES RISQUES ou exister sous forme de documents séparés dans le DOSSIER DE GESTION DES RISQUES associé au RÉSEAU TI MÉDICAL. Les plans d'actions résultant de L'APPRÉCIATION DU RISQUE doivent suivre le PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS.

NOTE Il existe un seul ensemble de documents de GESTION DES RISQUES par RÉSEAU TI MÉDICAL car les mesures DE MAÎTRISE DU RISQUE pour un projet ou une modification donnée ne doivent pas entrer en conflit avec les mesures de MAÎTRISE DU RISQUE existantes pour le RÉSEAU TI MÉDICAL ou avec les mesures de MAÎTRISE DU RISQUE proposées par un projet concomitant.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.2 ANALYSE DU RISQUE

L'ORGANISME RESPONSABLE doit identifier les PHÉNOMÈNES DANGEREUX susceptibles de provenir du RÉSEAU TI MÉDICAL.

Pour chaque PHÉNOMÈNE DANGEREUX identifié, l'ORGANISME RESPONSABLE doit évaluer les RISQUES associés à l'aide des informations ou des données disponibles.

NOTE LES RISQUES à analyser couvrent le cycle de vie entier, particulièrement ceux comprenant la mise en application de la modification et l'utilisation régulière du RÉSEAU TI MÉDICAL.

Si la probabilité d'un PHÉNOMÈNE DANGEREUX ne peut pas être estimée, une liste des conséquences possibles doit être établie et utilisée lors de L'ÉVALUATION DU RISQUE et du MAÎTRISE DU RISQUE.

Les résultats de ces activités doivent être enregistrés dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.3 ÉVALUATION DU RISQUE

Pour chacun des PHÉNOMÈNES DANGEREUX identifiés, l'ORGANISME RESPONSABLE doit décider, à l'aide des critères définis dans le plan de GESTION DES RISQUES, si:

a) le(s) RISQUE(S) estimé(s) est(sont) si faible(s) que la poursuite de la réduction des RISQUES ne s'avère pas nécessaire. Dans ce cas, la justification de cette décision doit être documentée dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI.

b) le(s) RISQUE(S) estimé(s) n'est (ne sont) pas acceptable(s). Dans ce cas, les mesures de MAÎTRISE DU RISQUE doivent être mises en application conformément à 4.4.4.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.4 MAÎTRISE DU RISQUE

4.4.4.1 Analyse optionnelle de MAÎTRISE DU RISQUE

L'ORGANISME RESPONSABLE doit identifier et documenter les mesures de MAÎTRISE DU RISQUE proposées pour chacun des RISQUES inacceptables jusqu'à ce que le(s) RISQUE(S) RÉSIDUEL(S) soi(en)t jugés acceptable(s).

Une ou plusieurs options de MAÎTRISE DU RISQUE doivent être utilisées dans l'ordre de priorité listé:

a) le contrôle implicite par la conception (ex. isolation physique d'un réseau de toutes menaces externes);

b) les mesures de protection (ex. y compris des alertes);

c) les informations pour l'assurance (ex. avertissements, documentation utilisateur, formation).

NOTE 1 Les mesures de MAÎTRISE DU RISQUE peuvent par exemple inclure:

– des instructions et des contraintes documentées comme AUTORISATION DE MODIFICATION (voir 2.3 et 4.5.2.2);
– les composants du réseau;
– la modification de la configuration du réseau;
– les considérations liées à l'organisation; ou
– les modifications apportées aux DISPOSITIFS MÉDICAUX incorporés.

NOTE 2 Il est recommandé pour chacun des RISQUES, que la conception prenne soigneusement en compte le meilleur endroit pour implémenter le contrôle afin de garantir la viabilité – par exemple, par des modifications du RÉSEAU TI MÉDICAL ou des modifications autorisées du DISPOSITIF MÉDICAL.

Etant donné que le MAÎTRISE DU RISQUE nécessite des compromis dans le domaine des PROPRIÉTÉS CLÉS, ces dernières doivent être prises en considération dans l'ordre de priorité suivant SÉCURITÉ, EFFICACITÉ, et SÉCURITÉ DES DONNÉES ET DES SYSTÈMES.

Si, durant l'analyse optionnelle de MAÎTRISE DU RISQUE, l'ORGANISME RESPONSABLE détermine que la réduction des RISQUES n'est pas réalisable, l'ORGANISME RESPONSABLE doit mener à bien et documenter une analyse RISQUE/bénéfice du RISQUE RÉSIDUEL (voir 4.4.5).

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.4.2 Mesures de MAÎTRISE DU RISQUE

Lorsqu'une mesure de MAÎTRISE DU RISQUE spécifique est sélectionnée et que celle-ci exige une modification du RÉSEAU TI MÉDICAL, les PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS doivent être suivis

Les mesures de MAÎTRISE DU RISQUE sélectionnées doivent être enregistrées dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.4.3 Mise en place des mesures de MAÎTRISE DU RISQUE

Les mesures de MAÎTRISE DU RISQUE choisies doivent être mises en application.

Il convient que les mesures de MAÎTRISE DU RISQUE au sein du DISPOSITIF MÉDICAL ne soient implémentées que par le fabricant de DISPOSITIFS MÉDICAUX ou par l'ORGANISME RESPONSABLE en suivant les instructions d'utilisation ou avec l'autorisation écrite du fabricant de DISPOSITIFS MÉDICAUX.

Des modifications du DISPOSITIF MÉDICAL entreprises par l'ORGANISME RESPONSABLE sans le consentement documenté du fabricant du DISPOSITIF ne sont pas recommandées. Si une telle modification est entreprise, l'ORGANISME RESPONSABLE doit notifier le fabricant et doit suivre toutes les étapes réglementaires nécessaires pour mettre ne service un tel DISPOSITIF MÉDICAL modifié.

Tout RISQUE RÉSIDUEL doit être documenté dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.4.4 VÉRIFICATION des mesures de MAÎTRISE DU RISQUE

La mise en application de toutes les mesures de MAÎTRISE DU RISQUE dans le système opérationnel doit être VÉRIFIÉE et documentée dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

L'efficacité de toutes les mesures de MAÎTRISE DU RISQUE doit être VÉRIFIÉE et documentée dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

NOTE Il pourrait s'avérer nécessaire de vérifier l'efficacité des mesures de MAÎTRISE DU RISQUE dans un environnement d'essai avant la mise en application dans un système opérationnel.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.4.5 Nouveaux RISQUES décelés suite à la MAÎTRISE DU RISQUE

Les mesures de MAÎTRISE DU RISQUE mises en application et le système opérationnel installé doivent être revus pour de nouveaux RISQUES inacceptables (c'est-à-dire une dégradation des PROPRIÉTÉS CLÉS ou d'autres attributs importants essentiels dans la réalisation de l'utilisation définie du RÉSEAU TI MÉDICAL).

L'évaluation doit être documentée dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.4.5 Evaluation et compte-rendu du RISQUE RÉSIDUEL

Le RISQUE RÉSIDUEL doit être évalué en se fondant sur l'évaluation avant déclenchement de l'efficacité des mesures de MAÎTRISE DU RISQUE mises en application.

Les RISQUES RÉSIDUELS individuels ainsi que le RISQUES RÉSIDUEL global doivent être évalués en termes d'acceptabilité.

NOTE Voir 4.4.3 pour l'ÉVALUATION DU RISQUE.

Si un RISQUE RÉSIDUEL individuel ou si LE RISQUE RÉSIDUEL global n'est pas jugé comme acceptable, des mesures de MAÎTRISE DU RISQUE supplémentaires doivent être appliquées.

L'ORGANISME RESPONSABLE doit établir et documenter un résumé des RISQUES RÉSIDUELS comportant une liste de tous les RISQUES RÉSIDUELS individuels et du RISQUE RÉSIDUEL global demeurant après la mise en application des mesures de MAÎTRISE DU RISQUE (voir 4.4.4.3), y compris les RISQUES RÉSIDUELS associés à un projet particulier de RÉSEAU TI MÉDICAL et le RISQUE RÉSIDUEL DU RÉSEAU TI MÉDICAL.

Si la réduction du RISQUE RÉSIDUEL à un niveau acceptable n'est pas réalisable, dans le cadre de la politique de L'ORGANISME RESPONSABLE pour déterminer le RISQUE acceptable (voir 3.3), la personne identifiée par la DIRECTION (voir 3.3) pour revoir les RISQUES RÉSIDUELS (il peut s'agir du GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL) doit mener à bien et documenter une analyse RISQUE/bénéfice du RISQUE RÉSIDUEL individuel ou global par rapport à l'augmentation des bénéfices santé depuis l'incorporation du DISPOSITIF MÉDICAL dans le RÉSEAU TI, et décider d'approuver ou non le RISQUE RÉSIDUEL DU RÉSEAU TI MÉDICAL.

NOTE Voir l'ISO 14971 [4] pour l'analyse RISQUE/bénéfice.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.5 GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et GESTION DE LA CONFIGURATION

4.5.1 PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS

L'ORGANISME RESPONSABLE doit documenter et appliquer un PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS.

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit s'assurer qu'un PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS existe pour le RÉSEAU TI MÉDICAL et que le PROCESSUS inclut une GESTION DES RISQUES.

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit utiliser les résultats du PROCESSUS DE GESTION DES RISQUES pour déterminer l'approbation et l'acceptabilité des modifications au cours du PROCESSUS DE GESTION DU DÉCLANCHEMENT DES MODIFICATIONS.

NOTE Des conséquences indésirables peuvent apparaître lorsque deux ou plus de deux projets parallèles sont insuffisamment coordonnés.

Un PROCESSUS DE GESTION DE LA CONFIGURATION doit être documenté et appliqué afin de contrôler les versions du RÉSEAU TI MÉDICAL lors de TOUS LES PROCESSUS DE GESTION DES RISQUES durant la GESTION DU DÉCLENCHEMENT DES MODIFICATIONS DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.5.2 Décision relative à l'application de la GESTION DES RISQUES

4.5.2.1 Vue d'ensemble

Le PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS doit être initié pour tout nouveau RÉSEAU TI MÉDICAL ou toute modification apportée à un RÉSEAU TI MÉDICAL.

L'ORGANISME RESPONSABLE doit tenir compte de la nature de la modification afin de décider si les exigences sont remplies à l'aide d'une AUTORISATION DE MODIFICATIONS applicable. En l'absence d'AUTORISATION DE MODIFICATIONS applicable, un projet de RÉSEAU TI MÉDICAL doit être initié.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.5.2.2 AUTORISATION DE MODIFICATIONS

Si l'ORGANISME RESPONSABLE décide, à l'issue des activités de GESTION DES RISQUES, qu'une modification de routine spécifique doit être effectuée avec un RISQUE acceptable, soumise à des contraintes spécifiques, alors l'ORGANISME RESPONSABLE peut définir une AUTORISATION DE MODIFICATIONS autorisant ces modifications de routine et précisant les contraintes.

NOTE 1 Par exemple, une AUTORISATION DE MODIFICATIONS pourrait permettre de faire varier, dans une plage donnée, le nombre de DISPOSITIFS MÉDICAUX d'un type spécifique dans un RÉSEAU TI MÉDICAL.

NOTE 2 Les modifications étant toujours effectuées conformément à l'AUTORISATION DE MODIFICATIONS et à ses limites, aucune GESTION DU DÉCLENCHEMENT DES MODIFICATIONS ou GESTION DES RISQUES n'est requise à chaque fois qu'une AUTORISATION DE MODIFICATIONS est utilisée.

Une AUTORISATION DE MODIFICATIONS doit préciser les comptes-rendus qui doivent être conservés pour chacune des modifications autorisées.

Les AUTORISATIONS DE MODIFICATIONS doivent être documentées dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

NOTE 3 LES AUTORISATIONS DE MODIFICATIONS ne peuvent être établies qu'à l'issue du PROCESSUS DE GESTION DES RISQUES (voir 4.4.4.2).

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.5.2.3 Projets du RÉSEAU TI MÉDICAL

L'ORGANISME RESPONSABLE doit établir et maintenir un plan de projet pour l'incorporation d'un nouveau type de DISPOSITIF MÉDICAL au sein d'un RÉSEAU TI, pour les modifications apportées au RÉSEAU TI MÉDICAL, pour les modifications apportées aux DISPOSITIFS MÉDICAUX incorporés dans le RÉSEAU TI MÉDICAL, pour la mise hors service d'un DISPOSITIF MÉDICAL ou d'un RÉSEAU TI MÉDICAL, ou pour toute autre activité susceptible d'introduire un nouveau RISQUE. Le premier plan de projet aurait pour objet le développement d'un nouveau RÉSEAU TI MÉDICAL. Le plan de projet doit fournir:

a) les exigences relatives aux activités de GESTION DES RISQUES comprenant:
   1) les activités pour établir ou mettre à jour les documents du DOSSIER DE GESTION DES RISQUES requis à l'issue de ce projet, tel que le plan de GESTION DES RISQUES ou les autres documents relatifs à la GESTION DES RISQUES;
   2) un plan afin de satisfaire aux exigences stipulées dans le PLAN DE GESTION DES RISQUES pour le(s) RÉSEAU(X) TI MÉDICAL(AUX) affecté(s); et
   3) les activités pour la VÉRIFICATION des mesures de MAÎTRISE DU RISQUE.

b) une description du projet comprenant:
   1) l'identification du(es) RÉSEAU(X) TI MÉDICAL(AUX) développé(s) ou affecté(s) par ce projet;
   2) les spécifications des exigences pour le projet; et
   3) la spécification de l'ensemble minimal de documents requis pour le projet du RÉSEAU TI MÉDICAL.

c) le domaine d'application des modifications prévues sur le RÉSEAU TI MÉDICAL comprenant mais ne se limitant pas à:
   1) la configuration physique et logique du RÉSEAU TI MÉDICAL avant et après les modifications prévues;
   2) le flux d'informations avant et après les modifications prévues;
   3) les composants à ajouter ou à supprimer;
   4) les spécifications des composants du réseau non médical le cas échéant; et
   5) les contraintes sur l'extensibilité du RÉSEAU TI MÉDICAL existant.

Le plan de projet doit être revu lorsque cela est nécessaire afin de refléter les modifications apportées au projet.

Le plan de projet doit être conservé dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL conformément aux PROCESSUS du cycle de vie de la GESTION DES ÉVÉNEMENTS, GESTION DU DÉCLENCHEMENT DES MODIFICATIONS, ET DE LA GESTION DE LA CONFIGURATION.

NOTE Lorsque des modifications sont fréquemment apportées au RÉSEAU TI, le plan de projet peut être établi sous forme de document protocolaire réutilisable comportant tous les éléments essentiels.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.5.3 Mise en service

Le passage du RÉSEAU TI MÉDICAL à "l'environnement réel" (Figure 2) constitue l'objectif de toutes les initiatives de projets ou de modification. Avant la mise en service, l'ORGANISME RESPONSABLE doit revoir le RISQUE RÉSIDUEL DU RÉSEAU TI MÉDICAL.

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL doit examiner tous les résumés des RISQUES RÉSIDUELS des projets ou des modifications afin de déterminer l'acceptabilité du RISQUE associée aux interactions avec des projets ou des modifications récents ou en cours (ex., l'incorporation du DISPOSITIF MÉDICAL au sein d'un RÉSEAU TI opérationnel et évolutif).

Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI doit approuver la modification spécifiée du RÉSEAU TI MÉDICAL avant la mise en service.

L'approbation du RISQUE RÉSIDUEL DU RÉSEAU TI MÉDICAL doit être documentée et les informations relatives à la configuration doivent être enregistrées dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.6 GESTION DES RISQUES du réseau en service

4.6.1 Surveillance

L'ORGANISME RESPONSABLE doit établir et maintenir un PROCESSUS afin de surveiller chacun des RÉSEAUX TI MÉDICAUX pour faire ressortir les RISQUES, l'efficacité des mesures de MAÎTRISE DU RISQUE, ainsi que l'exactitude des estimations initiales du RISQUE.

Les exigences relatives à la surveillance doivent être établies dans le PLAN DE GESTION DES RISQUES du RÉSEAU TI MÉDICAL. Exemples des éléments à surveiller:

a) les modifications de l'environnement (y compris l'environnement local/connecté ainsi que les vulnérabilités de la SÉCURITÉ DES DONNÉES ET DES SYSTÈMES du réseau ou des composants concernés);

b) le retour d'informations liées au fonctionnement/aux performances ex. retour utilisateur, problèmes de vitesse, taux d'erreur élevés, défaillances, attaques de logiciels malveillants;

c) les informations concernant les composants incorporés;

d) les informations relatives à des RÉSEAUX TI MÉDICAUX similaires;

e) les évènements consignés; et

f) l'audit des mesures de MAÎTRISE DU RISQUE non techniques telles que les politiques et les procédures de l'organisme.

Si la surveillance indique une augmentation réelle ou potentielle des RISQUES associés au RÉSEAU TI MÉDICAL ou à ses composants (impact négatif potentiel ou réel), le PROCESSUS DE GESTION DES ÉVÉNEMENTS doit être initié et les résultats significatifs doivent être transmis à la personne concernée de l'ORGANISME RESPONSABLE.

NOTE Dans certains cas, l'ORGANISME RESPONSABLE pourrait se voir demander de transmettre ces observations à des organismes réglementaires.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

4.6.2 Gestion des événements

L'ORGANISME RESPONSABLE doit établir la GESTION DES ÉVÉNEMENTS pour:

a) capturer et documenter les événements négatifs;

b) évaluer les événements et proposer des modifications à travers la GESTION DU DÉCLENCHEMENT DES MODIFICATIONS;

c) tracer toutes les actions de correction et de prévention menant à la fermeture; et

d) rapporter les résultats significatifs au GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL et/ou aux autres personnes de l'ORGANISME RESPONSABLE.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

5 Contrôle des documents

5.1 Procédure de contrôle des documents

Tous les documents impliqués dans le cycle de vie du RÉSEAU TI MÉDICAL doivent être révisés, amendés, revus et approuvés conformément à la procédure de contrôle des documents.

La conformité est vérifiée par examen du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

5.2 DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL

En complément des exigences stipulées dans les autres articles de la présente norme, le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL doit fournir la traçabilité pour chacun des PHÉNOMÈNES DANGEREUX identifiés:

a) l'ANALYSE DU RISQUE;

b) l'ÉVALUATION DU RISQUE;

c) la mise en application et la VÉRIFICATION des mesures de MAÎTRISE DU RISQUE; et

d) l'évaluation de l'acceptabilité de tout RISQUE RÉSIDUEL avec approbation.

NOTE 1 Les comptes-rendus et les autres documents constituant le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL peuvent faire partie d'autres documents et fichiers. Le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL n'a pas besoin de contenir tous les comptes-rendus et tous les autres documents, cependant, il convient qu'il contienne au moins les références ou les indications à la documentation requise. Il convient que l'ORGANISME RESPONSABLE soit capable de rassembler les informations référencées dans le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL de manière opportune.

NOTE 2 Le DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL peut être de tout type ou sous toute forme de support.

NOTE 3 Dans ces organismes où un "cas d'assurance" constitue le moyen d'organiser le DOSSIER DE GESTION DES RISQUES DU RÉSEAU, se référer à l'ISO/CEI 15026-2 [5] (actuellement en cours d'élaboration) pour de plus amples informations.

La conformité est vérifiée par inspection du DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL.

Annexe A
(informative)

Justifications

A.1 Généralités

La convergence entre les DISPOSITIFS MÉDICAUX et les systèmes de gestion de l'information a débouché sur le besoin de modifications en matière de SÉCURITÉ et l'EFFICACITÉ des DISPOSITIFS MÉDICAUX est maintenue suite à leur mise en service. Bien que la responsabilité du fabricant de DISPOSITIFS MÉDICAUX (souvent abrégé en anglais en MDM pour médical device manufacturer) dans la commercialisation de DISPOSITIFS MÉDICAUX surs et efficaces n'ait pas changé, l'environnement (c'est-à-dire le RÉSEAU-TI) dans lequel les DISPOSITIFS MÉDICAUX se trouvent, change constamment. Le fabricant du DISPOSITIF MÉDICAL ne peut pas prévoir toutes les modifications potentielles et n'a aucun moyen de garantir que le DISPOSITIF MÉDICAL fonctionnera correctement dans toutes les situations.

Au même moment, L'ORGANISME RESPONSABLE (souvent abrégé en anglais en HDO pour healthcare delivery organization) possède des exigences relatives à l'efficacité de sa capacité à délivrer des soins médicaux de haute qualité, ainsi qu'à la sécurité et au caractère privé des données du PATIENT devant être obtenus dans le même environnement constamment en modification. Ces exigences ne peuvent être satisfaites sans le fonctionnement correct des DISPOSITIFS MÉDICAUX faisant partie de l'environnement, incorporé dans leur RÉSEAU TI.

La présente Norme internationale reconnaît que la coopération est nécessaire entre les parties impliquées dans la fourniture et la connexion des DISPOSITIFS MÉDICAUX dans les RÉSEAUX IT pour satisfaire à toutes ces exigences compte tenu de l'évolution rapide des technologies à l'heure actuelle. Elle identifie les fonctions et responsabilités nécessaires, et un PROCESSUS afin de gérer le RISQUE engendré par l'incorporation des DISPOSITIFS MÉDICAUX dans l'infrastructure de technologie de l'information de l'organisme délivrant les soins médicaux. Alors que l'ORGANISME RESPONSABLE a la responsabilité des décisions qu'il prend concernant l'incorporation des DISPOSITIFS MÉDICAUX dans les RÉSEAUX TI, ces décisions sont en partie fondées sur des demandes émanant de ses fournisseurs et sur des informations partagées par ces mêmes fournisseurs. Dans certains cas, la documentation mise à disposition lorsque des produits sont commercialisés sera suffisante pour étayer les décisions de l'ORGANISME RESPONSABLE. Dans d'autres cas, l'ORGANISME RESPONSABLE devra obtenir des informations supplémentaires qui pourraient être normalement indisponibles. La présente norme suggère d'utiliser un ACCORD DE RESPONSABILITÉ pour identifier quelles informations sont nécessaires tout au long de la vie du RÉSEAU TI MÉDICAL et les responsabilités pour fournir et contrôler l'accès à ces informations.

Afin de pouvoir prouver à tout moment la conformité aux exigences de la présente norme, il est nécessaire de collecter et de conserver la documentation dans le DOSSIER DE GESTION DES RISQUES pour chacun des RÉSEAUX TI MÉDICAUX.

A.2 Article 3 – Fonctions et responsabilités

Cet article identifie les fonctions et les responsabilités nécessitant de coopérer afin de gérer le RISQUE engendré par l'incorporation des DISPOSITIFS MÉDICAUX dans les RÉSEAUX TI.

L'organisme délivrant les soins médicaux qui possède et utilise le RÉSEAU TI MÉDICAL est entièrement responsable de son fonctionnement. Il s'agit de l'ORGANISME RESPONSABLE. Afin de garantir que la GESTION DES RISQUES est correctement traitée pour le RÉSEAU TI MÉDICAL, la DIRECTION de l'ORGANISME RESPONSABLE doit, selon la présente norme, établir une politique, fournir des ressources et assigner des personnes qualifiées et revoir les résultats des activités liées à la GESTION DES RISQUES. Il est important qu'une personne soit désignée

comme responsable de la réalisation du PROCESSUS DE GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL. L'une des principales responsabilités de la DIRECTION consiste à désigner un GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL et à s'assurer que les autres membres de l'ORGANISME RESPONSABLE coopèrent avec ce dernier afin de gérer les RISQUES engendrés lors de l'incorporation des DISPOSITIFS MÉDICAUX au sein des RÉSEAUX TI.

Etant donné que le concept de RISQUE dépend de l'impact clinique de la défaillance ainsi que de la probabilité de défaillance, les responsabilités des fabricants de DISPOSITIFS MÉDICAUX sont différentes de celles de fournisseurs d'autres technologies de l'information. Les fabricants de DISPOSITIFS MÉDICAUX comprennent l'impact clinique d'une défaillance du réseau basée sur L'EMPLOI PRÉVU du DISPOSITIF MÉDICAL, tandis que les fournisseurs informatiques ne peuvent fournir des informations que sur les modes de défaillances, les probabilités de défaillance, etc., des appareils informatiques. C'est pourquoi ces deux fonctions sont abordées de manière indépendante.

Le fabricant de DISPOSITIF MÉDICAL doit mettre à disposition des DOCUMENTS D'ACCOMPAGNEMENT. Ces DOCUMENTS D'ACCOMPAGNEMENT doivent être mis à la disposition de l'ORGANISME RESPONSABLE dans la mesure où le contenu de ces documents est essentiel pour les activités de GESTION DES RISQUES de l'ORGANISME RESPONSABLE au cours de l'incorporation des DISPOSITIFS MÉDICAUX dans le RÉSEAU TI. Il est noté qu'il peut y avoir différentes compréhensions du contenu et de l'étendue des DOCUMENTS D'ACCOMPAGNEMENT. C'est pour cette raison que les exigences 3.5 a) à 3.5 f) définissent le contenu minimal de tels DOCUMENTS D'ACCOMPAGNEMENT dans la mesure où certains DISPOSITIFS MÉDICAUX n'ont pas à être conformes à la CEI 60601-1 (par exemple les dispositifs médicaux IVD). Toutefois, l'application du 14.13 de la CEI 60601-1:2005 [1] pour satisfaire à ces exigences pour les fabricants de DISPOSITIFS MÉDICAUX est fortement encouragée.

Les modes de défaillance du réseau et leur probabilité dépendent également des éléments hors du contrôle à la fois des fabricants de DISPOSITIFS MÉDICAUX et des fournisseurs d'autres technologies de l'information tels que la conception du système, la configuration, la topologie, les processus et les procédures informatiques, ainsi que l'utilisation réelle (par rapport à celle prévue) du DISPOSITIF MÉDICAL, etc. Par conséquent, seul l'ORGANISME RESPONSABLE possède la visibilité finale sur les RISQUES du RÉSEAU TI MÉDICAL et assume la responsabilité principale en matière de GESTION DES RISQUES du DISPOSITIF TI MÉDICAL.

A.3 Article 4 GESTION DES RISQUES du cycle de vie des RÉSEAUX TI MÉDICAUX

L'un des principes fondamentaux de la présente norme est que le RISQUE doit être pris en compte pour toutes les modifications avant qu'elles soient apportées à un RÉSEAU TI MÉDICAL. La présente norme exige qu'une GESTION DES RISQUES soit effectuée sur les RÉSEAUX TI MÉDICAUX. Il peut exister plusieurs RÉSEAUX TI MÉDICAUX par ORGANISME RESPONSABLE. Les activités de GESTION DES RISQUES exigées par le présent document sont largement fondées sur celles de l'ISO 14971 [4] mais elles vont au-delà de la SÉCURITÉ telle qu'elle est définie dans l'ISO 14971 pour inclure la gestion du RISQUE sur l'EFFICACITÉ et du risque sur la SÉCURITÉ DES DONNÉES et des SYSTÈMES. Ceci nécessite quelques modifications des termes définis dans l'ISO 14971. Pour la présente norme, la notion de DOMMAGE est étendue pour inclure la réduction d'EFFICACITÉ et les brèches dans la sécurité. Ceci implique que la SÉCURITÉ spécifie quel type de DOMMAGE est inclus dans le RISQUE. Ainsi la définition de SÉCURITÉ devient absence de RISQUE inacceptable de blessure physique ou d'atteinte à la santé des personnes ou de dommages sur les biens ou l'environnement. Avec ces modifications, les activités de GESTION DES RISQUES de l'ISO 14971 peuvent être appliquées pour la présente norme. Dans la mesure où elles sont appliquées à la gestion du cycle de vie d'un RÉSEAU TI MÉDICAL, elles sont décrites dans le contexte d'un RÉSEAU TI MÉDICAL qui fonctionne. L'article 4 se divise en paragraphes mettant en parallèle la répartition des activités de GESTION DES RISQUES durant la modification d'un RÉSEAU TI MÉDICAL ou durant la phase d'environnement réel d'un RÉSEAU TI MÉDICAL. Le Tableau A.1 représente la relation des activités de la GESTION DES RISQUES de l'ISO 14971 avec celles de la présente norme.

Paragraphe 4.2 – GESTION DES RISQUES DE L'ORGANISME RESPONSABLE

Le paragraphe 4.2 décrit les activités et les produits livrables qui sont exigés au niveau de l'ORGANISME RESPONSABLE. Ces produits à livrer s'appliquent à tous les RÉSEAUX TI MÉDICAUX au sein de l'ORGANISME RESPONSABLE.

Paragraphe 4.3 – Planification et documentation de la GESTION DES RISQUES DU RÉSEAU TI MÉDICAL

Le paragraphe 4.3 décrit les activités et éléments requis par RÉSEAU TI MÉDICAL afin que les activités liées à la GESTION DES RISQUES débutent.

Tableau A.1 – Relations entre l'ISO 14971 et la CEI 80001-1

ISO 14971:2007 section		CEI 80001-1 section	
4	**ANALYSE DU RISQUE**		
4.1	PROCESSUS D'ANALYSE DU RISQUE	n/a	
4.2	EMPLOI PRÉVU et identification des caractéristiques liées à la SÉCURITÉ		
4.3	Identification des PHÉNOMÈNES DANGEREUX	4.4.2	**ANALYSE DU RISQUE**
4.4	Estimation du ou des RISQUE(S) pour chaque situation dangereuse – "Les séquences raisonnablement prévisibles ou les combinaisons d'évènements qui peuvent donner lieu à une situation dangereuse doivent être prises en compte et la ou les situation(s) qui en résulte(nt) doit/doivent être consignée(s)" – "Pour chaque situation dangereuse identifiée, le ou les RISQUE(S) associé(s) doit/doivent être estimé(s)"	4.4.2	Pour chaque PHÉNOMÈNE DANGEREUX identifié, l'ORGANISME RESPONSABLE doit estimer les RISQUES associés …"
5	**ÉVALUATION DU RISQUE**	4.4.3	**ÉVALUATION DU RISQUE**
6	**MAÎTRISE DU RISQUE**	4.4.4	**MAÎTRISE DU RISQUE**
6.1	Réduction des RISQUES	n/a	
6.2	Analyse d'option de MAÎTRISE DU RISQUE	4.4.4.1	Analyse optionnelle de MAÎTRISE DU RISQUE
		4.4.4.2	Mesures DE MAÎTRISE DU RISQUE
6.3	Mise en place des mesures de MAÎTRISE DU RISQUE	4.4.4.3	Mise en place des mesures de MAÎTRISE DU RISQUE
		4.4.4.4	VÉRIFICATION des mesures de MAÎTRISE DU RISQUE
6.4	Evaluation du RISQUE RÉSIDUEL		(traité en 4.4.4)
6.5	Analyse du rapport bénéfice /RISQUE		(traité en 4.4.4 et 4.4.5)
6.6	RISQUES découlant des mesures de MAÎTRISE DU RISQUE	4.4.4.5	Nouveaux RISQUES décelés suite à la MAÎTRISE DU RISQUE
7	**Evaluation de l'acceptabilité globale du RISQUE RÉSIDUEL**	4.4.5	**Evaluation et compte-rendu du RISQUE RÉSIDUEL**

Paragraphe 4.5 – GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et GESTION DE LA CONFIGURATION

Le paragraphe 4.5 décrit les activités de GESTION DES RISQUES requises lors de la modification d'un RÉSEAU TI MÉDICAL avant qu'il n'entre en phase d'environnement de production. Ceci inclut la modification d'un RÉSEAU TI MÉDICAL existant ainsi que l'élaboration initiale d'un RÉSEAU TI MÉDICAL ou la transformation d'un RÉSEAU TI non MÉDICAL en RÉSEAU TI MÉDICAL. A cette étape, les activités de GESTION DES RISQUES traditionnelles surviennent dans le contexte d'un projet. Le GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL est responsable de la consolidation de toutes les activités de GESTION DES RISQUES du projet dans un seul DOSSIER DE GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL.

Certaines mesures de MAÎTRISE DU RISQUE définies pour le RÉSEAU TI MÉDICAL peuvent inclure des activités durant la phase d'environnement réel, telles que les procédures cliniques afin d'atténuer les pannes de courant du réseau.

Pour les activités qui sont réalisées de manière fréquente, il est souhaitable d'éviter une répétition inutile de la GESTION DES RISQUES. La présente norme mentionne les AUTORISATIONS DE MODIFICATION comme une manière de répondre à ce besoin. Si la GESTION DES RISQUES démontre qu'une modification de routine, par exemple l'ajout d'un utilisateur, peut être réalisée avec un RISQUE acceptable, dans le respect de certaines contraintes (par exemple une limite quant au type et au nombre d'utilisateurs), alors l'ORGANISME RESPONSABLE peut définir une AUTORISATION DE MODIFICATION qui permet de telles modifications de routine et il spécifie des contraintes.

Paragraphe 4.6 – GESTION DES RISQUES DU RÉSEAU ACTIF

Le paragraphe 4.6 décrit les activités de GESTION DES RISQUES requises après mise en service du RÉSEAU TI MÉDICAL (environnement réel).

La surveillance désigne la revue en cours de toutes les activités de GESTION DES RISQUES et les CONTRÔLES DES RISQUES mis en place afin d'atteindre des RISQUES acceptables lors de l'utilisation (environnement réel) de RÉSEAU(X) TI MÉDICAL(AUX). Elle prouve que les RISQUES globaux associés aux PROPRIÉTÉS CLÉS dans le(s) RÉSEAU(X) TI MÉDICAL(AUX) sont acceptables.

La GESTION DES ÉVÉNEMENTS décrit les actions requises lorsqu'un événement négatif potentiel ou réel survient au cours de l'utilisation d'un RÉSEAU TI MÉDICAL dans l'environnement réel.

Annexe B
(informative)

Vue d'ensemble des relations entre les intervenants dans la GESTION DES RISQUES

La Figure B.1 fournit une vue d'ensemble des différentes fonctions et relations impliquées dans la réalisation d'un effort de GESTION DES RISQUES impliquant l'incorporation de DISPOSITIFS MÉDICAUX dans les RÉSEAUX TI.

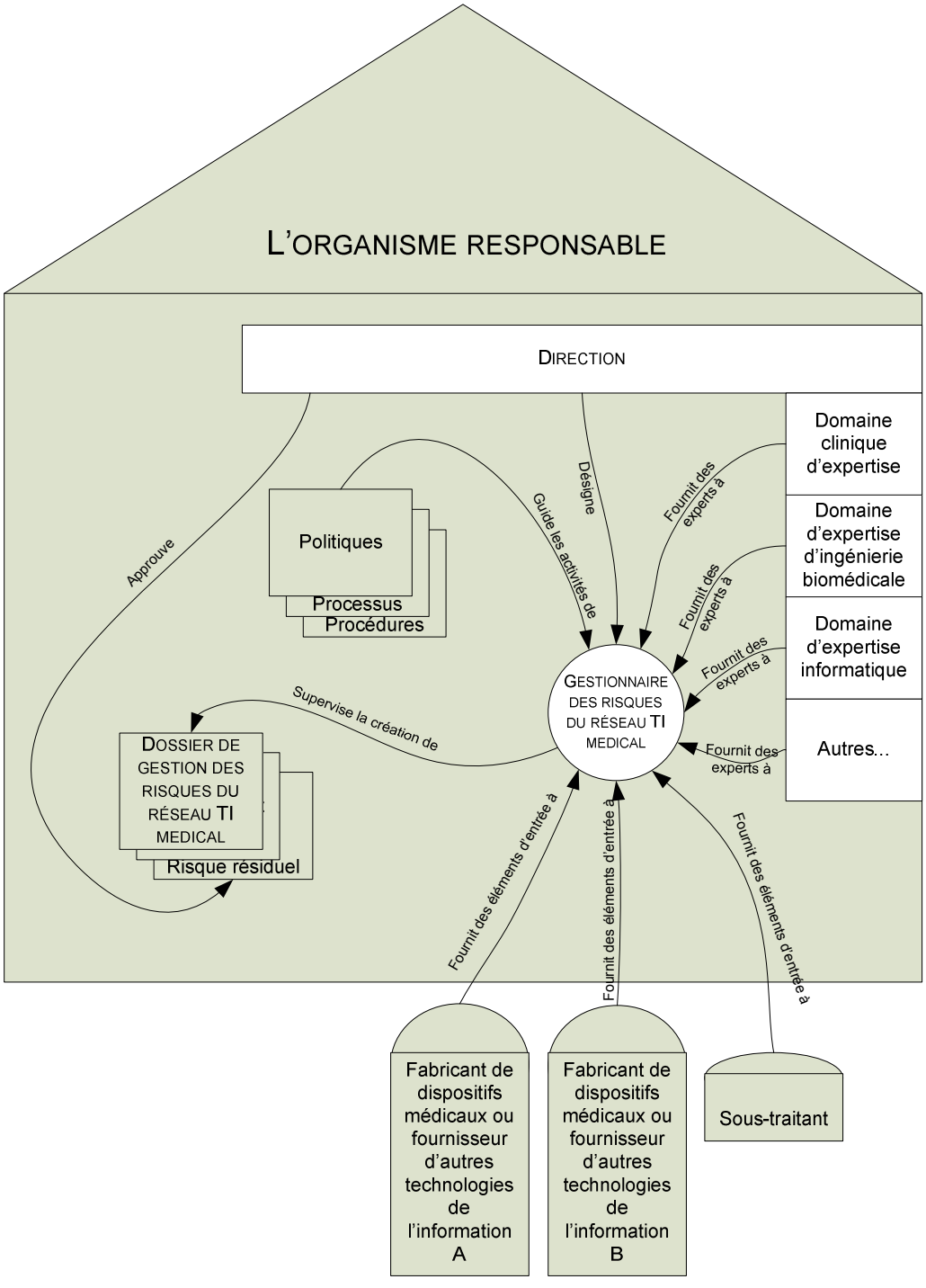


Figure B.1 – Vue d'ensemble des fonctions et des relations

Annexe C
(informative)

Directive relative au champ d'application

C.1 Vue d'ensemble

La définition du champ d'application pour la CEI 80001-1 fournit un point de départ dans la description des RÉSEAUX TI relevant du domaine d'application de la norme. Ce document fournit des directives supplémentaires y compris des exemples de réseaux TI relevant ou non du domaine d'application.

C.2 Dans quels cas appliquer la présente norme

Le Tableau C.1 fournit des directives concernant plusieurs scénarios de RÉSEAUX TI pouvant être rencontrés dans un environnement clinique et indique si les PROCESSUS de la CEI 80001-1 doivent leur être appliqués.

Tableau C.1 – Scénarios de réseaux TI pouvant être rencontrés dans un environnement clinique

Configur-ation système	Description du scénario		Composants du réseau	Réseau	Responsabilité du réseau	Norme
1	a	DISPOSITIFS MÉDICAUX d'un fabricant de DISPOSITIFS MÉDICAUX et DISPOSITIFS NON MÉDICAUX incorporés par le même fabricant de DISPOSITIFS MÉDICAUX et installés comme requis par le fabricant de DISPOSITIFS MÉDICAUX sur un RÉSEAU TI isolé.	DISPOSITIF(S) MÉDICAL(UX) et non MÉDICAL(AUX) provenant d'un seul fabricant de DISPOSITIFS MÉDICAUX	Physiquement isolé	Fabricant de DISPOSITIFS MÉDICAUX	14971
	b	DISPOSITIFS MÉDICAUX de plusieurs fabricants de DISPOSITIFS MÉDICAUX et de DISPOSITIFS NON MÉDICAUX incorporés par un seul fabricant de DISPOSITIFS MÉDICAUX et installés comme exigé par ce fabricant de DISPOSITIFS MÉDICAUX sur un RÉSEAU TI isolé.	DISPOSITIF(S) MÉDICAL(UX) et non MÉDICAL(AUX) provenant de plusieurs fabricants de DISPOSITIFS MÉDICAUX	Physiquement isolé	Fabricant de DISPOSITIFS MÉDICAUX	14971
2	a	DISPOSITIFS MÉDICAUX et non MÉDICAUX incorporés par un fabricant de DISPOSITIFS MÉDICAUX et DISPOSITIFS MÉDICAUX et non MÉDICAUX incorporés par d'autres fabricants de DISPOSITIFS MÉDICAUX interconnectés sur le même RÉSEAU TI par un tiers (tel qu'un hôpital).	DISPOSITIF(S) médical(aux) et non MÉDICAL(AUX) provenant de plusieurs fabricants de DISPOSITIFS MÉDICAUX	Partagé	ORGANISME RESPONSABLE	80001-1
	b	DISPOSITIFS MÉDICAUX et non MÉDICAUX incorporés par un fabricant de DISPOSITIFS MÉDICAUX et DISPOSITIFS MÉDICAUX et non MÉDICAUX incorporés par d'autres fabricants de DISPOSITIFS MÉDICAUX ainsi que des DISPOSITIFS MÉDICAUX et applications interconnectés sur un RÉSEAU TI PARTAGÉ par un tiers (tel qu'un hôpital).	DISPOSITIF(S) MÉDICAL(UX) et non MÉDICAL(AUX) provenant de plusieurs fabricants de DISPOSITIFS MÉDICAUX et de plusieurs fabricants de DISPOSITIFS non MÉDICAUX	Partagé	ORGANISME RESPONSABLE	80001-1

Configur-ation système	Description du scénario		Composants du réseau	Réseau	Responsabilité du réseau	Norme
3		Installations avec des DISPOSITIFS non MÉDICAUX provenant de plusieurs fabricants à l'aide du RÉSEAU TI pour la transmission des Informations de Santé Protégées électroniques (ePHI).	Plusieurs fabricants de DISPOSITIFS non MÉDICAUX	Partagé	ORGANISME RESPONSABLE	En dehors du domaine d'application de 80001-1 [a]

[a] Les réglementations nationales locales relatives à la sécurité des données médicales s'appliquent, cependant, l'ORGANISME RESPONSABLE peut également choisir d'appliquer la CEI 80001-1.

Certains exemples peuvent aider à mieux comprendre les différents types de réseaux listés dans le Tableau C.1:

- Configuration 1a – Dispositifs de surveillance des PATIENTS sur leur propre réseau isolé ou les mêmes dispositifs dotés d'une passerelle avec le RÉSEAU TI de l'hôpital dans le cas d'utilisations de DISPOSITIFS non MÉDICAUX.
- Configuration 1b – Dispositifs de surveillance des PATIENTS provenant du vendeur A combinés aux dispositifs d'infusion rattachés au réseau provenant du vendeur B fournis en tant que solution contrôlée intégrée par un seul vendeur (A, B ou C).
- Configuration 2a – Plusieurs DISPOSITIFS MÉDICAUX provenant de différents fabricants de DISPOSITIFS MÉDICAUX placés sur un RÉSEAU TI commun par un hôpital.
- Configuration 2b – Dispositifs d'infusion rattachés au réseau sur un RÉSEAU TI partagé avec d'autres applications hospitalières, et/ou dispositifs de surveillance du PATIENT sur un réseau isolé doté d'une passerelle avec le RÉSEAU TI de l'hôpital dans le cas d'utilisations de DISPOSITIFS MÉDICAUX telles que le compte-rendu des alertes.
- Configuration 3 – Systèmes hospitaliers communicant les caractéristiques démographiques du PATIENT et les Informations de Santé Protégées électroniques (ePHI).

Annexe D
(informative)

Relation avec l'ISO/CEI 20000-2:2005, *Technologies de l'information – Gestion des services – Partie 2: Code de pratique*

D.1 Généralités

La CEI 80001-1 applique le concept de GESTION DES RISQUES du cycle de vie au RÉSEAU TI pour l'incorporation des DISPOSITIFS MÉDICAUX. Comme c'est le cas pour les RÉSEAUX TI, les RÉSEAUX TI MÉDICAUX peuvent être des systèmes très complexes et très dynamiques pour lesquels la surveillance conduit souvent à des besoins de modifications. La mise en œuvre de ces modifications nécessite une préparation soigneuse. Dans la plupart des cas, compte tenu de leur réglementation couverte par des lois sur les systèmes de qualité et la validation, les fabricants de DISPOSITIFS MÉDICAUX sont moins capables de modifier rapidement leurs DISPOSITIFS MÉDICAUX. Compte tenu de la réglementation, les modifications et la maintenance exigent des stratégies strictement formelles et des procédures qui nécessitent souvent l'implication directe du fabricant de DISPOSITIFS MÉDICAUX. Dans le cas des RÉSEAUX TI MÉDICAUX, l'ORGANISME RESPONSABLE et le fabricant de DISPOSITIFS MÉDICAUX ont tous les deux besoin de reconnaître ces contraintes, différentes par nature, sur la gestion du service. En outre, l'incorporation des DISPOSITIFS MÉDICAUX peut conduire à une co-dépendance du RÉSEAU TI MÉDICAL et des DISPOSITIFS MÉDICAUX, de telle sorte que la modification de l'un entraîne le besoin de modification de l'autre.

La GESTION DES RISQUES du cycle de vie dans un RÉSEAU TI MÉDICAL doit être menée dans le contexte des conditions de fonctionnement spécifiques nécessaires pour une délivrance efficace des soins médicaux. C'est pourquoi les concepts de la gestion de service informatique comme décrits dans l'ISO/CEI 20000-2 [10] ont été révisés pour satisfaire aux exigences de la CEI 80001-1. La présente Annexe fournit une vue d'ensemble simple de la relation entre la CEI 80001-1 et l'ISO/CEI 20000-2 pour aider dans la recherche de stratégies de service qui pourraient répondre aux besoins de service d'un RÉSEAU TI MÉDICAL. Ces informations sont également destinées à aider pour la communication entre les parties responsables des RÉSEAUX TI et des DISPOSITIFS MÉDICAUX (c'est-à-dire l'ORGANISME RESPONSABLE, le fabricant de DISPOSITIFS MÉDICAUX et les fournisseurs d'autres technologies informatiques).

La conformité à l'ISO/CEI 20000-2 [10] n'est pas équivalente à la conformité à la CEI 80001-1.

D.2 Terminologie et définitions

Lorsque les DISPOSITIFS MÉDICAUX nécessitent une maintenance, une réparation ou une modification et éventuellement un remplacement, les RÉSEAUX TI ont des incidents et des problèmes devant être pris en charge, ainsi que des modifications (majeures) nécessitant une mise en application précise. Il existe de nombreuses similarités en matière de service entre le(s) DISPOSITIF(S) MÉDICAL(AUX) et le(s) RÉSEAU(X) TI. Pour information, la Figure D.1 de l'ISO/CEI 20000-1:2005 [10] indique la relation entre les processus de services pour les RÉSEAUX TI.

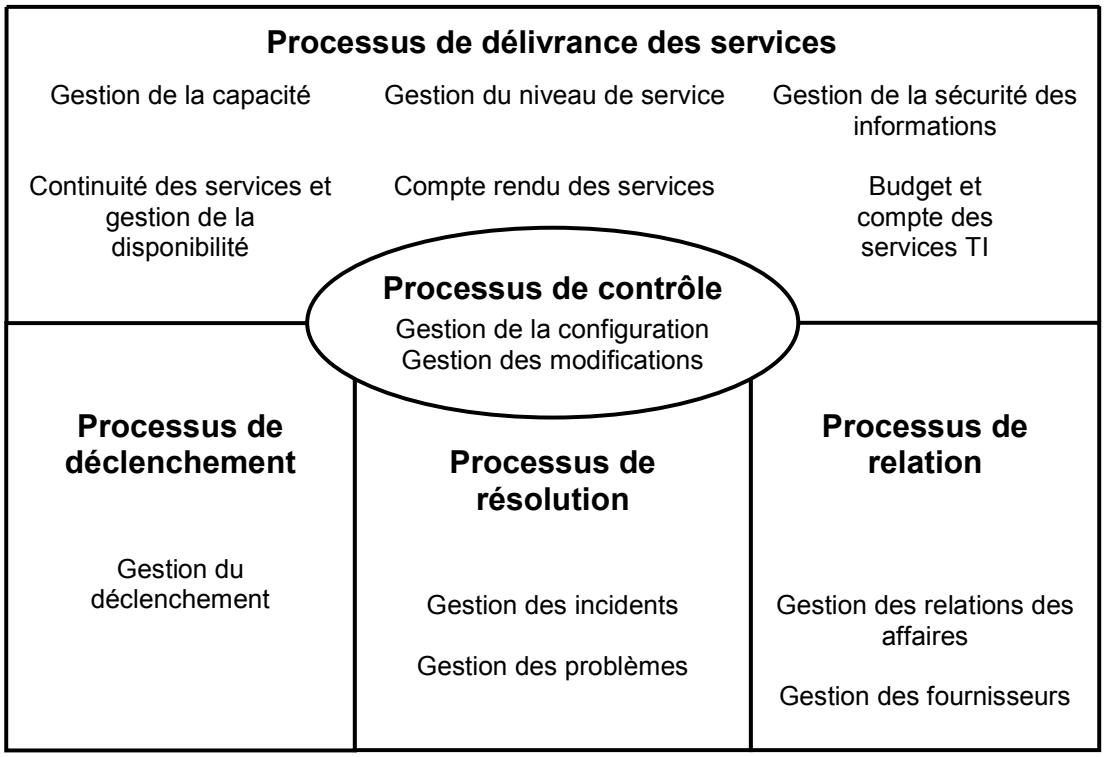


Figure D.1 – Processus de gestion des services

(ISO/CEI 20000-1:2005, Figure 1)

Le Tableau D.1 met en correspondance la terminologie ainsi que les sections de la CEI 80001-1 avec celles de l'ISO/CEI 20000-1 et de l'ISO/CEI 20000-2. Les numéros indiquent la section dans les normes ultérieures.

Tableau D.1 – Relations entre la CEI 80001-1 et l'ISO/CEI 20000-1:2005 ou l'ISO/CEI 20000-2:2005

CEI 80001-1	ISO/CEI 20000-1:2005 ou ISO/CEI 20000-2:2005
2.4 GESTION DE LA CONFIGURATION Dans la CEI 80001-1, LA GESTION DE LA CONFIGURATION est un PROCESSUS mémorisé dans la CMDB.	**2.5 base de données de gestion des configurations** La CMDB désigne la base de données utilisée pour la gestion de la configuration. [ISO/CEI 20000-1:2005]
2.7 GESTION DES ÉVÈNEMENTS La nature des événements n'est pas définie dans le document 80001-1. Ils se réfèrent à la fois au RÉSEAU TI et au DISPOSITIF MÉDICAL	**2.7 incident** Les incidents et les problèmes se rapportent tous aux événements gérés par la GESTION DES ÉVÉNEMENTS dans la CEI 80001-1. [ISO/CEI 20000-1:2005]
2.21 ACCORD DE RESPONSABILITÉ Un accord entre par exemple les fournisseurs, les fabricants, le fournisseur de services, l'intégrateur du système et l'organisme responsable	**2.13 contrat de service (SLA pour *service level agreement*);** **2.14 gestion des services** Définit la relation entre le propriétaire d'un réseau TI et le fournisseur de services [ISO/CEI 20000-1:2005]
2.22 ORGANISME RESPONSABLE	**2.15 fournisseur de services** L'ORGANISME RESPONSABLE doit certifier le fournisseur de services du RÉSEAU TI dans sa politique [ISO/CEI 20000-1:2005]
2.29 DOSSIER DE GESTION DES RISQUES	**2.9 enregistrement; 2.3 enregistrement d'un changement; 2.11 demande de changement** élément(s) du DOSSIER DE GESTION DES RISQUES **2.5 base de données de gestion des configurations (CMDB pour *configuration management database*)** élément du DOSSIER DE GESTION DES RISQUES (description des avantages) NOTE Le DOSSIER DE GESTION DES RISQUES peut être stocké dans une base de données y compris la CMDB [ISO/CEI 20000-1:2005]
3.3 Responsabilités de la DIRECTION	**3.1 Responsabilité de la direction** Les deux normes traitent des responsabilités de gestion supérieure. L'ISO/CEI 20000-1:2005 et l'ISO/CEI 20000-2:2005 laissent plus de liberté d'organisation.
3.4 GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL Le gestionnaire des RISQUES est responsable du PROCESSUS DE GESTION DES RISQUES.	**3.1 Responsabilité de la direction** La GESTION DES RISQUES n'est pas considérée comme une tâche en matière de gestion **6.6.7 Documents et comptes-rendus** Il convient que les comptes-rendus soient analysés. Dans la CEI 80001-1, il s'agit de la responsabilité du GESTIONNAIRE DES RISQUES du RÉSEAU TI MÉDICAL [ISO/IEC 20000-2:2005]
3.5Fabricant(s) de DISPOSITIFS MÉDICAUX; **3.6 Fournisseurs d'autres technologies de l'information** Ces sections décrivent les informations à fournir via les fournisseurs à l'ORGANISME RESPONSABLE	**7.1 Processus de gestion des relations – Généralités** **6.6.5 Sécurité et disponibilité des informations** [ISO/IEC 20000-2:2005] **7.3 Gestion des fournisseurs** Les deux normes exigent que les relations soient formalisées par contrat. Les sections 6.6.5 et 7.3 traitent des fournisseurs des composants du RÉSEAU TI MÉDICAL.
4.2.1 Politique de GESTION DES RISQUES pour l'incorporation des DISPOSITIFS MÉDICAUX	**3.1 Responsabilité de la direction**
4.2.2 PROCESSUS DE GESTION DES RISQUES Couvre la SÉCURITÉ, l'EFFICACITÉ et la SÉCURITÉ DES DONNÉES ET DES SYSTÈMES	**6.6.3 Pratiques d'appréciation du risque de sécurité** [ISO/IEC 20000-2:2005] La sécurité est un sous-ensemble des PROPRIÉTÉS CLÉS d'un RÉSEAU TI MÉDICAL. La CEI 80001-1 fournit le PROCESSUS général de GESTION DES RISQUES pour le RÉSEAU TI.
4.3 Planification et documentation de la GESTION DES RISQUES DU RÉSEAU TI MÉDICAL	**4.1 Planification de la gestion des services (Planifier);** **4.4.2 Gestion des améliorations;** **5.1 Sujets à prendre en compte** L'ISO/CEI 20000 peut comprendre la GESTION DES RISQUES. La CEI 80001-1 définit les exigences relatives à la gestion des services pour les RÉSEAUX TI MÉDICAUX.

CEI 80001-1	ISO/CEI 20000-1:2005 ou ISO/CEI 20000-2:2005
4.3.2 Description des avantages liés aux RISQUES	**6.6.2 Identification et classification des éléments d'actifs informationnels** Il convient que le domaine d'application comprenne toutes les PROPRIÉTÉS CLÉS
4.3.3 Documentation relative au RÉSEAU TI MÉDICAL Cette section spécifie les informations relatives au PROCESSUS DE GESTION DES RISQUES.	**4.1.1 Domaine d'application de la gestion des services; 6.6.2 Identification et classification des éléments d'actifs informationnels** Le contenu des informations recoupe le paragraphe 4.3.3 de la CEI 80001-1.
4.3.4 ACCORD DE RESPONSABILITÉ	**7.3 Gestion des fournisseurs (1er alinéa)** Les deux sections visent à clarifier les intentions de collaboration de tous les intervenants correspondants
4.3.5 Plan de GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL	**6.6.3 Pratiques d'appréciation du risque de sécurité** **La sécurité est un sous-ensemble des PROPRIÉTÉS CLÉS d'un RÉSEAU TI MÉDICAL.** La CEI 80001-1 fournit le PROCESSUS général de GESTION DES RISQUES pour le RÉSEAU TI.
4.4.4 MAÎTRISE DU RISQUE	**9.1.5 Vérification et audit de la configuration; 9.2.2 Planification et implémentation** L'ISO/CEI 20000 couvre une large gamme d'éléments nécessitant la vérification. La VÉRIFICATION des mesures de MAÎTRISE DU RISQUE est élaborée dans la CEI 80001-1.
4.5 GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et GESTION DE LA CONFIGURATION	**9 Processus de contrôle; 10 Processus de mise en production** La gestion des modifications et de la configuration ainsi que le déclenchement et la mise en service sont couverts dans les Articles 9 et 10. L'Article 4 de la CEI 80001-1 décrit les activités de GESTION DES RISQUES comme incluses dans ces PROCESSUS
4.5.2.3 Projets du RÉSEAU TI MÉDICAL Les modifications importantes nécessitent un projet afin d'évaluer les RISQUES avant mise en application de la modification.	**9.2.1 Planification et implémentation** L'ISO/CEI 20000 indique toutes les modifications prévues avant mise en application. La CEI 80001-1 exige que l'ensemble des modifications fassent l'objet d'une gestion des risques incluant la planification.
4.5.3 Mise en service	**9.2.1 Planification et implémentation; 10.1.6 Vérification et acceptation du déclenchement** La CEI 80001-1 assigne la responsabilité d'approbation au GESTIONNAIRE DES RISQUES du RÉSEAU TI MÉDICAL.
4.6.1 Surveillance	**10.1.8 Sortie, distribution et installation; 10.1.9 Post déclenchement et sortie** La surveillance peut se rapporter aux mesures de CONTRÔLE organisationnel ou technique DES RISQUES
5.1 Procédure de contrôle des documents	**3.2 Exigences relatives à la documentation**
5.2 DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL	**5.2 Enregistrement d'un changement; 6.6.7 Documents et enregistrements; 10.1.7 Documentation**

Bibliographie

[1] CEI 60601-1:2005, *Appareils électromédicaux – Partie 1: Exigences générales pour la sécurité de base et les performances essentielles*

[2] CEI 61907:2009, *Ingénierie de la sûreté de fonctionnement des réseaux de communication*

[3] CEI 62304:2006, *Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel*

[4] ISO 14971:2007, *Dispositifs médicaux – Application de la gestion des risques aux dispositifs médicaux*

[5] ISO/CEI 15026-2: —[2)], *Ingénierie du logiciel et des systèmes -- Assurance du logiciel et des systèmes – Partie 2: Cas d'assurance*

[6] ISO/CEI 15408 (toutes les parties), *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI*

[7] ISO 16484-2:2004, *Systèmes de gestion technique du bâtiment – Partie 2: Equipement*

[8] ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[9] ISO/CEI 20000-1:2005, *Technologies de l'information – Gestion des services – Partie 1: Spécifications*

[10] ISO/CEI 20000-2:2005, *Technologies de l'information – Gestion des services – Partie 2: Code de pratique*

[11] ISO 31000:2009, *Management du risque – Principes et lignes directrices*

[12] GHTF/SG1/N29R16:2005, *Information Document Concerning the. Definition of the Term "Medical Device"*. Groupe de Travail d'Harmonisation Universelle (GHTF) – Groupe de Travail 1 (SG1)

2) A publier.

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