IEC 80001-1

Edition 2.0 2021-09

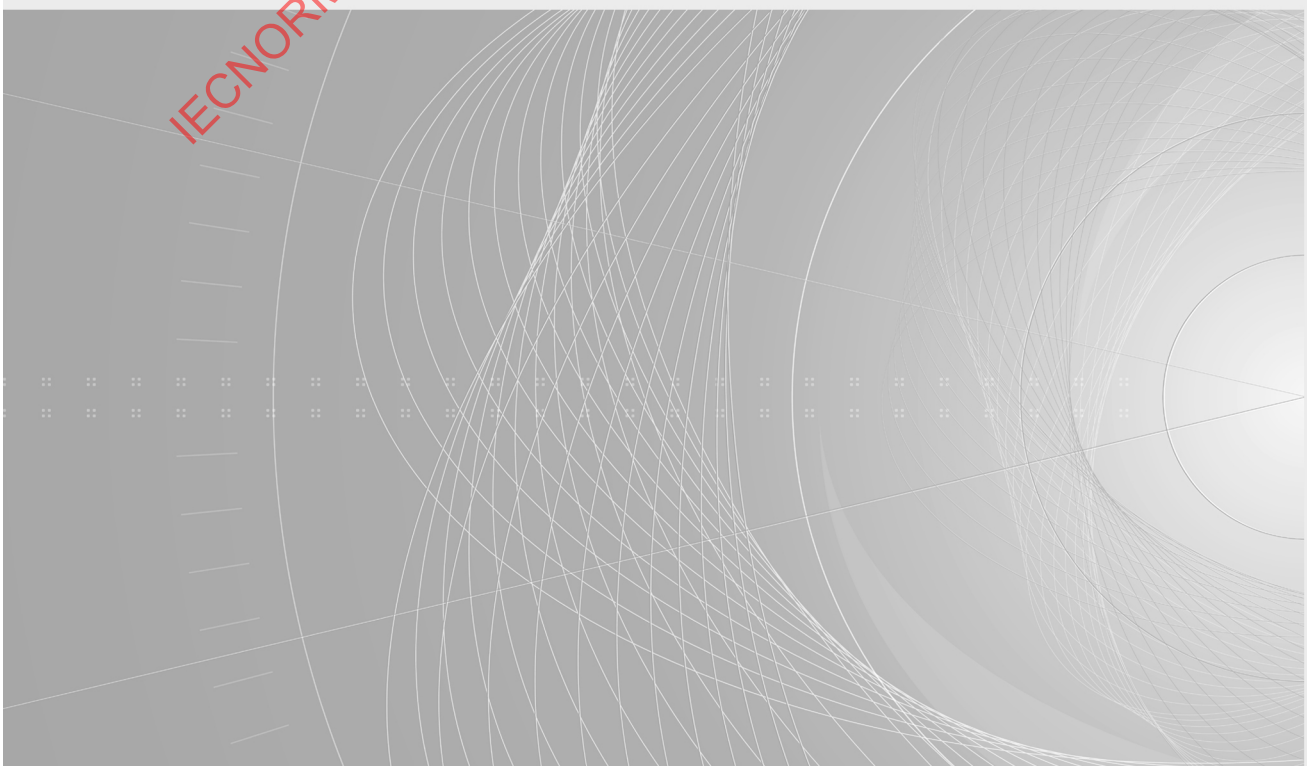
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux – Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés



IEC 80001-1:2021-09 en-fr)

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

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

IEC 80001-1

Edition 2.0 2021-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux – Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 11.040.01; 35.240.80

ISBN 978-2-8322-9748-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

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 of ISO Technical Committee 215: Health informatics.

It is published as a double logo standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) structure changed to better align with ISO 31000;
b) establishment of requirements for an ORGANIZATION in the application of RISK MANAGEMENT;

c) communication of the value, intention and purpose of RISK MANAGEMENT through principles that support preservation of the KEY PROPERTIES during the implementation and use of connected HEALTH SOFTWARE and/or HEALTH IT SYSTEMS.

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

FDIS	Report on voting
62A/1434/FDIS	62A/1448/RVD

Full information on the voting for the approval of this document can be found in the report on voting indicated in the above table.

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

In this document, the following print types are used:

- requirements and definitions: roman type;
- *test specifications: italic type*;
- informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type;
- TERMS DEFINED IN CLAUSE 3 OF THIS DOCUMENT OR AS NOTED ARE PRINTED IN SMALL CAPITALS.

In referring to the structure of this document, the term

- “clause” means one of the five numbered divisions within the table of contents, inclusive of all subdivisions (e.g. Clause 5 includes subclauses 5.1, 5.2, etc.);
- “subclause” means a numbered subdivision of a clause (e.g. 5.1, 5.2 and 5.3 are all subclauses of Clause 5).

References to clauses within this document are preceded by the term “Clause” followed by the clause number. References to subclauses within this particular standard are by number only.

In this document, the conjunctive “or” is used as an “inclusive or” so a statement is true if any combination of the conditions is true.

The verbal forms used in this document conform to usage described in Clause 7 of the ISO/IEC Directives, Part 2. For the purposes of this document, the auxiliary verb:

- “shall” means that compliance with a requirement or a test is mandatory for compliance with this document;
- “should” means that compliance with a requirement or a test is recommended but is not mandatory for compliance with this document;
- “may” is used to describe a permissible way to achieve compliance with a requirement or test.

A list of all parts of the IEC 80001 series, published under the general title *Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software,* can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

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

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

IMPORTANT – The "colour inside" logo on the cover page of this document 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

HEALTHCARE DELIVERY ORGANIZATIONS rely on safe, effective and secure systems as business-critical factors. However, ineffective management of the implementation and use of connected systems can threaten the ability to deliver health services.

Connected systems that deliver health services, generally involve multiple software applications, various medical devices and complex HEALTH IT SYSTEMS that rely upon shared infrastructure including wired or wireless networks, point to point connections, application servers and data storage, interface engines, security and performance management software, etc. These HEALTH IT INFRASTRUCTURES are often used for both clinical (e.g. patient monitoring systems) and non-clinical organizational functions (e.g. accounting, scheduling, social networking, multimedia, file sharing). These connected systems can involve small departmental networks to large integrated infrastructures spanning multiple locations as well as cloud-based services operated by third parties. The requirements in this document are intended for multiple stakeholders involved in the application of RISK MANAGEMENT to systems that include HEALTH IT SYSTEMS and / or HEALTH IT INFRASTRUCTURE.

Within the context of ISO 81001-1, this document covers the generic lifecycle phase “implementation and clinical use” (see the lifecycle diagram in Figure 1).

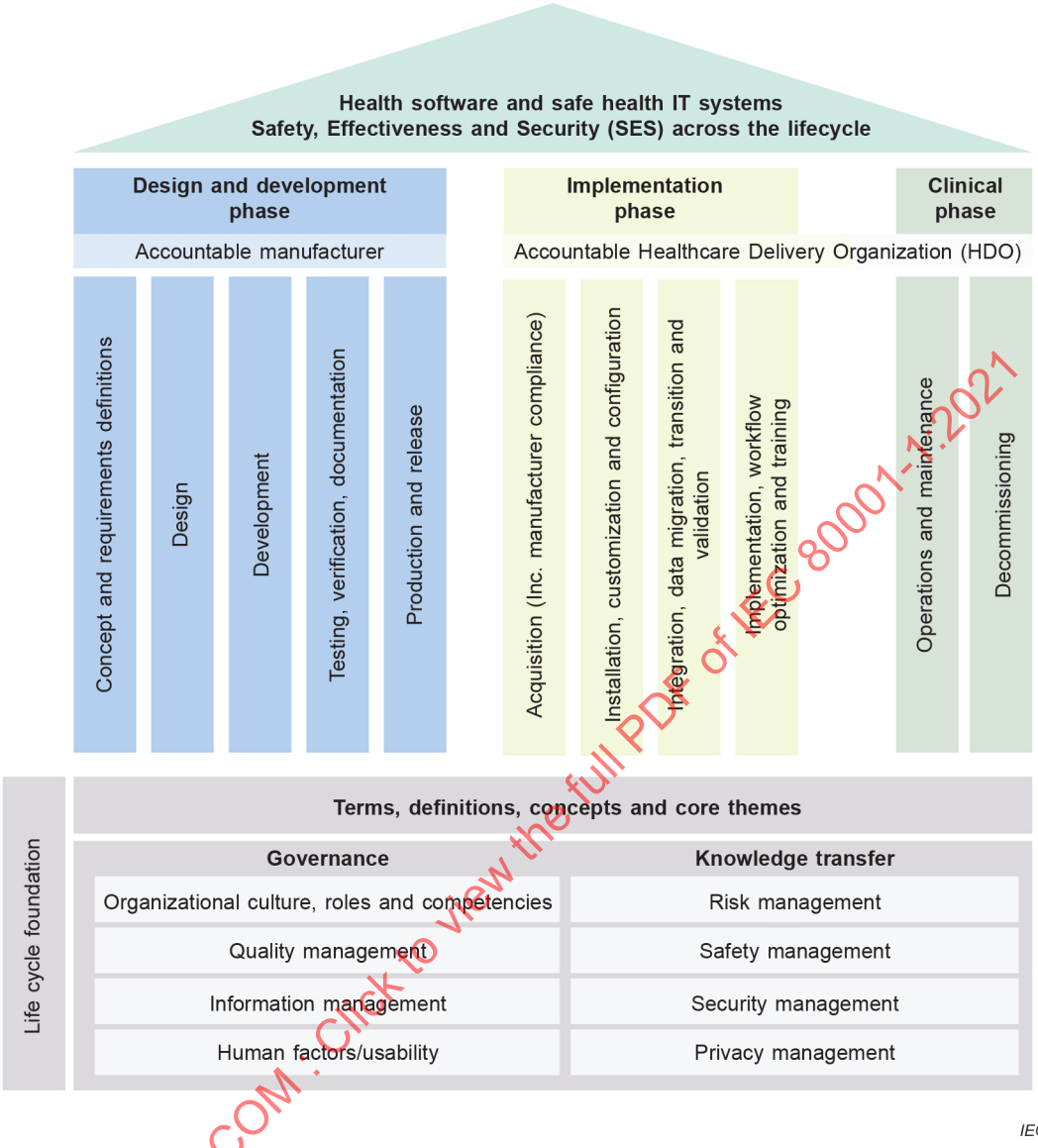


Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health software and health IT systems

This document facilitates ORGANIZATIONS in using or adapting existing work practices and processes, personnel and tools wherever practicable to address the requirements of this document. For example, if an organization has an existing RISK MANAGEMENT PROCESS, this can be used or adapted to support the three KEY PROPERTIES of SAFETY, EFFECTIVENESS, and SECURITY. Requirements are defined such that they can be evaluated and as such support an ORGANIZATION in verifying and demonstrating the degree of compliance with this document.

The RISK MANAGEMENT requirements of this document are based upon existing concepts adapted and extended for use by all stakeholders supporting implementation and clinical use of connected HEALTH SOFTWARE and HEALTH IT SYSTEMS (including medical devices). This document aligns with ISO 81001-1, ISO/IEC Guide 63, IEC Guide 120.

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

Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

1 Scope

This document specifies general requirements for ORGANIZATIONS in the application of RISK MANAGEMENT before, during and after the connection of a HEALTH IT SYSTEM within a HEALTH IT INFRASTRUCTURE, by addressing the KEY PROPERTIES of SAFETY, EFFECTIVENESS and SECURITY whilst engaging appropriate stakeholders.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

NOTE For the purpose of this document, the terms and definitions given in ISO 81001-1:20XX and the following apply.

3.1
CONSEQUENCE
outcome of an event affecting objectives

Note 1 to entry: A CONSEQUENCE can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: CONSEQUENCES can be expressed qualitatively or quantitatively.

Note 3 to entry: Any CONSEQUENCE can escalate through cascading and cumulative effects.

[SOURCE:ISO 31000:2018, 3.6]

3.2
HEALTHCARE
care activities, services, management or supplies related to the health of an individual or population

Note 1 to entry: This includes more than performing procedures for subjects of care. It includes, for example, the management of information about patients, health status and relations within the HEALTHCARE delivery framework and may also include the management of clinical knowledge.

[SOURCE: ISO 13940:2015, 3.1.1, modified – The definition was reworded to include population.]

3.3
INCIDENT
unplanned interruption to a service a reduction in the quality of a service or an event that has not yet impacted the service to the customer or user

[SOURCE: ISO/IEC 20000-1:2018, 3.2.5]

3.4
INITIAL RISK
RISK derived during risk estimation taking into consideration any retained RISK control measures

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.3, modified – The definition was reworded.]

3.5
LIKELIHOOD
chance of something happening

Note 1 to entry: In risk management terminology, the word "LIKELIHOOD" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "LIKELIHOOD" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "LIKELIHOOD" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7]

3.6
PROCESS
set of interrelated or interacting activities that use inputs to deliver an intended result

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

[SOURCE: IEC 81001-1:2021, 3.2.10]

3.7
HEALTH IT RISK MANAGER
person accountable for risk management of a HEALTH IT SYSTEM

3.8
RISK MANAGEMENT PLAN
description of how the elements and resources of the risk management PROCESS will be implemented within an organization or project

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.3529]

4 Principles

The following principles provide the basis for RISK MANAGEMENT. They communicate the value, intention and purpose of RISK MANAGEMENT and their application supports the preservation of the KEY PROPERTIES during the implementation and use of HEALTH IT SYSTEMS within a HEALTH IT INFRASTRUCTURE:

– RISK MANAGEMENT is an integral part of an ORGANIZATION'S activities at all stages of the HEALTH IT SYSTEM lifecycle;

– accountability for the RISK MANAGEMENT PROCESS remains with the HEALTHCARE DELIVERY ORGANIZATION;

– a HEALTHCARE DELIVERY ORGANIZATION may assign responsibility for RISK MANAGEMENT of the HEALTH IT SYSTEM and/or HEALTH IT INFRASTRUCTURE to a different ORGANIZATION such as providers of HEALTH IT SYSTEMS, HEALTH IT INFRASTRUCTURE or a collaboration of HEALTHCARE DELIVERY ORGANIZATIONS.

RISK MANAGEMENT creates and protects value. It contributes to the demonstrable maintenance or/and improvement of SAFETY, EFFECTIVENESS and SECURITY in the implementation and use of connected HEALTH IT SYSTEMS.

– A structured and comprehensive approach to RISK MANAGEMENT contributes to consistent and comparable clinical outcomes;
– The RISK MANAGEMENT PROCESS is scalable and can be customised and made proportionate to the ORGANIZATION'S objectives;
– Appropriate and timely involvement of stakeholders leads to improved awareness and alignment across the ORGANIZATION and enables informed RISK MANAGEMENT;
– RISKS can emerge, change or disappear as new HEALTHCARE tools and methodologies are developed. Proactive RISK MANAGEMENT anticipates, detects, acknowledges and responds to changes and events in a timely manner;
– The inputs to RISK MANAGEMENT are based on historical and current information, as well as future expectations. RISK MANAGEMENT explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders;
– The SOCIOTECHNICAL ECOSYSTEM significantly influences all aspects of RISK MANAGEMENT at each level within the HEALTHCARE DELIVERY ORGANIZATION and at each lifecycle stage; and
– RISK MANAGEMENT is a continuous activity, improved through learning and experience. RISK MANAGEMENT strengthens the ORGANIZATION resilience and supports the ORGANIZATION'S business needs and objectives.

NOTE RISK is balanced across the KEY PROPERTIES wherever practical.

5 Framework

5.1 General

The purpose of the RISK MANAGEMENT framework is to assist the ORGANIZATION in integrating the RISK MANAGEMENT with other significant activities and functions. Effective RISK MANAGEMENT depends on its integration with the governance of the ORGANIZATION, including decision-making. This requires support from all stakeholders, particularly TOP MANAGEMENT. Requirements in this document apply to HEALTHCARE DELIVERY ORGANIZATIONS and other ORGANIZATIONS seeking conformance with this RISK MANAGEMENT framework. Those requirements that apply to HEALTHCARE DELIVERY ORGANIZATIONS only are clearly identified.

5.2 Leadership and commitment

It is the responsibility of the TOP MANAGEMENT of the ORGANIZATION to ensure that RISK MANAGEMENT is implemented throughout the HEALTH IT SYSTEM lifecycle, and that its effectiveness is evaluated.

The ORGANIZATION shall establish and adhere to a defined PROCESS for RISK MANAGEMENT.

5.3 Integrating RISK MANAGEMENT

Effective integration of RISK MANAGEMENT relies on an understanding of the ORGANIZATION'S structures and context. Structures differ depending on the ORGANIZATION'S purpose, goals and complexity. The RISK is managed in every part of the ORGANIZATION'S structure. Everyone in an ORGANIZATION is responsible for managing RISK.

Integrating RISK MANAGEMENT is a dynamic and iterative PROCESS that can be customised to the ORGANIZATION'S culture and objectives. The RISK MANAGEMENT should be part of, and not separate from, organizational purpose, governance, leadership, commitment, strategy, objectives and operations.

5.4 Design/planning

5.4.1 General

The safe acquisition, installation, integration, implementation, use, maintenance and decommissioning of a HEALTH IT SYSTEM is dependent on effective RISK MANAGEMENT planning. Planning activities apply to new implementations and modifications to existing HEALTH IT SYSTEMS.

The purpose of the HEALTH IT SYSTEM RISK MANAGEMENT PLAN is to document and schedule the RISK MANAGEMENT activities throughout all lifecycle phases of the HEALTH IT SYSTEM and describe how a specific HEALTH IT SYSTEM project will adhere to the RISK MANAGEMENT PLAN. The RISK MANAGEMENT PROCESS which establishes the requirements of this document is depicted at Figure 2 and applies throughout the lifecycle of the HEALTH IT SYSTEM.

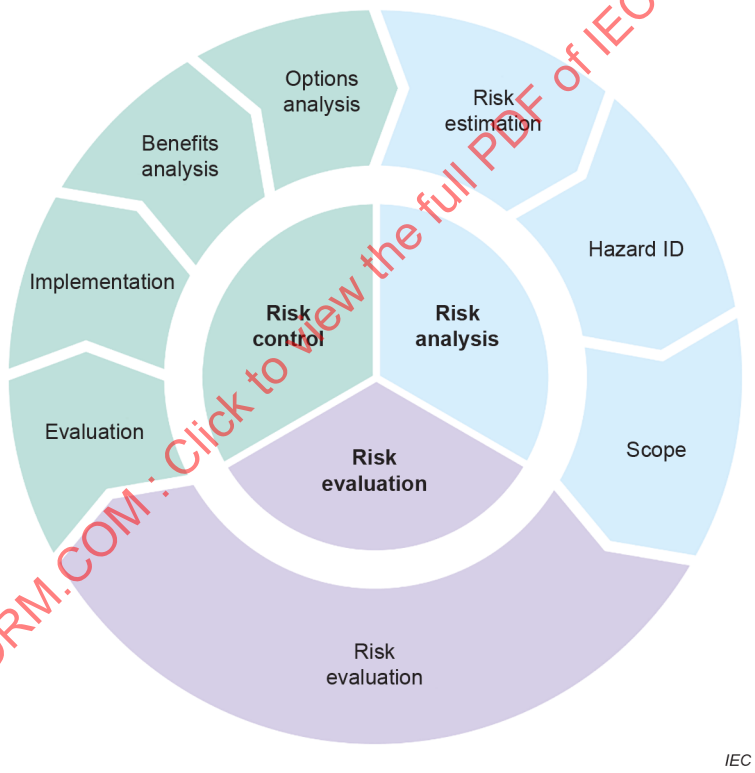


Figure 2 – RISK MANAGEMENT PROCESS

The extent of the RISK MANAGEMENT PLAN should be flexible and commensurate with the scale and scope of functionality of the HEALTH IT SYSTEM whilst addressing the RISK MANAGEMENT requirements specified within this document. The contents of the RISK MANAGEMENT PLAN should include:

– a framework for RISK ANALYSIS;
– defined risk acceptance criteria for individual risks and the overall RESIDUAL RISK;
– a list of the relevant procedures, policies and resources required; and
– a reference to any ACCOMPANYING DOCUMENTS

5.4.2 RISK MANAGEMENT FILE

The ORGANIZATION shall:

a) establish, at the start of a project, a HEALTH IT SYSTEM RISK MANAGEMENT FILE;

b) maintain the RISK MANAGEMENT FILE throughout the lifecycle of the HEALTH IT SYSTEM; and

c) ensure that the RISK MANAGEMENT FILE is recoverable in the event of failure.

The HEALTH IT SYSTEM RISK MANAGEMENT FILE provides a store of all records which relate to the RISK MANAGEMENT PROCESS and any decisions that influence RISK MANAGEMENT.

5.4.3 Understanding the organization and the SOCIOTECHNICAL ECOSYSTEM

Before starting the design and implementation of the RISK MANAGEMENT PLAN it is important to evaluate and understand the internal and external SOCIOTECHNICAL ECOSYSTEM as this will significantly influence the design of the PROCESS.

The ORGANIZATION shall establish and maintain a defined list of ASSETS that interface with or constitute part of a HEALTH IT SYSTEM.

Factors which can affect the external SOCIOTECHNICAL ECOSYSTEM include but are not limited to: key drivers and trends which affect the ORGANIZATION'S objectives; contractual relationships and commitments; the complexity of networks and dependencies and any local regulatory conditions.

Factors which can affect the internal SOCIOTECHNICAL ECOSYSTEM include but are not limited to: the vision, mission and values of the ORGANIZATION; the governance, structure and accountabilities of the ORGANIZATION; and standards adopted by the ORGANIZATION and the ORGANIZATION'S capability and assets.

5.4.4 Articulating RISK MANAGEMENT commitment

It is the responsibility of the ORGANIZATION'S TOP MANAGEMENT to demonstrate and articulate their continual commitment to RISK MANAGEMENT by establishing and applying a RISK MANAGEMENT PLAN and appraising the EFFECTIVENESS of RISK MANAGEMENT activities.

The ORGANIZATION'S TOP MANAGEMENT shall:

a) be accountable for ensuring that the ORGANIZATION adheres to the HEALTH IT SYSTEM RISK MANAGEMENT PLAN;

b) be accountable for ensuring that the ORGANIZATION achieves compliance with this document; and

c) authorise the sale or deployment of the HEALTH IT SYSTEM.

5.4.5 Assigning organizational roles, authorities, responsibilities and accountabilities

It is the responsibility of the ORGANIZATION'S TOP MANAGEMENT to ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to RISK MANAGEMENT are assigned and communicated at all levels of the organization. This will include identifying accountable individuals who have the authority to manage RISK and the appointment of a HEALTH IT RISK MANAGER who holds responsibility for the implementation of the RISK MANAGEMENT PROCESS.

The ORGANIZATION'S TOP MANAGEMENT shall:

a) identify a HEALTH IT RISK MANAGER who has the necessary qualifications, knowledge and competence for the application of RISK MANAGEMENT to HEALTH IT SYSTEMS;

NOTE 1 As a minimum, the list of approvers will include the HEALTH IT RISK MANAGER.

b) ensure that the roles and responsibilities of the personnel engaged in RISK MANAGEMENT activities, including the roles who can review and approve the RISK MANAGEMENT artefacts, are defined and recorded;

c) ensure that all personnel performing the roles are aware of their responsibilities with respect to following the ORGANIZATIONS RISK MANAGEMENT PROCESS.

The HEALTH IT RISK MANAGER shall:

d) be responsible for ensuring that the RISK MANAGEMENT PROCESS is followed;

e) be responsible for reporting on the RISK MANAGEMENT PROCESS to the TOP MANAGEMENT.

The responsibilities of the HEALTH IT RISK MANAGER apply to new HEALTH IT SYSTEM implementations and modifications to existing HEALTH IT SYSTEMS.

The ORGANIZATION shall:

f) incorporate the results of the RISK MANAGEMENT activities undertaken through these requirements in the assurance case and record them in the RISK MANAGEMENT FILE.

NOTE 2 The concept of an assurance case is described in ISO 81001-1.

5.4.6 Allocating resources

The level of resources required to support RISK MANAGEMENT will need to be commensurate with the scale, complexity and RISK profile of the HEALTH IT SYSTEM and is also dependent on the HEALTH IT SYSTEM deployment timescales. The assessment of the required resources may be guided by experience gained from previous deployments.

Appropriate resources for RISK MANAGEMENT can include, but are not limited to: people with the appropriate skills, experience and competence, the organization's RISK MANAGEMENT PROCESSES, methods and tools and information and knowledge management systems.

THE ORGANIZATION'S TOP MANAGEMENT shall:

a) provide sufficient resources to support RISK MANAGEMENT;

b) ensure that personnel engaged in RISK MANAGEMENT are suitably qualified and experienced.

The organization should consider the capabilities of, and constraints on, existing resources and ensure that the nominated resources have sufficient time available to allow them to apply a suitable level of effort to ensure the RISK MANAGEMENT PROCESS is completed in a robust and competent manner.

5.4.7 Establishing communication and consultation

Communication involves sharing information with targeted audiences and consultation involves participants providing information with the understanding that it will contribute to and shape decisions or other activities. Communication and consultation methods and content shall reflect the expectations of all stakeholders.

Communication and consultation shall be timely and ensure that relevant information is collected, collated, synthesised and shared as appropriate. Where the responsibility for RISK MANAGEMENT is shared the details will be recorded in a RESPONSIBILITY AGREEMENT.

The ORGANIZATION shall:

a) establish effective means of sharing information with internal and external RISK MANAGEMENT stakeholders;

b) establish effective means of gathering information from internal and external RISK MANAGEMENT stakeholders; and

c) retain communications that have an impact on RISK MANAGEMENT outcomes.

Internal and external RISK MANAGEMENT stakeholders could include: OPERATORS, HEALTH IT SYSTEM MANUFACTURERS, technical support function, internal IT function and other facilities management functions.

5.5 Implementation

Successful implementation of the RISK MANAGEMENT PROCESS requires the engagement and awareness of stakeholders. This enables ORGANIZATIONS to explicitly address uncertainty in decision making, whilst also ensuring that any new or subsequent uncertainty is considered as soon as it arises.

Successful implementation of the RISK MANAGEMENT PROCESS will be achieved through adherence to the RISK MANAGEMENT PLAN. The RISK MANAGEMENT PLAN should clearly define the associated timescales, milestones and resource requirements.

5.6 Evaluation

Compliance to the RISK MANAGEMENT PLAN and effectiveness of the risk management PROCESS should be periodically evaluated. The evaluations may be conducted annually or more frequently as circumstances change.

The ORGANIZATION shall:

a) evaluate the EFFECTIVENESS of the RISK MANAGEMENT PROCESS at defined intervals; and

b) record evidence of the evaluation in the RISK MANAGEMENT FILE.

Evaluation of the EFFECTIVENESS of the RISK MANAGEMENT PROCESS should include a review of concerns and incidents relating to the HEALTH IT SYSTEM and assess their impact on the KEY PROPERTIES, monitor the timeliness of INCIDENT reporting; and review EVENT MANAGEMENT.

5.7 Improvement

The ORGANIZATION should strive to continually improve the suitability, adequacy and EFFECTIVENESS of the RISK MANAGEMENT PROCESS and the way that the RISK MANAGEMENT PROCESS is implemented. As gaps or improvement opportunities are identified, the ORGANIZATION can develop plans and tasks and assign them to those accountable for implementation. Once implemented these improvements can contribute to the enhancement of RISK MANAGEMENT.

The ORGANIZATION shall:

a) continually monitor and adapt the RISK MANAGEMENT PROCESS to address external and internal changes; and

b) record evidence of any improvements in the RISK MANAGEMENT FILE.

By continually monitoring and adapting its RISK MANAGEMENT PROCESS the ORGANIZATION can optimise the effectivity and efficiency of the PROCESS.

6 RISK MANAGEMENT PROCESS

6.1 Generic requirements

6.1.1 General

The generic RISK MANAGEMENT PROCESS is depicted in Figure 2. Three key activities, which are supported by related sub-activities, are conducted in a continual cycle through-out the lifecycle

of a HEALTH IT SYSTEM from initial acquisition through to decommission. Requirements in this document apply to HEALTHCARE DELIVERY ORGANIZATIONS and other ORGANIZATIONS seeking conformance with this RISK MANAGEMENT framework. Those requirements that apply to HEALTHCARE DELIVERY ORGANIZATIONS only are clearly identified.

The ORGANIZATION shall:

a) at the start of the project establish a RISK MANAGEMENT PLAN detailing the RISK ANALYSIS, RISK EVALUATION and RISK CONTROL activities to be undertaken;

b) maintain the clinical RISK MANAGEMENT PLAN in the RISK MANAGEMENT FILE throughout the lifecycle of the HEALTH IT SYSTEM;

c) record the justification for any deviations from the RISK MANAGEMENT PLAN within the RISK MANAGEMENT FILE;

d) at the start of the project establish an ASSURANCE CASE for the project;

e) incorporate the results of the RISK MANAGEMENT activities undertaken through these requirements in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.1.2 RISK ANALYSIS

6.1.2.1 General

RISK ANALYSIS involves establishing the scope of the HEALTH IT SYSTEM both in terms of its technological architecture, functionality and its INTENDED USE. Once this is understood, analysis is conducted to identify any HAZARDS that could occur. The RISK associated with identified HAZARDS is then estimated. This is best achieved through a multi-disciplinary workshop typically involving competent representatives from the following specialist areas

– TOP MANAGEMENT;
– HEALTHCARE professionals;
– business owners;
– SYSTEM INTEGRATORS;
– IMPLEMENTERS;
– ADMINISTRATORS;
– USERS; and
– SECURITY practitioners

The scale, complexity and level of RISK will vary across different HEALTH IT SYSTEM deployments. It is important to recognise this and ensure the level of resources required to support the PROCESS is commensurate.

6.1.2.2 Defining the purpose and scope of the PROCESS

Prior to commencing RISK ANALYSIS activities for any HEALTH IT SYSTEM deployment or modification it is essential to define the scope of the RISK ANALYSIS. Defining the scope correctly will bound the extent of the RISK ANALYSIS as well as ensuring that all areas impacted by the deployment are considered. It is important to understand how the HEALTH SOFTWARE or MEDICAL DEVICE will integrate with the existing HEALTH IT INFRASTRUCTURE. Consideration should also be given to any data migration required to support the deployment.

The ORGANIZATION shall:

a) define the HEALTHCARE setting in which the HEALTH IT SYSTEM will be deployed and used;

b) define the INTENDED USE of the HEALTH IT SYSTEM in the context of supporting HEALTHCARE;

c) identify the USERS of the HEALTH IT SYSTEM;

d) define the scale and complexity of the deployment HEALTH IT SYSTEM including the integration of components within the HEALTH IT SYSTEM;

e) identify and consider any inter/intra HEALTH IT SYSTEM functional and data dependencies.

Additionally, a HEALTHCARE DELIVERY ORGANIZATION shall:

f) define the scale and complexity of the HEALTH IT SYSTEM deployment including the integration of the HEALTH IT SYSTEM within the HEALTH IT INFRASTRUCTURE; and

g) gather suitable and sufficient information via ACCOMPANYING DOCUMENTS from each MEDICAL DEVICE MANUFACTURER or HEALTH IT SYSTEM MANUFACTURER to support RISK MANAGEMENT.

For recommendations of suitable and sufficient information via ACCOMPANYING DOCUMENTS, see "Guidance for accompanying document information" in Annex B. Additional details on system security are detailed in IEC TR 80001-2-2:2012 and IEC TR 80001-2-8:2016 and reflected in the manufacturer disclosure statement for medical device security. The responsibility agreement in ISO/TR 80001-2-6:2014 provides information on the formation of contractual or RFP arrangements between the HEALTHCARE DELIVERY ORGANIZATION and the HEALTH IT SYSTEM provider.

The ORGANIZATION shall:

h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.1.2.3 HAZARD identification

The purpose of HAZARD identification is to uncover and describe events or conditions that have the potential to result in HARM when the HEALTH IT SYSTEM is deployed or used.

It is recommended that a HAZARD workshop is run to support complete HAZARD identification involving stakeholders suggested in 6.1.2.1. HAZARD identification activities should be undertaken using a recognised technique such as Structured What If Technique (SWIFT) and consider:

- the HEALTHCARE delivery processes that will be impacted by the HEALTH IT SYSTEM, including workflow and human factors considerations;
- the intended use of the HEALTH IT SYSTEM within the HEALTHCARE DELIVERY ORGANIZATION(S);
- the interdependencies associated with the health it system, including data-flows;

The ORGANIZATION shall:

a) identify and document known, and foreseeable HAZARDS associated with deployment of the HEALTH IT SYSTEM and its use under both normal and foreseeable operating conditions;

b) review HAZARDS identified in the ACCOMPANYING DOCUMENTS provided by the HEALTH SOFTWARE or MEDICAL DEVICE MANUFACTURER or provided by suppliers of other key system components for applicability in the context of deployment, use or decommissioning of the HEALTH IT SYSTEM; and

c) where no HAZARDS are identified, record the justification for this conclusion within the RISK MANAGEMENT FILE.

Additionally, the HEALTHCARE DELIVERY ORGANIZATION shall:

d) consider HAZARDS associated with the integration of the HEALTH IT SYSTEM into the HEALTH IT INFRASTRUCTURE.

It will be necessary to identify and record any vulnerabilities and/or threats to the HEALTH IT SYSTEM and/or its integration into the HEALTH IT INFRASTRUCTURE

The ORGANIZATION shall:

e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.1.2.4 RISK ESTIMATION

RISK ESTIMATION is the PROCESS of categorising the RISK of the identified HAZARD by determining the HAZARD causes and CONSEQUENCES and considering the LIKELIHOOD of HARM occurring as a result of the HAZARD and the SEVERITY of that HARM.

Using the criteria specified in the RISK MANAGEMENT PLAN, for each identified HAZARD the ORGANIZATION shall:

a) estimate the SEVERITY of the CONSEQUENCE of the HARM;

b) estimate the LIKELIHOOD of HARM;

c) estimate and record the resulting RISK.

RISK criteria can vary across different ORGANIZATIONS so the HEALTHCARE DELIVERY ORGANIZATION shall:

d) reconcile the criteria used by the HEALTH SOFTWARE or MEDICAL DEVICE MANUFACTURER with the criteria used by the HEALTHCARE DELIVERY ORGANIZATION (e.g. risk classification scheme).

The ORGANIZATION shall:

e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

This PROCESS considers the most realistic and typical scenario that could result in HARM. It is possible that a HAZARD CONSEQUENCE can have more than one SEVERITY rating. For example, the CONSEQUENCE of a patient being inadvertently prescribed an overdose of one particular drug could be more severe and immediate, giving little or no time for intervention, than the overdose of a different drug which could simply induce inconvenience after an elapsed period of time. The LIKELIHOOD of the former occurring can be significantly lower than the latter if it is used to treat a very rare condition. The RISK ASSESSMENT shall consider all the HAZARD scenarios and determine the associated SEVERITY and LIKELIHOOD ratings. Where the HAZARD cause is common in the different scenarios then the highest RISK rating can be used, noting that a single HAZARD can have multiple causes.

The assessment of SEVERITY is made on a qualitative scale which considers the HARM that could credibly occur. Each SEVERITY category will have an associated meaning assigned which enables a distinction to be made between the categories.

HEALTH IT SYSTEMS are vulnerable to systematic faults which means that, unlike random faults, the LIKELIHOOD of their occurrence is not amenable to quantification. Therefore, LIKELIHOOD is subject to judgement on a qualitative scale. Each LIKELIHOOD category will have an associated meaning assigned which enables a distinction to be made between the categories.

6.1.3 RISK EVALUATION

RISK EVALUATION is the PROCESS of evaluating whether, using the criteria defined in the RISK MANAGEMENT PLAN, the RISK of a HAZARD is acceptable or whether further action is necessary. INITIAL RISK is the RISK that exists before any additional control measures are introduced. Generally, the RISK is evaluated using a matrix that combines both SEVERITY and LIKELIHOOD and will yield a range in which RISK is considered “acceptable”. If the RISK falls outside of the “acceptable” range, it may still be “accepted” by an ORGANIZATION in circumstances where the benefits of proceeding with the deployment outweigh the RISK of doing so. Such decisions will be supported by Benefits-RISK analysis (6.1.4.2).

Using the criteria specified in the RISK MANAGEMENT PLAN, the ORGANIZATION shall for each HAZARD:

a) evaluate the acceptability of the INITIAL RISK;

b) where the INITIAL RISK is considered to be unacceptable, all requirements within 6.1.4 shall be addressed; and

c) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.1.4 RISK CONTROL

6.1.4.1 RISK CONTROL analysis

RISK CONTROL measures can reduce the LIKELIHOOD of the HAZARD occurring or lessen the SEVERITY of the HAZARD'S CONSEQUENCES.

For each HAZARD, the ORGANIZATION shall:

a) identify RISK CONTROL measures;

b) assess RISK CONTROL measures to determine whether new HAZARDS will be introduced as a result of their implementation or whether the RISKS for previously identified HAZARDS will be affected;

c) manage any new HAZARDS or increased RISKS in accordance with the requirements of this document;

d) evaluate the RESIDUAL RISK using the RISK acceptability criteria defined in the RISK MANAGEMENT PLAN;

e) where the RESIDUAL RISK is unacceptable, identify additional RISK CONTROL measures in order to reduce the RISK;

f) where a RISK CONTROL measure is to be implemented by another ORGANIZATION, clearly record this dependency in the ASSURANCE CASE;

g) where no suitable RISK CONTROL measures are possible, conduct a benefit-RISK analysis (see 6.1.4.2) of the RISK; and

h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE;

RISK CONTROL measures have different strengths of effectiveness. The order of effectiveness is:

– design changes (e.g. removal of hazards), or the inclusion of protective measures in the HEALTH IT SYSTEM;

– administrative and implementation procedures; and

– USER and other stakeholder training and briefing.

The introduction of RISK CONTROL measures may result in trade-offs having to be made between the KEY PROPERTIES of SAFETY, EFFECTIVENESS, and SECURITY. Wherever practical, a balanced view should be taken and RISK CONTROL measures selected that introduce optimum risk reduction across the three KEY PROPERTIES. This is especially important in HEALTHCARE DELIVERY ORGANIZATIONS where the introduction of the HEALTH IT SYSTEM into the existing HEALTH IT INFRASTRUCTURE shall be considered and balanced in the wider context of holistic HEALTHCARE delivery.

There is an important distinction to be made between RESIDUAL RISKS that are so low that there is no need to manage them further beyond verification of the effectiveness of the RISK CONTROL measures and RESIDUAL RISKS that are greater but accepted because of the associated benefits introduced and the impracticability of reducing the RISKS further. If, during RISK CONTROL

analysis, the ORGANIZATION determines that the necessary RISK reduction is not practicable, the ORGANIZATION shall conduct and document a benefit-RISK analysis of the RESIDUAL RISK (6.1.4.2).

6.1.4.2 Benefit-RISK analysis

A decision shall be made as to whether the RESIDUAL RISK associated with a HAZARD (and the overall RESIDUAL RISK) is outweighed by the benefit that the HEALTH IT SYSTEM provides. The decision is generally made by the judgement of experienced and knowledgeable individuals, including the HEALTH IT RISK MANAGER. Those involved in making benefit-RISK judgements have a responsibility to understand and consider the technical, clinical, regulatory, economic, sociological and political context of their RISK MANAGEMENT decisions. The analysis shall also consider the aggregated benefit-RISK i.e. the summation of all unaccepted risks versus the net clinical benefit of deployment. If the analysis does not support the conclusion that the benefits outweigh the RESIDUAL RISK, then the RISK remains unacceptable.

Proceeding with a deployment where RISK is unacceptable requires explicit approval by TOP MANAGEMENT in accordance with any existing governance PROCESSES.

For each HAZARD where the RESIDUAL RISK remains unacceptable the following consideration of all practical controls the ORGANIZATION shall:

a) demonstrate that no further practicable measures can be applied to reduce the RESIDUAL RISK to an acceptable level;

b) where a decision has been made to accept the RESIDUAL RISK, record the rationale and context of the judgement in the ASSURANCE CASE.

The HEALTHCARE DELIVERY ORGANIZATION shall also:

c) consider the aggregated RESIDUAL RISK of all HAZARDs in relation to the clinical benefits that could be realized; and

d) where the RESIDUAL RISK cannot be accepted, record the justification for any decision made by TOP MANAGEMENT to deploy in the ASSURANCE CASE.

The ORGANIZATION shall:

e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subcause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.1.4.3 VERIFICATION of RISK CONTROL measures

The VERIFICATION of risk control measures establishes confidence that implementation of the control measure is effective in reducing RISK to acceptable levels. The ORGANIZATION shall:

a) implement the RISK CONTROL measures identified in accordance with 6.1.4.1;

b) verify the EFFECTIVENESS of each RISK CONTROL measure; and

c) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

The VERIFICATION of the EFFECTIVENESS of implemented RISK CONTROL measures is conducted prior to the HEALTH IT SYSTEM being implemented or before a decision is made to deploy. The means and responsibility by which the VERIFICATION is carried out will depend on the nature of the RISK CONTROL measure. For example, a RISK CONTROL measure for network link failure could be the provision of a redundant link. The VERIFICATION of EFFECTIVENESS would involve simulating a primary link failure and verifying that the redundant link was effective. In some cases, EFFECTIVNESS cannot be verified objectively, for example, in the case of additional training and changes to business PROCESSES and procedures.

NOTE It is possible to verify the EFFECTIVENESS of RISK CONTROL measures in a test environment prior to implementation in the operational system.

6.1.4.4 RESIDUAL RISK EVALUATION and reporting

Prior to deploying a new or modified HEALTH IT SYSTEM, the ORGANIZATION shall:

a) review the acceptability of both the individual RESIDUAL RISK of each HAZARD and the overall RESIDUAL RISK; and

b) where the RESIDUAL RISK exceeds acceptability thresholds, demonstrate that a benefit-RISK analysis has been conducted in support of any decision to deploy the HEALTH IT SYSTEM.

In addition, the HEALTHCARE DELIVERY ORGANIZATION shall

c) review the health IT system manufacturer's assurance case or equivalent documentation to ensure that the RESIDUAL RISK from all recorded HAZARDS has been considered in the context of the deployment and intended use and that the acceptability of individual RESIDUAL RISKS and the overall RESIDUAL RISK is justified.

The ORGANIZATION shall:

d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.2 Lifecycle specific requirements

6.2.1 General

The following subclauses consider each lifecycle phase as identified in Figure 1 and explicitly defines the minimum set of requirements that are in scope for that lifecycle phase. In all cases this will include a subset of requirements from 6.1 and specific requirements for the particular lifecycle phase. Wherever practical, consideration should also be given to requirements in other subclauses if the necessary information and understanding is available at the lifecycle phase.

A subclause will include all child subclauses unless stated differently.

6.2.2 Acquisition

There is a need to initiate RISK MANAGEMENT early in the lifecycle in order to identify potential HAZARDS and associated RISKS and to influence subsequent lifecycle activities.

During this lifecycle phase the HEALTHCARE DELIVERY ORGANIZATION shall:

a) comply with 6.1.1, 6.1.2.2 and 6.1.2.3;

b) communicate the scope of the HEALTH IT SYSTEM that it is planning to implement to all parties (both internal and external) involved in the acquisition PROCESS;

c) engage key stakeholders (including both clinical and IT experts) in an objective evaluation of the benefits and RISKS of implementing the HEALTH IT SYSTEM; and

d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

As discussed in 6.1.2, the scope includes the functional and technical requirements, data and system integration specifications, and a detailed description of the system's intended use within the HEALTHCARE DELIVERY ORGANIZATION's specific clinical and business context. The evaluation of benefits and risks during this lifecycle phase extends to include those that are inherent in the HEALTH IT SYSTEM and associated ASSETS and also the degree of customisation and integration into the HEALTHCARE DELIVERY ORGANIZATION's SOCIOTECHNICAL ECOSYSTEM that would be required.

6.2.3 Installation, customization and configuration

HEALTH IT SYSTEMS are usually configured to support local requirements. In such cases each HEALTHCARE DELIVERY ORGANIZATION shall:

a) review the findings of 6.2.2 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information;

b) comply with 6.1.1, 6.1.2 and 6.1.3;

c) review the ASSURANCE CASE report or the equivalent documentation and any supporting information provided by a HEALTH SOFTWARE or MEDICAL DEVICE MANUFACTURER to be satisfied that it remains applicable and valid in their own context;

d) if any deficiencies are identified, conduct additional RISK MANAGEMENT in accordance with 6.1; and

e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.2.4 Integration, data migration, transition and validation

HEALTHCARE related RISKS can occur when the HEALTH IT SYSTEM is physically integrated into the HEALTH IT INFRASTRUCTURE. To minimise RISK, the HEALTHCARE DELIVERY ORGANIZATION shall

a) review findings of 6.2.3 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information;

b) comply with 6.1.1;

c) manage integration of the HEALTH IT SYSTEM (including both technical and data integration) through a comprehensive plan that identifies all activities and stakeholders who shall be engaged; and

d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.2.5 Implementation, workflow optimization and training

Prior to deployment of the HEALTH IT SYSTEM for live use, the HEALTHCARE DELIVERY ORGANIZATION shall ensure that all RISK MANAGEMENT activities have been completed and that the RISK profile is known and understood.

The HEALTHCARE DELIVERY ORGANIZATION shall:

a) review findings of 6.2.4 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information;

b) comply with subclause of 6.1.4.4;

c) confirm that the RISK MANAGEMENT PLAN has been implemented and the outcomes recorded;

d) undertake a formal review of the HEALTH IT SYSTEM prior to its deployment to ensure that the requirements of this document have been addressed;

e) confirm that TOP MANAGEMENT understand and accept the RISK profile of the deployment. (In all circumstances TOP MANAGEMENT retain responsibility for deployment of the HEALTH IT SYSTEM); and

f) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Particular consideration shall be taken to ensure that any RISK CONTROLS transferred from another ORGANIZATION to the HEALTHCARE DELIVERY ORGANIZATION have been implemented and demonstrated to be effective. It is possible that existing workflows will need to be adjusted to accommodate the HEALTH IT SYSTEM and that OPERATORS and USERS will need to be trained.

6.2.6 Operation and maintenance

Once deployed, the ORGANIZATION shall proactively monitor and review the achieved characteristics of the KEY PROPERTIES of the HEALTH IT SYSTEM. If incidents do occur, they shall be detected and resolved in a timely manner. Maintenance that is undertaken either to support the on-going effectiveness of the RISK CONTROL measures or to introduce new functionality also falls within scope of this document.

The ORGANIZATION shall:

a) comply with subclauses 6.1.2, 6.2.4 and 6.2.5 to an extent that is propionate to the risk of the INCIDENT or scope of modification;

b) demonstrate that RISK performance is being monitored and effectively managed;

c) where necessary, make changes to existing RISK CONTROL measures to maintain an acceptable level of RISK;

d) establish an INCIDENT management PROCESS to collect and review reported concerns and incidents for the HEALTH IT SYSTEM following its deployment;

e) assess the impact of any incidents on the ongoing validity of the ASSURANCE CASE;

f) where the INCIDENT compromises the ASSURANCE CASE, take appropriate corrective actions in accordance with the RISK MANAGEMENT PLAN;

g) maintain a record of incidents including their resolution; and

h) incorporate the results of the risk management activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

An INCIDENT management PROCESS should:

– enable USERS of the HEALTH IT SYSTEM to report incidents that have or could have resulted in harm;

– provide a communication mechanism that can be used by each HEALTHCARE DELIVERY ORGANIZATION and each HEALTH IT SYSTEM MANUFACTURER;

– ensure appropriate and sufficient resources are allocated by the ORGANIZATION to manage and resolve reported incidents;

– enable each HEALTHCARE DELIVERY ORGANIZATION to respond to any alert or bulletin issued by a HEALTH IT SYSTEM MANUFACTURER;

– provide a central point of contact (helpdesk) where incidents are logged;

– incorporate a means by which a RISK ASSESSMENT can be made. In practice this will be the same criteria defined in the RISK MANAGEMENT PLAN;

– facilitate a review of the existing ASSURANCE CASE to determine whether reported incidents constitute a new HAZARD, are a realisation of an existing HAZARD or that RISK CONTROL measures have failed;

– include root cause analysis;

– permit the appropriate authorities to deploy HEALTH IT SYSTEM changes, make business PROCESS amendments and close incidents;

– establish key performance indicators to ensure effective INCIDENT management; and

– provide a means by which the USER community can be advised that a particular INCIDENT has been resolved.

A HEALTH IT SYSTEM can be modified or updated during its service. The motivation for change could be defection of fixes, introduction of new functionality or in response to a security threat. The ORGANIZATION shall also consider the methods for carrying out scheduled activities such as the application of patches, data back-up and automatic updates.

The ORGANIZATION shall

i) document and apply a CHANGE-RELEASE MANAGEMENT PROCESS that includes RISK MANAGEMENT.

Where a change is made to a HEALTH IT SYSTEM, the ORGANIZATION shall:

j) apply RISK MANAGEMENT to any changes or modifications that are introduced to the HEALTH IT SYSTEM.

Where a change is made to a HEALTH IT SYSTEM by the HEALTH DELIVERY ORGANIZATION with consent from HEALTH IT SYSTEM MANUFACTURER, the HEALTHCARE DELIVERY ORGANIZATION shall:

k) confirm that the change has been made in accordance with the instructions of the HEALTH IT SYSTEM MANUFACTURER;

It is strongly recommended that a HEALTHCARE DELIVERY ORGANIZATION does not make changes to a HEALTH IT SYSTEM without documented consent from the HEALTH IT SYSTEM MANUFACTURER . If such a change is undertaken, the HEALTHCARE DELIVERY ORGANIZATION shall:

l) notify the MANUFACTURER ORGANIZATION of the change; and

m) if the change is made to a MEDICAL DEVICE, follow all necessary regulatory steps for putting such a modified HEALTH IT SYSTEM into service (e.g. configuration aligned to the manufacturer's instructions for use may provide implied consent).

The ORGANIZATION shall:

n) incorporate the results of the risk management activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

6.2.7 Decommission

HEALTH IT SYSTEMS that are being decommissioned from use are subject to the same RISK MANAGEMENT activities as when they were first deployed. At this point in the lifecycle the focus will be on controlling the RISK of HAZARDS associated with the removal of the HEALTH IT SYSTEM from service.

The HEALTHCARE DELIVERY ORGANIZATION shall:

a) comply with requirements of 6.1.2, 6.2.4 and 6.2.5;

b) apply their RISK MANAGEMENT PROCESS to support the deployment of any succeeding HEALTH IT SYSTEM;

c) consider the impact of removal of HEALTH IT SYSTEM functionality from the HEALTHCARE DELIVERY ORGANIZATION on care provision;

d) where necessary, introduce new or amended business PROCESSES and/or training to compensate for the loss of the HEALTH IT SYSTEM or in support of an alternative HEALTH IT SYSTEM;

e) ensure that RISK MANAGEMENT considers the migration of data between the decommissioned HEALTH IT SYSTEM and the succeeding HEALTH IT SYSTEM;

f) make suitable arrangements for the retention and recovery of health information following decommissioning;

g) where no HAZARDS are identified, record the justification for this conclusion within the RISK MANAGEMENT FILE; and

h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Annex A
(informative)

IEC 80001-1 requirements mapping table

Table A.1 maps the requirements in this edition of IEC 80001-1 to the subclauses of the standard.

Table A.1 – IEC 80001-1 requirements table

Subclause	Requirement
5.2 Leadership and commitment	**The ORGANIZATION shall:** a) establish and adhere to a defined PROCESS for RISK MANAGEMENT
5.4.2 RISK MANAGEMENT FILE	**The ORGANIZATION shall:** a) establish, at the start of a project, a HEALTH IT SYSTEM RISK MANAGEMENT FILE; b) maintain the RISK MANAGEMENT FILE throughout the lifecycle of the HEALTH IT SYSTEM; and c) ensure that the RISK MANAGEMENT FILE is recoverable in the event of failure.
5.4.3 Understanding the ORGANIZATION and the SOCIOTECHNICAL ECOSYSTEM	**The ORGANIZATION shall:** a) establish and maintain a defined list of ASSETS that interface with or constitute part of a HEALTH IT SYSTEM.
5.4.4 Articulating risk management commitment	**The ORGANIZATION'S TOP MANAGEMENT shall:** a) be accountable for ensuring that the ORGANIZATION adheres to the HEALTH IT SYSTEM RISK MANAGEMENT PLAN; b) be accountable for ensuring that the organization achieves compliance with this document; and c) authorise the sale or deployment of the HEALTH IT SYSTEM.
5.4.5 Assigning organizational roles, authorities, responsibilities and accountabilities	**The ORGANIZATION'S TOP MANAGEMENT shall:** a) identify a HEALTH IT RISK MANAGER who has the necessary qualifications, knowledge and competence for the application of RISK MANAGEMENT to HEALTH IT SYSTEMS; b) ensure that the roles and responsibilities of the personnel engaged in RISK MANAGEMENT activities, including the roles who can review and approve the RISK MANAGEMENT artefacts, are defined and recorded; c) ensure that all personnel performing the roles are aware of their responsibilities with respect to following the ORGANIZATIONS RISK MANAGEMENT PROCESS; **The HEALTH IT RISK MANAGER shall:** d) be responsible for ensuring that the RISK MANAGEMENT PROCESS is followed; e) be responsible for reporting on the RISK MANAGEMENT PROCESS to the TOP MANAGEMENT. **The ORGANIZATION shall:** f) incorporate the results of the risk management activities undertaken through these requirements in the assurance case and record them in the risk management file.
5.4.6 Allocating resources	**The ORGANIZATION'S TOP MANAGEMENT shall:** a) provide sufficient resources to support RISK MANAGEMENT; b) ensure that personnel engaged in RISK MANAGEMENT are suitably qualified and experienced.

Subclause	Requirement
5.4.7 Establishing communication and consultation	**The ORGANIZATION shall:** a) establish effective means of sharing information with internal and external RISK MANAGEMENT stakeholders; b) establish effective means of gathering information from internal and external RISK MANAGEMENT stakeholders; and c) retain communications that have an impact on RISK MANAGEMENT outcomes.
5.6 Evaluation	**The ORGANIZATION shall:** a) evaluate the EFFECTIVENESS of the RISK MANAGEMENT PROCESS at defined intervals; and b) record evidence of the evaluation in the RISK MANAGEMENT FILE.
5.7 Improvement	**The ORGANIZATION shall:** a) continually monitor and adapt the RISK MANAGEMENT PROCESS to address external and internal changes; and b) record evidence of any improvements in the RISK MANAGEMENT FILE.
6.1.1 Generic requirements General	**The ORGANIZATION shall:** a) at the start of the project establish a RISK MANAGEMENT PLAN detailing the RISK ANALYSIS, RISK EVALUATION and RISK CONTROL activities to be undertaken; b) maintain the clinical RISK MANAGEMEN PLAN in the RISK MANAGEMENT FILE throughout the lifecycle of the HEALTH IT SYSTEM; c) record the justification for any deviations from the RISK MANAGEMENT PLAN within the RISK MANAGEMENT FILE; d) at the start of the project establish an ASSURANCE CASE for the project; e) incorporate the results of the RISK MANAGEMENT activities undertaken through these requirements in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.2.2 Defining the purpose and scope of the PROCESS	**The ORGANIZATION shall:** a) define the HEALTHCARE setting in which the HEALTH IT SYSTEM will be deployed and used; b) define the INTENDED USE of the HEALTH IT SYSTEM in the context of supporting HEALTHCARE; c) identify the USERS of the HEALTH IT SYSTEM; d) define the scale and complexity of the deployment HEALTH IT SYSTEM including the integration of components within the HEALTH IT SYSTEM; e) identify and consider any inter/intra HEALTH IT SYSTEM functional and data dependencies;. **The HEALTHCARE DELIVERY ORGANIZATION shall:** f) define the scale and complexity of the HEALTH IT SYSTEM deployment including the integration of the HEALTH IT SYSTEM within the HEALTH IT INFRASTRUCTURE; and g) gather suitable and sufficient information via ACCOMPANYING DOCUMENTS from each MEDICAL DEVICE MANUFACTURER or HEALTH IT SYSTEM MANUFACTURER to support RISK MANAGEMENT; **The ORGANIZATION shall:** h) incorporate the results of the risk management activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Subclause	Requirement
6.1.2.3 HAZARD identification	**The ORGANIZATION shall:** a) identify and document known, and foreseeable HAZARDS associated with deployment of the HEALTH IT SYSTEM and its use under both normal and foreseeable operating conditions; b) review HAZARDS identified in the ACCOMPANYING DOCUMENTS provided by the HEALTH SOFTWARE or MEDICAL DEVICE MANUFACTURER or provided by suppliers of other key system components for applicability in the context of deployment, use or decommissioning of the HEALTH IT SYSTEM; and c) where no HAZARDS are identified, record the justification for this conclusion within the RISK MANAGEMENT FILE. **The HEALTHCARE DELIVERY ORGANIZATION shall:** d) consider HAZARDS associated with the integration of the HEALTH IT SYSTEM into the HEALTH IT INFRASTRUCTURE. **The ORGANIZATION shall:** e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.2.4 RISK estimation	**The ORGANIZATION shall:** a) estimate the SEVERITY of the CONSEQUENCE of the HARM; b) estimate the LIKELIHOOD of HARM; c) estimate and record the resulting RISK. RISK criteria can vary across different ORGANIZATIONS so the HEALTHCARE DELIVERY ORGANIZATION shall: d) reconcile the criteria used by the ORGANIZATION that supplies a HEALTH IT SYSTEM with the criteria used by the HEALTHCARE DELIVERY ORGANIZATION; The ORGANIZATION shall: e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.3 RISK EVALUATION	**The ORGANIZATION shall:** a) evaluate the acceptability of the INITIAL RISK; b) where the INITIAL RISK is considered to be unacceptable, all requirements within 6.1.4 shall be addressed; and c) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.4.1 RISK CONTROL analysis	**The ORGANIZATION shall:** a) identify RISK CONTROL measures; b) assess RISK CONTROL measures to determine whether new HAZARDS will be introduced as a result of their implementation or whether the RISKS for previously identified HAZARDS will be affected; c) manage any new HAZARDS or increased RISKS in accordance with the requirements of this document; d) evaluate the RESIDUAL RISK using the RISK acceptability criteria defined in the RISK MANAGEMENT PLAN; e) where the RESIDUAL RISK is unacceptable, identify additional RISK CONTROL measures in order to reduce the RISK; f) where a RISK CONTROL measure is to be implemented by another ORGANIZATION, clearly record this dependency in the ASSURANCE CASE; g) where no suitable RISK CONTROL measures are possible, conduct a benefit-RISK analysis (see 6.1.4.2) of the RISK; and h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE;

Subclause	Requirement
6.1.4.2 Benefit-RISK analysis	**The ORGANIZATION shall:** a) demonstrate that no further practicable measures can be applied to reduce the RESIDUAL RISK to an acceptable level; b) where a decision has been made to accept the RESIDUAL RISK, record the rationale and context of the judgement in the ASSURANCE CASE. **The HEALTHCARE DELIVERY ORGANIZATION shall also** c) consider the aggregated RESIDUAL RISK of all hazards in relation to the clinical benefits that could be realized; and d) where the RESIDUAL RISK cannot be accepted, record the justification for any decision made by TOP MANAGEMENT to deploy in the ASSURANCE CASE. **The ORGANIZATION shall:** e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.4.3 VERIFICATION of RISK CONTROL measures	**The ORGANIZATION shall:** a) implement the RISK CONTROL measures identified in accordance with 6.1.4.1; b) verify the EFFECTIVENESS of each RISK CONTROL measure; and c) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.1.4.4 RESIDUAL RISK EVALUATION and reporting	**The ORGANIZATION shall:** a) review the acceptability of both the individual RESIDUAL RISK of each HAZARD and the overall RESIDUAL RISK; and b) where the RESIDUAL RISK exceeds acceptability thresholds, demonstrate that a benefit-RISK analysis has been conducted in support of any decision to deploy the HEALTH IT SYSTEM. **The HEALTHCARE DELIVERY ORGANIZATION shall:** c) review the HEALTH IT SYSTEM MANUFACTURER'S ASSURANCE CASE or equivalent documentation to ensure that the RESIDUAL RISK from all recorded HAZARDS has been considered in the context of the deployment and intended use and that the acceptability of individual RESIDUAL RISKS and the overall RESIDUAL RISK is justified. **The ORGANIZATION shall:** d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.2.2 Acquisition	**The HEALTHCARE DELIVERY ORGANIZATION shall:** a) comply with 6.1.1, 6.1.2.2 and 6.1.2.3; b) communicate the scope of the HEALTH IT SYSTEM that it is planning to implement to all parties (both internal and external) involved in the acquisition PROCESS; c) engage key stakeholders (including both clinical and IT experts) in an objective evaluation of the benefits and RISKS of implementing the HEALTH IT SYSTEM; and d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Subclause	Requirement
6.2.3 Installation, customization and configuration	**The HEALTHCARE DELIVERY ORGANIZATION shall:** a) review the findings of 6.2.2 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information; b) comply with 6.1.1, 6.1.2 and 6.1.3 c) review the ASSURANCE CASE report or equivalent documentation and any supporting information provided by a HEALTH IT SYSTEM MANUFACTURER to be satisfied that it remains applicable and valid in their own context; d) if any deficiencies are identified, conduct additional RISK MANAGEMENT in accordance with 6.1; and e) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.2.4 Integration, data migration, transition and validation	**The HEALTHCARE DELIVERY ORGANIZATION shall:** a) review findings of 6.2.3 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information; b) comply with 6.1.1; c) manage integration of the HEALTH IT SYSTEM (including both technical and data integration) through a comprehensive plan that identifies all activities and stakeholders who shall be engaged; and d) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.2.5 Implementation, workflow optimization and training	**The HEALTHCARE DELIVERY ORGANIZATION shall:** a) Review findings of 6.2.4 to ensure they remain valid. There may be a need to repeat those activities in the context of new or additional information; b) comply with 6.1.4.4; c) confirm that the RISK MANAGEMENT PLAN has been implemented and the outcomes recorded; d) undertake a formal review of the HEALTH IT SYSTEM prior to its deployment to ensure that the requirements of this document have been addressed; e) confirm that TOP MANAGEMENT understand and accept the RISK profile of the deployment. (In all circumstances TOP MANAGEMENT retain responsibility for deployment of the HEALTH IT SYSTEM); and f) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Subclause	Requirement
6.2.6 Operation and maintenance	**The ORGANIZATION shall:** a) comply with 6.1.2, 6.2.4 and 6.2.5 to an extent that is proportionate to the **RISK** of the INCIDENT or scope of modification; b) demonstrate that RISK performance is being monitored and effectively managed; c) where necessary, make changes to existing RISK CONTROL measures to maintain an acceptable level of RISK; d) establish an INCIDENT management PROCESS to collect and review reported concerns and incidents for the HEALTH IT SYSTEM following its deployment; e) assess the impact of any incidents on the ongoing validity of the ASSURANCE CASE; f) where the INCIDENT compromises the ASSURANCE CASE, take appropriate corrective action in accordance with the RISK MANAGEMENT PLAN; g) maintain a record of incidents including their resolution; and h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE. i) document and apply a CHANGE-RELEASE MANAGEMENT PROCESS that includes RISK MANAGEMENT. **Where a change is made to a HEALTH IT SYSTEM, the ORGANIZATION shall:** j) apply RISK MANAGEMENT to any changes or modifications that are introduced to the HEALTH IT SYSTEM. **Where a change is made to a HEALTH IT SYSTEM by the HEALTH DELIVERY ORGANIZATION with consent from HEALTH IT SYSTEM MANUFACTURER, the HEALTHCARE DELIVERY ORGANIZATION shall:** k) confirm that the change has been made in accordance with the instructions of the HEALTH IT SYSTEM MANUFACTURER. It is strongly recommended that a HEALTHCARE DELIVERY ORGANIZATION does not make changes to a HEALTH IT SYSTEM without documented consent from the HEALTH IT SYSTEM MANUFACTURER ORGANIZATION. If such a change is undertaken, the HEALTHCARE DELIVERY ORGANIZATION shall: l) notify the MANUFACTURER ORGANIZATION of the change; and m) if the change is made to a MEDICAL DEVICE, follow all necessary regulatory steps for putting such a modified HEALTH IT SYSTEM into service. The ORGANIZATION shall: n) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.
6.2.7 Decommission	**The HEALTHCARE DELIVERY ORGANIZATION shall:** a) comply with requirements of 6.1.2, 6.2.4 and 6.2.5; b) apply their RISK MANAGEMENT PROCESS to support the deployment of any succeeding HEALTH IT SYSTEM; c) consider the impact of removal of HEALTH IT SYSTEM functionality from the HEALTHCARE DELIVERY ORGANIZATION on care provision; d) where necessary, introduce new or amended business PROCESSES and/or training to compensate for the loss of the HEALTH IT SYSTEM or in support of an alternative HEALTH IT SYSTEM; e) ensure that RISK MANAGEMENT considers the migration of data between the decommissioned HEALTH IT SYSTEM and the succeeding HEALTH IT SYSTEM; f) make suitable arrangements for the retention and recovery of health information following decommissioning; g) where no HAZARDS are identified, record the justification for this conclusion within the RISK MANAGEMENT FILE; and h) incorporate the results of the RISK MANAGEMENT activities undertaken through the requirements in this subclause in the ASSURANCE CASE and record them in the RISK MANAGEMENT FILE.

Annex B
(informative)

Guidance for accompanying document Information

Annex B is provided as guidance for ORGANIZATIONS to gather system level information from their medical device manufacturers. The subclauses and content may be edited or deleted at the discretion of the ORGANIZATION or medical device manufacturers.

B.1 Foreword

Table B.1 – Organization name and location

Identification of organization that prepared this document		
Insert company logo	**Organization name**	<Enter Company/Organization>.
	Street address	<Enter Street Address>
	Suite/room/building	<Enter Suite/Room/Building>
	City, state zip	<Enter Zip Code>

This document is supplied by <the company> in order to provide the operator with information to be used for the integration of <system name> into the operator's health IT infrastructure. This document was generated based on current knowledge of IT-networks and is subject to change as conditions in this area change/advance. Since framework conditions, installations, and the operation of the network are the responsibility of the operator, *(the company)* cannot fully guarantee failure-free operation.

B.2 Information system categorization

The overall information system cybersecurity device characterization level is recorded in Table B.2.

Table B.2 – Cybersecurity device characterization level

Cybersecurity device characterization level:	

B.3 Overview

This document is intended to support hospital organizations to work with their health IT systems suppliers to risk manage the implementation and operation of networked health IT systems. It is not intended to include and address configuration and other information that should be referenced externally in instruction and configuration manuals, but provide a high level overview of the system including data flows, risk assessment associated with the networking services and functions, and provide both clinical and operational characteristics.

Provide a list of system devices as part of the solution, intended use and other system level standard and optional features.

B.4 Reference documents

It is not expected that the level of detail is sufficient to cover all aspects of the implementation and operation of the Health-IT system, so this clause should include references to more detailed and focused content for the operator. Examples include manuals, security documents (e.g. manufacturer disclosure statement for medical device security), configuration guides, IFU (instructions for use), etc.

B.5 System level description

B.5.1 Environment description

Provide a system level overview of the connection of device(s) across the networking environment including wireless networking, connectivity to a data center, the use of cloud services, etc. As applicable, provide the necessary requirements in order to incorporate the device into the health IT infrastructure including but not limited to the following:

- *the required characteristics for the health IT infrastructure incorporating the MEDICAL DEVICE (PEMS in IEC 60601-1 terminology) including achieving its intended use;*
- *the required configuration of the health IT infrastructure incorporating the MEDICAL DEVICE;*
- *the technical specifications of the network connection of the MEDICAL DEVICE including security specifications;*

- *the intended information flow between the MEDICAL DEVICE, the Health IT-System and other devices on the Health IT-System and, if relevant to the KEY PROPERTIES safety, effectiveness, and data and system security, the intended routing through the health IT infrastructure.*

B.5.2 Network ports, protocols and services

Table B.3 below lists the ports, protocols and services enabled in this health IT system.

Table B.3 – Ports, protocols and services

Ports (TCP/UDP)*	Protocols	Services	Purpose
Example: 3389	TCP/UDP	TermService	For remote management of the application for service/support
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>
* Transmission control protocol (TCP), User datagram protocol (UDP).			

B.5.3 Purpose of connection to the health IT infrastructure

Simple statement offering the purpose of the network connection. Example could be patient monitoring information sent from the bedside to a central station located on the nursing floor continuing on to sending HL7 based information to EMR's and other backend servers in the data center.

B.5.4 Networking requirements

For each leg of a data journey, show the typical networking requirements including bandwidth, latency, jitter. Also include a table or other means to show ports that shall be opened through firewalls for example.

B.5.5 Required IT-network services

In addition to required IT-network transmission characteristics, a system solution may require certain network services. Depending on the scope, scale, and complexity of a deployment, these services may include DNS, DHCP, NTP, AD, and others. Provide a table or other means of showing which devices require services as it can be expected that different devices will have different service requirements.

B.5.6 Data flows and protocols

B.5.6.1 General

Provide a diagram that portrays the Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g. routers, firewalls). Provide a key to symbols used.

B.5.6.2 Clinical information flow

Including directional flows, descriptions, information types (e.g. ePHI), protocols and flow diagrams would be useful.

B.5.6.3 Operational information flow

Including directional flows, descriptions, information types (e.g. control plane data), protocols and flow diagrams would be useful.

B.6 Security and user access

B.6.1 General

This system security plan provides an overview of the security requirements and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the [Company Address] information system.

The security safeguards implemented for the [Company Address] system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table B.4 – Information system name and title

Unique identifier	Information system name	Information system abbreviation	Software version	Software version date
	[Abstract]	[Company Address]		

B.6.2 Malware / antivirus / allow-list

Include the following statement as applicable:

- *Malware / antivirus / allow-list protection software may be installed and run under certain conditions.*
- *The operator should configure the protection software such that it does not limit the operation of the appliance. Please take resource intensive processes, such as video storage during surgery and other real-time applications, into consideration.*
- *The initial installation as well as the installation of updates or safety patches of anti-malware programs should be tested in advance within the respective environment.*
- *Please note that the operator is generally responsible for malware protection in view of risk management in accordance with the IEC 80001 series.*

B.6.3 Security exclusions

List any exclusion and the appropriate justification. (E.g. this product does not include screen-lock, because it could lead to a patient adverse effect by activating screenlock during use)

B.6.4 System access

B.6.4.1 Types of users

User privileges (authorization permission after authentication takes place) are described in Table B.5.

Table B.5 – Roles and privileges

Role	Internal or external	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity level	Authorized privileges	Functions performed
Application Admin	Internal	P	Severe	Custom administrative access	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups, export log files
System Admin	Internal	P	Severe		
Service	External	P	Limited	Custom administrative access	Install and configure software, perform backups, perform tests, export log files
Authenticated user	Internal	P	Moderate	Access PII/PHI	Process PII/PHI, functional capabilities of device
	Internal	NP	Limited	N/A	functional capabilities of device
Auditor	Internal	NP	N/A	N/A	Export audit log
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
NOTE In some devices, not all roles are necessarily available.					

B.6.4.2 Remote access and maintenance

As applicable provide a brief description including:

- *options for remotely accessing the device;*
- *the (the company) policy regarding external access to devices in the field;*
- *the (the company) policy regarding employees with access to patient data.*

B.6.4.3 Patch management

As applicable provide a brief description of patch management including:

- *the operating system manufacturer and the version;*
- *(the company) policy for patch management for this particular device;*
- *whether patches may be applied by the operator and any limitations;*
- *instructions on how to test a system in order to provide a minimum level of confidence that the device remains functional after applying patches;*
- *the cybersecurity release deployment schedule.*

B.7 RISK MANAGEMENT

Provide a table or other format to show the clinical impact (features and functions) of data flow failure at each point in the data path. Include severity of data failure with table, color coding, etc. Note that the receiving organization should determine the final risk severity for their implementation.

Bibliography

[1] ISO 31000:2018, *Risk management – Guidelines*

[2] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[3] ISO 14971:2019, *Medical devices – Application of risk management to medical devices*

[4] IEC Guide 120:2018, *Security aspects – Guidelines for their inclusion in publications*

[5] ISO 13940:2015, *Health informatics – System of concepts to support continuity of care*

[6] ISO/IEC/IEEE 15026-1:2019, *Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary*

[7] ISO/IEC/IEEE 16085:2021, *Systems and software engineering – Life cycle processes – Risk management*

[8] IEC 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*
IEC 60601-1:2005/AMD1:2012
IEC 60601-1:2005/AMD2:2020

[9] ISO/TR 80001-2-6:2014, *Application of risk management for IT-networks incorporating medical device – Part 2-6: Application guidance – Guidance for responsibility agreements*

[10] ISO/IEC 20000-1:2018, *Information technology – Service management – Part 1: Service management system requirements*

[11] IEC TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*

[12] IEC TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*

[13] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Foundational principles, concepts, and terms*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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

Elle est publiée en tant que norme double logo.

Cette deuxième édition annule et remplace la première édition parue en 2010. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) modification de la structure pour mieux s'aligner sur l'ISO 31000;
b) établissement d'exigences en faveur d'une ORGANISATION dans l'application de la GESTION DES RISQUES;
c) communication de la valeur, de l'objectif et de la finalité de la GESTION DES RISQUES à travers des principes qui favorisent la préservation des PROPRIETES CLES lors de la mise en œuvre et de l'utilisation des LOGICIELS DE SANTE et/ou SYSTEMES TI DE SANTE connectés.

Le texte de ce document est issu des documents suivants:

FDIS	Rapport de vote
62A/1434/FDIS	62A/1448/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de ce document.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Dans le présent document, les caractères d'imprimerie suivants sont employés:

- exigences et définitions: caractères romains;
- *modalités d'essais*: *caractères italiques*;
- indications de nature informative apparaissant hors des tableaux, comme les notes, les exemples et les références: petits caractères. Le texte normatif à l'intérieur des tableaux est également en petits caractères;
- LES TERMES DEFINIS A L'ARTICLE 3 DU PRESENT DOCUMENT OU COMME NOTES SONT IMPRIMES EN PETITES MAJUSCULES.

Concernant la structure du présent document, le terme:

- "article" désigne l'une des cinq sections numérotées dans la table des matières, avec toutes ses subdivisions (par exemple, l'Article 5 inclut les paragraphes 5.1, 5.2, etc.);
- "paragraphe" désigne une subdivision numérotée d'un article (par exemple, 5.1, 5.2 et 5.3 sont tous des paragraphes appartenant à l'Article 5).

Dans le présent document, les références à des articles sont précédées du mot "Article" suivi du numéro de l'article concerné. Dans la présente norme particulière, les références aux paragraphes utilisent uniquement le numéro du paragraphe concerné.

Dans le présent document, la conjonction "ou" est utilisée avec la valeur d'un "ou inclusif", ainsi un énoncé est vrai si une combinaison des conditions, quelle qu'elle soit est vraie.

Les formes verbales utilisées dans le présent document sont conformes à l'usage donné à l'Article 7 des Directives ISO/IEC, Partie 2. Pour les besoins du présent document:

- "devoir" mis au présent de l'indicatif signifie que la satisfaction à une exigence ou à un essai est impérative pour la conformité au présent document;
- "il convient/il est recommandé" signifie que la satisfaction à une exigence ou à un essai est recommandée, mais n'est pas obligatoire pour la conformité au présent document;
- "pouvoir" ("may", en anglais) mis au présent de l'indicatif est utilisé pour décrire un moyen admissible pour satisfaire à une exigence ou à un essai.

Une liste de toutes les parties de la série IEC 80001, publiées sous le titre général *Sécurité, efficacité et sûreté dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés*, peut être consultée sur le site web de l'IEC.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

Le comité a décidé que le contenu de cette norme ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "https://webstore.iec.ch" dans les données relatives à la norme recherchée. À cette date, la norme 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 ce document en utilisant une imprimante couleur.

INTRODUCTION

Les ORGANISMES RESPONSABLES reposent sur des systèmes sûrs, efficaces et solides qui représentent des facteurs déterminants pour les entreprises. Cependant, une gestion inefficace de la mise en œuvre et de l'utilisation de systèmes connectés peut compromettre la capacité à fournir des services de santé.

Les systèmes connectés qui fournissent des services de santé impliquent généralement plusieurs applications logicielles, différents dispositifs médicaux et des SYSTEMES TI DE SANTE complexes fondés sur une infrastructure partagée comprenant des réseaux câblés ou sans fil, des connexions point-à-point, des serveurs d'applications et des fonctions de stockage de données, des moteurs d'interface, des logiciels de gestion de la sécurité et des performances, etc. Ces INFRASTRUCTURES TI DE SANTE sont souvent utilisées à la fois pour des fonctions organisationnelles cliniques (par exemple, des systèmes de surveillance des patients) et non cliniques (par exemple, comptabilité, planification, réseautage social, multimédia, partage de fichiers). Ces systèmes connectés peuvent comprendre de petits réseaux départementaux, de grandes infrastructures intégrées couvrant plusieurs sites, ainsi que des services en nuage exploités par des tiers. Les exigences du présent document s'adressent à plusieurs intervenants impliqués dans l'application de la GESTION DES RISQUES aux systèmes qui incluent des SYSTEMES TI DE SANTE et/ou des INFRASTRUCTURES TI DE SANTE.

Dans le contexte de l'ISO 81001-1, le présent document couvre la phase générique du cycle de vie "mise en œuvre et utilisation clinique" (voir le schéma du cycle de vie à la Figure 1).

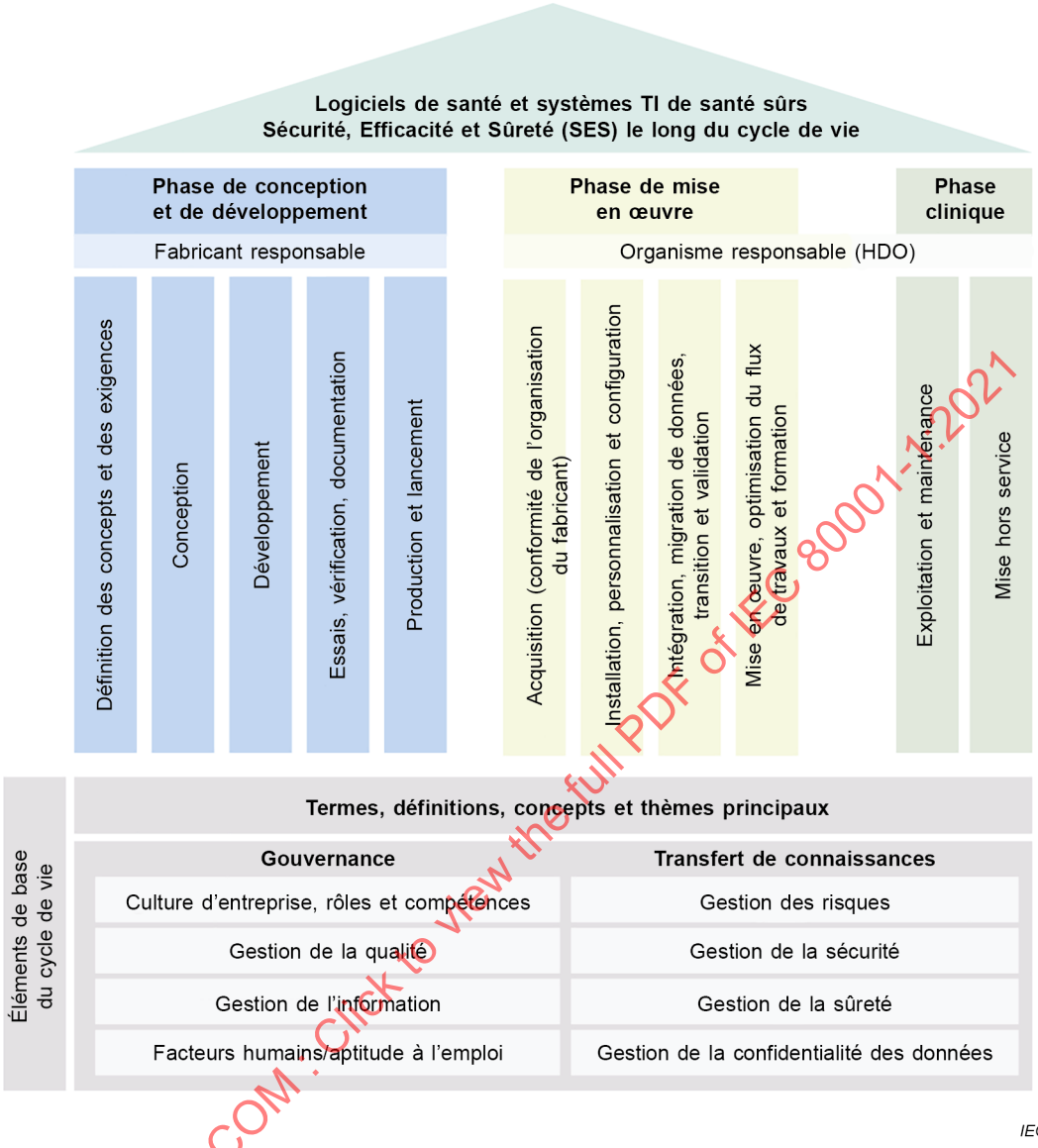


Figure 1 – Cadre de cycle de vie traitant de la sécurité, de l'efficacité et de la sûreté des logiciels de santé et des systèmes TI de santé

Le présent document aide les ORGANISATIONS dans l'utilisation ou l'adaptation, dans la mesure du possible, des pratiques et processus de travail, du personnel et des outils existants pour satisfaire aux exigences de ce document. Par exemple, si une organisation dispose déjà d'un PROCESSUS DE GESTION DES RISQUES, celui-ci peut être utilisé ou adapté de manière à prendre en charge les trois PROPRIETES CLES: SECURITE, EFFICACITE et SURETE. Les exigences sont définies de manière à pouvoir être évaluées et, donc, à appuyer l'ORGANISATION dans la vérification et la démonstration du degré de conformité au présent document.

Les exigences de GESTION DES RISQUES du présent document reposent sur les concepts existants, adaptés et étendus pour l'utilisation par tous les intervenants qui prennent en charge la mise en œuvre et l'utilisation clinique des LOGICIELS DE SANTE et des SYSTEMES TI DE SANTE connectés (y compris les dispositifs médicaux). Le présent document est conforme à l'ISO 81001-1, au Guide ISO/IEC 63 et au Guide IEC 120.

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

Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés

1 Domaine d'application

Le présent document spécifie des exigences générales au profit des ORGANISATIONS pour l'application de la GESTION DES RISQUES avant, pendant et après la connexion d'un SYSTEME TI DE SANTE au sein d'une INFRASTRUCTURE TI DE SANTE. Il traite des PROPRIETES CLES de SECURITE, d'EFFICACITE et de SURETE tout en impliquant les intervenants concernés.

2 Références normatives

Il n'y a pas référence normative.

3 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse https://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

NOTE Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 81001-1:20XX et les suivants s'appliquent.

3.1
CONSEQUENCE
effet d'un évènement affectant les objectifs

Note 1 à l'article: Une CONSEQUENCE peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects, sur l'atteinte des objectifs.

Note 2 à l'article: Les CONSEQUENCES peuvent être exprimées de façon qualitative ou quantitative.

Note 3 à l'article: Toute CONSEQUENCE peut déclencher des effets en cascade ou cumulatifs.

[SOURCE: ISO 31000:2018, 3.6]

3.2
SOINS DE SANTE
activités, prestations, gestion ou fournitures relatives à la santé d'un individu ou d'une population

Note 1 à l'article: Les soins de santé ne se limitent pas à l'exécution de procédures pour des sujets de soins. Ils comprennent, par exemple, la gestion des informations concernant les patients, l'état de santé et les relations dans le cadre des SOINS DE SANTE, et peuvent également inclure la gestion des connaissances cliniques.

[SOURCE: ISO 13940:2015, 3.1.1, modifiée – La définition a été reformulée pour inclure "ou d'une population".]

3.3
INCIDENT
interruption non planifiée d'un service, altération de la qualité d'un service ou évènement qui n'a pas encore eu d'impact sur le service au client ou à l'utilisateur

[SOURCE: ISO/IEC 20000-1:2018, 3.2.5]

3.4
RISQUE INITIAL
RISQUE dérivé pendant l'estimation des risques en prenant en considération toutes les mesures de MAITRISE DU RISQUE

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.3.3, modifiée – La définition a été reformulée.]

3.5
VRAISEMBLANCE
possibilité que quelque chose se produise

Note 1 à l'article: Dans la terminologie du management du risque, le mot «VRAISEMBLANCE» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article: Le terme anglais «LIKELIHOOD» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «VRAISEMBLANCE» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

[SOURCE: ISO 31000:2018, 3.7]

3.6
PROCESSUS
ensemble d'activités corrélées ou interactives liées qui transforme des éléments d'entrée en éléments de sortie attendus

Note 1 à l'article: Le terme "activités" couvre l'utilisation des ressources.

[SOURCE: IEC 81001-1:2021, 3.2.10]

3.7
GESTIONNAIRE DES RISQUES TI DE SANTE
personne responsable de la gestion des risques d'un SYSTEME TI DE SANTE

3.8
PLAN DE GESTION DES RISQUES
description de la manière dont les éléments et ressources du PROCESSUS de gestion des risques sont mis en œuvre au sein d'une organisation ou d'un projet

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.3529]

4 Principes

Les principes suivants constituent la base de la GESTION DES RISQUES. Ils communiquent la valeur, l'objectif et la finalité de la GESTION DES RISQUES et leur application contribue à la préservation des PROPRIETES CLES lors de la mise en œuvre et de l'utilisation des SYSTEMES TI DE SANTE au sein d'une INFRASTRUCTURE TI DE SANTE:

– la GESTION DES RISQUES fait partie intégrante des activités d'une ORGANISATION à toutes les étapes du cycle de vie du SYSTEME TI DE SANTE;

– la responsabilité du PROCESSUS DE GESTION DES RISQUES incombe à l'ORGANISME RESPONSABLE;

– un ORGANISME RESPONSABLE peut attribuer la responsabilité de la GESTION DES RISQUES du SYSTEME TI DE SANTE et/ou de l'INFRASTRUCTURE TI DE SANTE à une autre ORGANISATION (par exemple, un fournisseur de SYSTEMES TI DE SANTE, un fournisseur d'INFRASTRUCTURE TI DE SANTE ou un consortium d'ORGANISMES RESPONSABLES.

La GESTION DES RISQUES crée de la valeur et en assure la protection. Elle contribue à la sauvegarde et/ou à l'amélioration vérifiables de la SECURITE, de l'EFFICACITE et de la SURETE dans la mise en œuvre et l'utilisation des SYSTEMES TI DE SANTE connectés;

– Une approche structurée et globale de la GESTION DES RISQUES permet d'obtenir des résultats cliniques cohérents et comparables;

– Le PROCESSUS DE GESTION DES RISQUES est évolutif et peut être personnalisé et adapté aux objectifs de l'ORGANISATION;

– L'implication appropriée et opportune des intervenants conduit à une meilleure sensibilisation et à un meilleur alignement à travers l'ORGANISATION et permet une GESTION DES RISQUES en connaissance de cause;

– Les RISQUES peuvent survenir, se transformer ou disparaître à mesure que de nouveaux outils et méthodologies de SOINS DE SANTE sont développés. La gestion proactive des risques anticipe, détecte, reconnaît et répond aux changements et aux évènements en temps utile;

– Les données d'entrée dans la GESTION DES RISQUES sont fondées sur des informations historiques et actuelles, ainsi que sur les attentes futures. La GESTION DES RISQUES prend expressément en considération les limites et incertitudes éventuelles associées à ces informations et attentes. Il convient que les informations soient opportunes, claires et disponibles pour les intervenants concernés;

– L'ECOSYSTEME SOCIOTECHNIQUE influence de manière significative tous les aspects de la GESTION DES RISQUES à chaque niveau au sein l'ORGANISME RESPONSABLE et à chaque étape du cycle de vie; et

– La GESTION DES RISQUES est une activité continue, améliorée par l'apprentissage et l'expérience. Elle renforce la résilience de l'ORGANISATION et soutient cette dernière dans ses besoins et objectifs d'affaires.

NOTE Dans la mesure du possible, le RISQUE est réparti de façon équilibrée entre les PROPRIETES CLES.

5 Cadre

5.1 Généralités

Le cadre de GESTION DES RISQUES a pour objet d'aider l'ORGANISATION à intégrer la gestion des risques à d'autres activités et fonctions importantes. Une GESTION DES RISQUES efficace dépend de son intégration à la gouvernance de l'ORGANISATION, y compris à la prise de décision. Elle exige le soutien de tous les intervenants, en particulier de la DIRECTION. Les exigences du présent document s'appliquent aux ORGANISMES RESPONSABLES et à d'autres ORGANISATIONS qui cherchent à être conformes au présent cadre de GESTION DES RISQUES. Les exigences qui s'appliquent uniquement aux ORGANISMES RESPONSABLES sont clairement identifiées.

5.2 Leadership et engagement

La DIRECTION de l'ORGANISATION a la responsabilité d'assurer la mise en œuvre de la GESTION DES RISQUES tout au long du cycle de vie du SYSTEME TI DE SANTE, et d'évaluer son efficacité.

L'ORGANISATION doit établir et adhérer à un PROCESSUS défini pour la GESTION DES RISQUES.

5.3 Intégration de la GESTION DES RISQUES

Une intégration efficace de la GESTION DES RISQUES repose sur la compréhension des structures et du contexte de l'ORGANISATION. Les structures diffèrent selon l'objet, les objectifs et la complexité de l'ORGANISATION. Le RISQUE est géré au niveau de toutes les parties de la structure de l'ORGANISATION. La GESTION DES RISQUES dans une ORGANISATION relève de la responsabilité de tous ses membres.

L'intégration de la GESTION DES RISQUES est un PROCESSUS dynamique et itératif qui peut être adapté à la culture et aux objectifs de l'ORGANISATION. Il convient que la GESTION DES RISQUES fasse partie intégrante (et non qu'elle soit séparée) de l'objet, de la gouvernance, du leadership, de l'engagement, de la stratégie, des objectifs et des opérations de l'ORGANISATION.

5.4 Conception/planification

5.4.1 Généralités

L'acquisition, l'installation, l'intégration, la mise en œuvre, l'utilisation, la maintenance et la mise hors service d'un SYSTEME TI DE SANTE en toute sécurité dépendent d'une planification efficace de la GESTION DES RISQUES. Les activités de planification s'appliquent aux nouvelles mises en œuvre et modifications des SYSTEMES TI DE SANTE existants.

Le PLAN DE GESTION DES RISQUES du SYSTEME TI DE SANTE vise à documenter et à planifier les activités de GESTION DES RISQUES tout au long du cycle de vie du SYSTEME TI DE SANTE. Il vise également à décrire la manière dont un projet spécifique de SYSTEME TI DE SANTE est conforme au PLAN DE GESTION DES RISQUES. Le PROCESSUS DE GESTION DES RISQUES qui établit les exigences du présent document est représenté à la Figure 2 et s'applique tout au long du cycle de vie du SYSTEME TI DE SANTE.

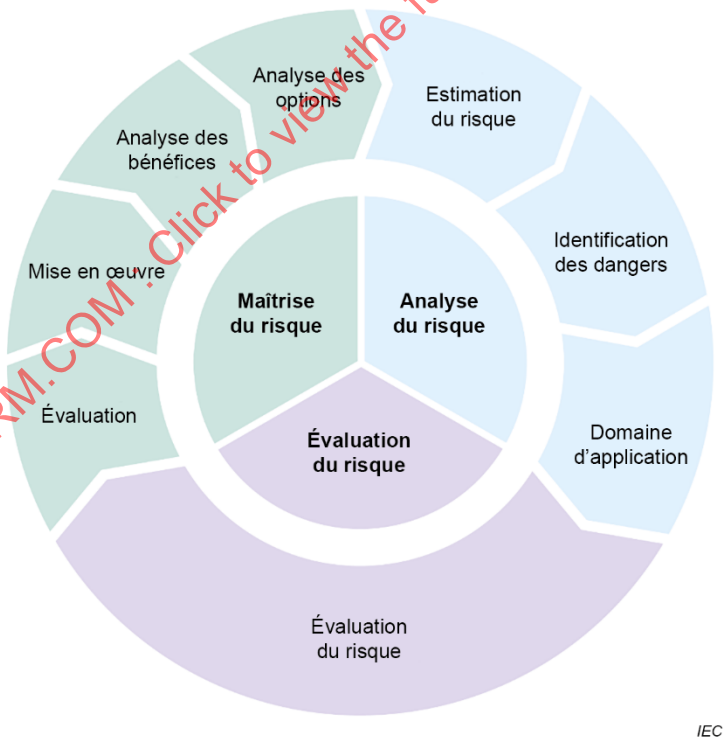


Figure 2 – PROCESSUS DE GESTION DES RISQUES

Il convient que l'étendue du PLAN DE GESTION DES RISQUES soit flexible et adaptée à l'échelle et au domaine d'application des fonctionnalités du SYSTEME TI DE SANTE, tout en traitant des exigences en matière de GESTION DES RISQUES spécifiées dans le présent document. Il convient que le PLAN DE GESTION DES RISQUES comprenne:

– un cadre d'ANALYSE DU RISQUE;

– les critères d'acceptation des risques définis pour les risques individuels et les RISQUES RESIDUELS globaux.
– une liste des procédures, politiques et ressources pertinentes exigées; et
– toute référence à des DOCUMENTS D'ACCOMPAGNEMENT éventuels.

5.4.2 DOSSIER DE GESTION DES RISQUES

L'ORGANISATION doit:

a) établir, au début d'un projet, un DOSSIER DE GESTION DES RISQUES du SYSTEME TI DE SANTE;
b) maintenir le DOSSIER DE GESTION DES RISQUES tout au long du cycle de vie du SYSTEME TI DE SANTE; et
c) assurer que le DOSSIER DE GESTION DES RISQUES est récupérable en cas de défaillance.

Le DOSSIER DE GESTION DES RISQUES du SYSTEME TI DE SANTE constitue une unité de stockage de tous les enregistrements liés au PROCESSUS DE GESTION DES RISQUES et de toutes les décisions qui influencent la GESTION DES RISQUES.

5.4.3 Comprendre l'organisation et l'ECOSYSTEME SOCIOTECHNIQUE

Il est important d'évaluer et de comprendre les ECOSYSTEMES SOCIOTECHNIQUES interne et externe avant de commencer la conception et la mise en œuvre du PLAN DE GESTION DES RISQUES, cette démarche ayant une influence considérable sur la conception du PROCESSUS.

L'ORGANISATION doit établir et maintenir une liste définie d'ELEMENTS D'ACTIFS qui se connectent au SYSTEME TI DE SANTE ou en font partie.

Les facteurs susceptibles d'affecter l'ECOSYSTEME SOCIOTECHNIQUE externe comprennent, entre autres, les éléments et tendances clés qui influent sur les objectifs de l'ORGANISATION, les relations et engagements contractuels, la complexité des réseaux et des dépendances et les conditions réglementaires locales éventuelles.

Les facteurs susceptibles d'affecter l'ECOSYSTEME SOCIOTECHNIQUE interne comprennent, entre autres, la vision, la mission et les valeurs de l'ORGANISATION, la gouvernance, la structure et les responsabilités de l'ORGANISATION, les normes adoptées par l'ORGANISATION, ainsi que ses capacités et actifs.

5.4.4 Articulation de l'engagement en matière de GESTION DES RISQUES

Il incombe à la DIRECTION de l'ORGANISATION de démontrer et d'exprimer son engagement continu en matière de GESTION DES RISQUES en établissant et en appliquant un PLAN DE GESTION DES RISQUES et en évaluant l'EFFICACITE des activités de GESTION DES RISQUES.

La DIRECTION de l'ORGANISATION doit:

a) être chargée de veiller à ce que l'ORGANISATION adhère au PLAN DE GESTION DES RISQUES du SYSTEME TI DE SANTE;
b) être chargée de veiller à ce que l'ORGANISATION se conforme au présent document; et
c) être chargée d'autoriser la vente ou le déploiement du SYSTEME TI DE SANTE.

5.4.5 Attribution de rôles, autorités, responsabilités et imputabilités dans l'organisation

Il revient à la DIRECTION de l'ORGANISATION d'assurer que les autorités, les responsabilités et les imputabilités pour les rôles pertinents en matière de GESTION DES RISQUES sont attribuées et communiquées à tous les niveaux de l'ORGANISATION. Cette tâche inclut l'identification des individus responsables qui ont le pouvoir de gérer les RISQUES et la nomination d'un GESTIONNAIRE DES RISQUES TI DE SANTE qui est responsable de la mise en œuvre du PROCESSUS DE GESTION DES RISQUES.

La DIRECTION de l'ORGANISATION doit:

a) identifier un GESTIONNAIRE DES RISQUES TI DE SANTE qui possède les qualifications, les connaissances et les compétences nécessaires pour appliquer la GESTION DES RISQUES aux SYSTEMES TI DE SANTE;

NOTE 1 La liste des approbateurs contient, au minimum, le GESTIONNAIRE DES RISQUES TI DE SANTE.

b) assurer que les rôles et responsabilités du personnel impliqué dans les activités de GESTION DES RISQUES, y compris les rôles de ceux qui peuvent examiner et approuver les artéfacts de GESTION DES RISQUES, sont définis et consignés;

c) assurer que tous les membres du personnel remplissant ces rôles sont conscients de leurs responsabilités en ce qui concerne le respect du PROCESSUS DE GESTION DES RISQUES de l'ORGANISATION.

Le GESTIONNAIRE DES RISQUES TI DE SANTE doit:

d) être chargé de veiller au respect du PROCESSUS DE GESTION DES RISQUES;

e) de rendre compte du PROCESSUS DE GESTION DES RISQUES à la DIRECTION.

Les responsabilités du GESTIONNAIRE DES RISQUES TI DE SANTE s'appliquent aux nouvelles mises en œuvre du SYSTEME TI DE SANTE et aux modifications apportées aux SYSTEMES TI DE SANTE existants.

L'ORGANISATION doit:

f) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément à ces exigences, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

NOTE 2 Voir l'ISO 81001-1 pour le concept de cas d'assurance.

5.4.6 Allocation de ressources

Le niveau de ressources exigées pour prendre en charge la GESTION DES RISQUES a besoin d'être adapté à l'échelle, à la complexité et au profil de RISQUES du SYSTEME TI DE SANTE et dépend également des calendriers d'exécution du déploiement du SYSTEME TI DE SANTE. L'expérience acquise des déploiements précédents peut orienter l'évaluation des ressources exigées.

Les ressources indiquées pour la GESTION DES RISQUES peuvent inclure, entre autres, des personnes possédant les habiletés, l'expérience et les compétences appropriées, des outils, méthodes, et PROCESSUS DE GESTION DES RISQUES de l'ORGANISATION, ainsi que des systèmes d'information et de gestion des connaissances.

La DIRECTION de l'ORGANISATION doit:

a) fournir des ressources suffisantes pour soutenir la GESTION DES RISQUES;

b) assurer que le personnel impliqué dans la GESTION DES RISQUES est dûment qualifié et expérimenté.

Il convient que l'ORGANISATION prenne en considération les capacités et les contraintes des ressources existantes et vérifie que les ressources désignées disposent d'assez de temps qui leur permet de déployer des efforts adéquats pour assurer une réalisation consistante et compétente du PROCESSUS DE GESTION DES RISQUES.

5.4.7 Établissement de la communication et de la consultation

La communication implique le partage d'informations avec des publics cibles et la consultation implique la fourniture d'informations par les participants conscients de ce que cela contribue aux décisions ou d'autres activités et leur donne forme. Les méthodes et le contenu en matière de communication et de consultation doivent refléter les attentes de tous les intervenants.

La communication et la consultation doivent être effectuées en temps utile. Elles doivent garantir la collecte, la compilation, la synthèse et le partage appropriés des informations pertinentes. Lorsque la responsabilité de la GESTION DES RISQUES est partagée, les détails sont consignés dans un ACCORD DE RESPONSABILITE.

L'ORGANISATION doit:

a) établir des moyens efficaces de partage d'informations avec les intervenants internes et externes dans la GESTION DES RISQUES;

b) établir des moyens efficaces de collecte d'informations chez les intervenants internes et externes dans la GESTION DES RISQUES; et

c) conserver les communications qui ont un impact sur les résultats de la GESTION DES RISQUES.

Les intervenants internes et externes dans la GESTION DES RISQUES peuvent comprendre les acteurs suivants: OPERATEURS, FABRICANTS DE SYSTEMES TI DE SANTE, fonction de support technique, fonction informatique interne et les autres fonctions de gestion des installations.

5.5 Mise en œuvre

La réussite de la mise en œuvre du PROCESSUS DE GESTION DES RISQUES exige de l'engagement et une prise de conscience de la part des intervenants. Cela permet aux ORGANISATIONS de traiter explicitement de l'incertitude dans la prise de décision, en assurant que toute incertitude nouvelle ou ultérieure est prise en considération dès qu'elle se présente.

La réussite de la mise en œuvre du PROCESSUS DE GESTION DES RISQUES dépend du respect du PLAN DE GESTION DES RISQUES. Il convient que le PLAN DE GESTION DES RISQUES définisse clairement les calendriers d'exécution, les étapes clés et les besoins en ressources correspondants.

5.6 Évaluation

Il convient que la conformité au PLAN DE GESTION DES RISQUES et l'efficacité du PROCESSUS DE GESTION DES RISQUES fassent l'objet d'évaluations périodiques. L'évaluation peut être effectuée annuellement ou plus fréquemment lorsque les circonstances changent.

L'ORGANISATION doit:

a) évaluer l'EFFICACITE du PROCESSUS DE GESTION DES RISQUES à des intervalles définis; et

b) enregistrer dans le DOSSIER DE GESTION DES RISQUES les preuves de l'évaluation.

Il convient que l'évaluation de l'EFFICACITE du PROCESSUS DE GESTION DES RISQUES examine les préoccupations et les incidents liés au SYSTEME TI DE SANTE, ainsi que l'impact de ceux-ci sur les PROPRIETES CLES, contrôle la rapidité de notification des INCIDENTS et passe en revue la GESTION DES EVENEMENTS.

5.7 Amélioration

Il convient que l'ORGANISATION s'efforce d'améliorer en continu la conformité, l'adéquation et l'EFFICACITE du PROCESSUS DE GESTION DES RISQUES, ainsi que la méthode de mise en œuvre de ce processus. L'ORGANISATION qui identifie des lacunes ou des possibilités d'amélioration peut concevoir des plans et des tâches et les affecter aux personnes responsables de leur mise en œuvre. Lorsqu'ils auront été mis en œuvre, ces plans et tâches peuvent contribuer à l'amélioration de la GESTION DES RISQUES.

L'ORGANISATION doit:

a) surveiller et adapter en permanence le PROCESSUS DE GESTION DES RISQUES pour faire face aux changements externes et internes; et

b) enregistrer dans le DOSSIER DE GESTION DES RISQUES les preuves de toute amélioration.

L'ORGANISATION peut optimiser l'efficacité et le rendement de son PROCESSUS DE GESTION DES RISQUES en le surveillant et en l'adaptant en permanence.

6 PROCESSUS DE GESTION DES RISQUES

6.1 Exigences générales

6.1.1 Généralités

Le PROCESSUS générique de GESTION DES RISQUES est représenté à la Figure 2. Trois activités principales, soutenues par des sous-activités connexes, sont exécutées en continu tout au long du cycle de vie d'un SYSTEME TI DE SANTE, depuis l'acquisition initiale jusqu'à la mise hors service. Les exigences du présent document s'appliquent aux ORGANISMES RESPONSABLES et à d'autres ORGANISATIONS qui cherchent à être conformes au présent cadre de GESTION DES RISQUES. Les exigences qui s'appliquent uniquement aux ORGANISMES RESPONSABLES sont clairement identifiées.

L'ORGANISATION doit:

a) établir, au début du projet, un PLAN DE GESTION DES RISQUES détaillant les activités d'ANALYSE DU RISQUE, d'EVALUATION DU RISQUE et de MAITRISE DU RISQUE à entreprendre;

b) maintenir le PLAN DE GESTION DES RISQUES cliniques dans le DOSSIER DE GESTION DES RISQUES tout au long du cycle de vie du SYSTEME TI DE SANTE;

c) enregistrer dans le DOSSIER DE GESTION DES RISQUES la justification de tout écart par rapport au PLAN DE GESTION DES RISQUES;

d) établir, au début du projet, un CAS D'ASSURANCE pour le projet;

e) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément à ces exigences, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.1.2 ANALYSE DU RISQUE

6.1.2.1 Généralités

L'ANALYSE DU RISQUE implique une définition du domaine d'application du SYSTEME TI DE SANTE, à la fois en matière d'architecture technologique, de fonctionnalités et d'UTILISATION PREVUE. Dès lors que ce principe est compris, une analyse est menée pour identifier tous les DANGERS susceptibles de se produire. Le RISQUE associé aux DANGERS identifiés est ensuite évalué. Pour ce faire, il est préférable d'organiser un atelier multidisciplinaire auquel participent généralement des représentants compétents des corps spécialisés suivants:

– LA DIRECTION;
– les professionnels des SOINS DE SANTE;
– les propriétaires d'entreprise;
– les INTEGRATEURS DE SYSTEMES;
– les RESPONSABLES DE MISES EN ŒUVRE;
– les ADMINISTRATEURS;
– les UTILISATEURS; et
– les spécialistes en SECURITE.

L'échelle, la complexité et le niveau du RISQUE varient selon les différents déploiements du SYSTEME TI DE SANTE. Il est important de le reconnaître et de veiller à ce que le niveau de ressources exigées pour prendre en charge le PROCESSUS soit proportionné au processus.

6.1.2.2 Définition de l'objet et du domaine d'application du PROCESSUS

Avant de démarrer les activités d'ANALYSE DU RISQUE pour le déploiement ou la modification d'un SYSTEME TI DE SANTE, il est essentiel de définir le domaine d'application de l'ANALYSE DU RISQUE. Une définition appropriée du domaine d'application limite l'étendue de l'ANALYSE DU RISQUE tout en assurant la prise en compte de tous les domaines touchés par le déploiement. Il est important de comprendre la façon dont le LOGICIEL DE SANTE ou le DISPOSITIF MEDICAL s'intègre à l'INFRASTRUCTURE TI DE SANTE existante. Il convient de prendre également en considération toute migration de données exigée pour venir à l'appui du déploiement.

L'ORGANISATION doit:

a) définir le milieu de SOINS DE SANTE dans lequel le SYSTEME TI DE SANTE sera déployé et utilisé;

b) définir l'UTILISATION PREVUE du SYSTEME TI DE SANTE dans le contexte de soutien aux SOINS DE SANTE;

c) identifier les UTILISATEURS du SYSTEME TI DE SANTE;

d) définir l'échelle et la complexité du déploiement du SYSTEME TI DE SANTE, y compris l'intégration de composants dans le SYSTEME TI DE SANTE;

e) identifier et prendre en considération les dépendances fonctionnelles et de données inter- ou intra-SYSTEMES TI DE SANTE.

En outre, un ORGANISME RESPONSABLE doit:

f) définir l'échelle et la complexité du déploiement du SYSTEME TI DE SANTE, y compris l'intégration du SYSTEME TI DE SANTE dans l'INFRASTRUCTURE TI DE SANTE; et

g) recueillir des informations appropriées et suffisantes à partir des DOCUMENTS D'ACCOMPAGNEMENT de chaque FABRICANT DE DISPOSITIF MEDICAL ou de SYSTEME TI DE SANTE pour soutenir la GESTION DES RISQUES.

Pour des recommandations d'informations appropriées et suffisantes à recueillir dans les DOCUMENTS D'ACCOMPAGNEMENT, voir l'Annexe B "Recommandations pour les informations dans les documents d'accompagnement". Des informations supplémentaires sur la sécurité du système sont détaillées dans l'IEC TR 80001-2-2:2012 et l'IEC TR 80001-2-8:2016 et sont reflétées dans le document de déclaration du fabricant sur la sécurité des dispositifs médicaux. L'accord de responsabilité spécifié dans l'ISO/TR 80001-2-6:2014 fournit des informations sur l'élaboration de dispositions contractuelles ou en matière d'appels d'offres entre l'ORGANISME RESPONSABLE et le fournisseur de SYSTEME TI DE SANTE.

L'ORGANISATION doit:

h) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.1.2.3 Identification des DANGERS

L'identification des DANGERS a pour objet de découvrir et de décrire les évènements ou les conditions susceptibles d'entraîner un DOMMAGE lors du déploiement ou de l'utilisation du SYSTEME TI DE SANTE.

Il est recommandé d'organiser un atelier sur les DANGERS, auquel prennent part les intervenants indiqués en 6.1.2.1, pour permettre une identification exhaustive des DANGERS. Il convient de mener les activités d'identification des DANGERS à l'aide d'une technique reconnue telle que la technique d'analyse structurée par simulation (SWIFT - *Structured what if technique*), et de prendre en considération:

- les processus de prestation de SOINS DE SANTE qui sont touchés par le SYSTEME TI DE SANTE, y compris les considérations en matière de flux de travaux et de facteurs humains;
- l'UTILISATION PREVUE du SYSTEME TI DE SANTE au sein de l'ORGANISME RESPONSABLE; et

- les interdépendances associées au SYSTEME TI DE SANTE, y compris les flux de données.

L'ORGANISATION doit:

a) identifier et documenter les DANGERS connus et prévisibles associés au déploiement du SYSTEME TI DE SANTE et à son utilisation dans des conditions de fonctionnement normales et prévisibles;

b) examiner les DANGERS identifiés dans les DOCUMENTS D'ACCOMPAGNEMENT fournis par le FABRICANT DE LOGICIEL DE SANTE ou de DISPOSITIF MEDICAL ou par les fournisseurs d'autres composants principaux de système pour leur applicabilité dans le cadre du déploiement, de l'utilisation ou de la mise hors service du SYSTEME TI DE SANTE; et

c) lorsqu'aucun DANGER n'est identifié, enregistrer cette conclusion et sa justification dans le DOSSIER DE GESTION DES RISQUES.

En outre, l'ORGANISME RESPONSABLE doit:

d) examiner les DANGERS associés à l'intégration du SYSTEME TI DE SANTE dans l'INFRASTRUCTURE TI DE SANTE.

Il est nécessaire d'identifier et d'enregistrer toutes les vulnérabilités et/ou menaces du SYSTEME TI DE SANTE et/ou de son intégration dans l'INFRASTRUCTURE TI DE SANTE.

L'ORGANISATION doit:

e) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.1.2.4 ESTIMATION DU RISQUE

L'ESTIMATION DU RISQUE est le PROCESSUS de catégorisation du RISQUE du DANGER identifié en déterminant les causes et les CONSEQUENCES du DANGER et en prenant en considération la VRAISEMBLANCE de survenue d'un DOMMAGE en raison du DANGER et de la GRAVITE de ce DOMMAGE.

En utilisant les critères spécifiés dans le PLAN DE GESTION DES RISQUES, pour chaque DANGER identifié l'ORGANISATION doit:

a) estimer la GRAVITE de la CONSEQUENCE du DOMMAGE;

b) estimer la VRAISEMBLANCE du DOMMAGE;

c) estimer et enregistrer le RISQUE résultant.

Les critères de RISQUE peuvent varier d'une ORGANISATION à l'autre. L'ORGANISME RESPONSABLE doit:

d) confronter les critères utilisés par le FABRICANT DE LOGICIEL DE SANTE ou de DISPOSITIF MEDICAL aux critères utilisés par l'ORGANISME RESPONSABLE (par exemple, au schéma de classification des risques).

L'ORGANISATION doit:

e) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

Ce PROCESSUS prend en compte le scénario le plus réaliste et le plus typique qui peut entraîner un DOMMAGE. Il est possible que la CONSEQUENCE d'un DANGER ait plus d'un degré de GRAVITE. Par exemple, la CONSEQUENCE d'une prescription par inadvertance d'une surdose d'un médicament particulier à un patient peut être plus grave et immédiate (ne laissant que peu ou pas de temps pour une intervention) par rapport à la conséquence de la surdose d'un autre médicament qui peut simplement entraîner des désagréments après une période écoulée. La

VRAISEMBLANCE de survenue du premier cas peut être nettement inférieure à celle du dernier cas si le premier porte sur le traitement d'une affection très rare. L'APPRECIATION DU RISQUE doit prendre en considération tous les scénarios de DANGER et en déterminer les degrés de GRAVITE et de VRAISEMBLANCE correspondants. Lorsque la cause du DANGER est commune pour les différents scénarios, le degré de RISQUE le plus élevé peut être utilisé, sur la base de ce qu'un même DANGER peut avoir plusieurs causes.

La GRAVITE est appréciée sur une échelle qualitative qui prend en compte le DOMMAGE susceptible de se produire. Il est attribué à chaque catégorie de GRAVITE une signification associée qui permet de différencier les catégories.

Les SYSTEMES TI DE SANTE sont vulnérables aux défauts systématiques, ce qui signifie que, contrairement aux défauts aléatoires, la VRAISEMBLANCE de leur occurrence ne peut pas être quantifiée. Par conséquent, la VRAISEMBLANCE est soumise à un jugement sur une échelle qualitative. Il est attribué à chaque catégorie de VRAISEMBLANCE une signification associée qui permet de différencier les catégories.

6.1.3 ÉVALUATION DU RISQUE

L'EVALUATION DU RISQUE est le PROCESSUS consistant à évaluer si, à l'aide des critères définis dans le PLAN DE GESTION DES RISQUES, le RISQUE lié à un DANGER est acceptable ou si des mesures supplémentaires sont nécessaires. Le RISQUE INITIAL est le RISQUE qui existe avant l'introduction de toute mesure supplémentaire de contrôle. En règle générale, le RISQUE est évalué à l'aide d'une matrice combinant à la fois la GRAVITE et la VRAISEMBLANCE et générant une plage dans laquelle le RISQUE est considéré comme "acceptable". Lorsque le RISQUE se situe hors de la plage "acceptable", il peut toujours être "accepté" par une ORGANISATION si les bénéfices associés au déploiement l'emportent sur le RISQUE associé. Ces décisions sont étayées par une analyse Bénéfice-RISQUE (voir 6.1.4.2).

En utilisant les critères spécifiés dans le PLAN DE GESTION DES RISQUES, pour chaque DANGER l'ORGANISATION doit:

a) évaluer l'acceptabilité du RISQUE INITIAL;

b) satisfaire à toutes les exigences de 6.1.4 lorsque le RISQUE INITIAL est considéré comme inacceptable; et

c) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.1.4 MAITRISE DU RISQUE

6.1.4.1 Analyse de MAITRISE DU RISQUE

Les mesures de MAITRISE DU RISQUE peuvent réduire la VRAISEMBLANCE de survenue du DANGER ou atténuer la GRAVITE des CONSEQUENCES du DANGER.

Pour chaque DANGER, l'ORGANISATION doit:

a) identifier les mesures de MAITRISE DU RISQUE;

b) évaluer les mesures de MAITRISE DU RISQUE afin de déterminer si de nouveaux DANGERS sont introduits par suite de la mise en œuvre de ces mesures ou si les RISQUES des DANGERS déjà identifiés sont affectés;

c) gérer conformément aux exigences du présent document tout nouveau DANGER ou tout RISQUE accru;

d) évaluer le RISQUE RESIDUEL en utilisant les critères d'acceptabilité du RISQUE définis dans le PLAN DE GESTION DES RISQUES;

e) lorsque le RISQUE RESIDUEL est inacceptable, identifier des mesures de MAITRISE DU RISQUE supplémentaires afin de réduire le RISQUE;

f) lorsqu'une mesure de MAITRISE DU RISQUE doit être mise en œuvre par une autre ORGANISATION, enregistrer clairement cette dépendance dans le CAS D'ASSURANCE;

g) effectuer une analyse bénéfice-RISQUE (voir 6.1.4.2) du RISQUE lorsqu'aucune mesure appropriée de MAITRISE DU RISQUE n'est possible; et

h) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES;

Les mesures de MAITRISE DU RISQUE ont différents domaines d'efficacité. Les domaines suivants sont présentés par ordre d'efficacité de ces mesures:

– modification de conceptions (suppression de dangers, par exemple) ou inclusion de mesures de protection dans le SYSTEME TI DE SANTE;

– procédures administratives et de mise en œuvre; et

– formation et briefing des UTILISATEURS et d'autres intervenants.

L'introduction des mesures de MAITRISE DU RISQUE peut donner lieu à des compromis entre les PROPRIETES CLES de SECURITE, d'EFFICACITE et de SURETE. Il convient d'adopter, dans la mesure du possible, une vision équilibrée et de choisir les mesures de MAITRISE DU RISQUE qui permettent une réduction optimale des RISQUES associés aux trois PROPRIETES CLES. Cette recommandation est particulièrement importante dans les ORGANISMES RESPONSABLES où l'introduction du SYSTEME TI DE SANTE dans l'INFRASTRUCTURE TI DE SANTE existante doit être prise en compte et équilibrée dans le contexte plus large de prestation de SOINS DE SANTE holistique.

Une distinction importante doit être faite entre les RISQUES RESIDUELS qui sont si faibles qu'il n'est pas nécessaire de les gérer par des moyens autres que la vérification de l'efficacité des mesures de MAITRISE DU RISQUE et les RISQUES RESIDUELS qui sont plus importants, mais acceptés en raison des bénéfices associés introduits et de l'impossibilité de réduire davantage les RISQUES. Si l'ORGANISATION détermine, au cours de l'analyse de MAITRISE DU RISQUE, que la réduction du RISQUE requise n'est pas raisonnablement possible, l'ORGANISATION doit effectuer et documenter une analyse bénéfice-RISQUE (voir 6.1.4.2) du RISQUE RESIDUEL.

6.1.4.2 Analyse bénéfice-RISQUE

Il faut décider si les bénéfices procurés par le SYSTEME TI DE SANTE l'emportent ou non sur les RISQUES RESIDUELS associés à un DANGER (et le RISQUE RESIDUEL global). La décision est généralement prise par le jugement de personnes expérimentées et bien averties, y compris le GESTIONNAIRE DES RISQUES TI DE SANTE. Les personnes chargées de porter des jugements bénéfice-RISQUE ont la responsabilité de comprendre et de prendre en considération le contexte technique, clinique, réglementaire, économique, sociologique et politique de leurs décisions en matière de GESTION DES RISQUES. L'analyse doit prendre également en considération le bénéfice-RISQUE global, c'est-à-dire la somme de tous les risques non acceptés et des bénéfices cliniques nets du déploiement. Si l'analyse ne permet pas de conclure que les bénéfices l'emportent sur le RISQUE RESIDUEL, le RISQUE reste inacceptable.

Procéder à un déploiement pour lequel le RISQUE est inacceptable exige l'approbation explicite de la DIRECTION conformément à tout PROCESSUS de gouvernance existant.

Pour chaque DANGER dont le RISQUE RESIDUEL reste inacceptable après la mise en application de toutes les mesures pratiques de MAITRISE DU RISQUE, l'ORGANISATION doit:

a) démontrer qu'aucune autre mesure réalisable ne peut être appliquée pour réduire le RISQUE RESIDUEL à un niveau acceptable;

b) lorsque la décision d'accepter le RISQUE RESIDUEL a été prise, consigner la justification et le contexte du jugement dans le CAS D'ASSURANCE.

L'ORGANISME RESPONSABLE doit également:

c) examiner le RISQUE RESIDUEL global de tous les DANGERS en relation avec les bénéfices cliniques pouvant être réalisés; et

d) lorsque le RISQUE RESIDUEL ne peut être accepté, consigner dans le CAS D'ASSURANCE la justification de toute décision de déploiement prise par la DIRECTION.

L'ORGANISATION doit:

e) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.1.4.3 VERIFICATION des mesures de MAITRISE DU RISQUE

La VERIFICATION des mesures DE MAITRISE DU RISQUE donne l'assurance que leur mise en œuvre réduit efficacement les RISQUES à un niveau acceptable. L'ORGANISATION doit:

a) mettre en œuvre les mesures de MAITRISE DU RISQUE identifiées selon le 6.1.4.1;

b) vérifier l'EFFICACITE de chaque mesure de MAITRISE DU RISQUE; et

c) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

La VERIFICATION de l'EFFICACITE des mesures de MAITRISE DU RISQUE mises en application est effectuée avant la mise en oeuvre du SYSTEME TI DE SANTE ou avant la décision de le déployer. Les moyens et la responsabilité de mise en œuvre de la VERIFICATION dépendent de la nature de la mesure de MAITRISE DU RISQUE. Par exemple, une mesure de MAITRISE DU RISQUE pour une défaillance de la liaison réseau peut être la fourniture d'une liaison redondante. La VERIFICATION de l'EFFICACITE implique la simulation d'une défaillance de la liaison principale et la vérification de l'efficacité de la liaison redondante. Il n'est pas possible de vérifier objectivement l'EFFICACITE dans certains cas, par exemple dans les cas de perfectionnement professionnel et de modification des PROCESSUS et procédures opérationnels.

NOTE Il est possible de vérifier l'EFFICACITE des mesures de MAITRISE DU RISQUE dans un environnement d'essai avant leur mise en application dans un système opérationnel.

6.1.4.4 ÉVALUATION et compte-rendu du RISQUE RESIDUEL

Avant de déployer un SYSTEME TI DE SANTE, nouveau ou modifié, l'ORGANISATION doit:

a) examiner l'acceptabilité à la fois du RISQUE RESIDUEL individuel de chaque DANGER et du RISQUE RESIDUEL global; et

b) si le RISQUE RESIDUEL dépasse les seuils d'acceptabilité, démontrer qu'une analyse bénéfice-RISQUE a été menée à l'appui de toute décision de déploiement du SYSTEME TI DE SANTE.

En outre, l'ORGANISME RESPONSABLE doit

c) examiner le CAS D'ASSURANCE du FABRICANT DE SYSTEMES TI DE SANTE ou une documentation équivalente pour assurer que le RISQUE RESIDUEL de tous les DANGERS consignés a été pris en compte dans le contexte du déploiement et de l'UTILISATION PREVUE et que l'acceptabilité des RISQUES RESIDUELS individuels et du RISQUE RESIDUEL global est justifiée.

L'ORGANISATION doit:

d) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.2 Exigences spécifiques au cycle de vie

6.2.1 Généralités

Les paragraphes suivants examinent chaque phase du cycle de vie identifiée à la Figure 1 et définissent explicitement l'ensemble minimal d'exigences applicables à une phase donnée du cycle de vie. Dans tous les cas, cet ensemble comprend un sous-ensemble d'exigences issues du 6.1 et des exigences spécifiques à la phase particulière du cycle de vie. De même, il convient de prendre en considération, dans la mesure du possible, les exigences figurant dans d'autres paragraphes si les informations et les éléments de compréhension nécessaires sont disponibles à la phase particulière du cycle de vie.

Un paragraphe inclut tous les paragraphes relatifs aux enfants, sauf indication contraire.

6.2.2 Acquisition

Il est nécessaire d'initier la GESTION DES RISQUES tôt dans le cycle de vie pour identifier les DANGERS potentiels et les RISQUES associés et pour influencer les activités ultérieures du cycle de vie.

Au cours de cette phase du cycle de vie, l'ORGANISME RESPONSABLE doit:

a) satisfaire aux exigences de 6.1.1, 6.1.2.2 et 6.1.2.3;

b) communiquer le domaine d'application du SYSTEME TI DE SANTE qu'il envisage de mettre en œuvre à toutes les parties (internes et externes) impliquées dans le PROCESSUS d'acquisition;

c) associer les principaux intervenants (y compris les cliniciens et les experts en technologie de l'information) à une évaluation objective des bénéfices et des RISQUES liés à la mise en œuvre du SYSTEME TI DE SANTE; et

d) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER de GESTION DES RISQUES.

Comme cela est indiqué en 6.1.2, le domaine d'application inclut les exigences fonctionnelles et techniques, les spécifications d'intégration des données et du système, ainsi qu'une description détaillée de l'UTILISATION PREVUE du système dans le contexte clinique et commercial spécifique de l'ORGANISME RESPONSABLE. L'évaluation des bénéfices et des RISQUES au cours de cette phase du cycle de vie inclut ceux inhérents au SYSTEME TI DE SANTE et aux ELEMENTS D'ACTIFS associés. Elle inclut également le degré de personnalisation et d'intégration (qui est exigé) dans l'ECOSYSTEME SOCIOTECHNIQUE de l'ORGANISME RESPONSABLE.

6.2.3 Installation, personnalisation et configuration

Les SYSTEMES TI DE SANTE sont généralement configurés pour prendre en charge les exigences locales. Dans de tels cas, chaque ORGANISME RESPONSABLE doit:

a) examiner les éléments du 6.2.2 pour assurer qu'ils restent valables. Il peut être nécessaire de répéter ces activités dans le cadre d'informations nouvelles ou supplémentaires;

b) satisfaire aux exigences de 6.1.1, 6.1.2 et 6.1.3;

c) examiner le rapport du CAS D'ASSURANCE ou une documentation équivalente et toute information justificative fournie par le FABRICANT DE LOGICIEL DE SANTE ou de DISPOSITIF MEDICAL afin d'assurer que le système reste applicable et valable dans son propre contexte;

d) si des défauts sont identifiés, effectuer une GESTION DES RISQUES supplémentaire selon 6.1; et

e) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.2.4 Intégration, migration de données, transition et validation

Les RISQUES liés aux SOINS DE SANTE peuvent survenir lorsque le SYSTEME TI DE SANTE est physiquement intégré dans l'INFRASTRUCTURE TI DE SANTE. Pour réduire le plus possible les RISQUES, l'ORGANISME RESPONSABLE doit

a) examiner les éléments du 6.2.3 pour assurer qu'ils restent valables. Il peut être nécessaire de répéter ces activités dans le cadre d'informations nouvelles ou supplémentaires;

b) satisfaire aux exigences de 6.1.1;

c) gérer l'intégration du SYSTEME TI DE SANTE (y compris l'intégration technique et des données) au moyen d'un plan global qui identifie toutes les activités à mener et tous les intervenants qui doivent être impliqués; et

d) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.2.5 Mise en œuvre, optimisation du flux de travaux et formation

Avant de déployer le SYSTEME TI DE SANTE pour son utilisation en temps réel, l'ORGANISME RESPONSABLE doit vérifier que toutes les activités de GESTION DES RISQUES sont achevées et que le profil de RISQUES est connu et compris.

L'ORGANISME RESPONSABLE doit:

a) examiner les éléments du 6.2.4 pour assurer qu'ils restent valables. Il peut être nécessaire de répéter ces activités dans le cadre d'informations nouvelles ou supplémentaires;

b) satisfaire aux exigences de 6.1.4.4;

c) confirmer que le PLAN DE GESTION DES RISQUES a été mis en œuvre et que les résultats ont été consignés;

d) effectuer un examen formel du SYSTEME TI DE SANTE avant son déploiement pour assurer que les exigences du présent document ont été satisfaites;

e) confirmer que la DIRECTION comprend et accepte le profil de RISQUES du déploiement. (Dans tous les cas, la DIRECTION se réserve la responsabilité du déploiement du SYSTEME TI DE SANTE); et

f) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

Toutes les mesures de MAITRISE DU RISQUE transférées d'une autre ORGANISATION à l'ORGANISME RESPONSABLE doivent faire l'objet d'une attention particulière pour assurer qu'elles ont été mises en œuvre et se sont révélées efficaces. Il est possible que les flux de travaux existants aient besoin d'être ajustés pour s'adapter au SYSTEME TI DE SANTE et que les OPERATEURS et les UTILISATEURS aient besoin d'être formés.

6.2.6 Exploitation et maintenance

L'ORGANISATION doit contrôler et examiner de manière proactive les caractéristiques atteintes pour les PROPRIETES CLES du SYSTEME TI DE SANTE après son déploiement. Les incidents doivent être détectés et résolus rapidement lorsqu'ils se produisent. La maintenance entreprise pour soutenir l'efficacité continue des mesures de MAITRISE DU RISQUE ou pour introduire de nouvelles fonctionnalités relève également du domaine d'application du présent document.

L'ORGANISATION doit:

a) satisfaire aux exigences de 6.1.2, 6.2.4 et 6.2.5 dans une mesure proportionnée au risque de l'INCIDENT ou à l'ampleur de la modification;

b) démontrer que les performances associées au RISQUE font l'objet d'un suivi et d'une gestion efficace;

c) le cas échéant, apporter des modifications aux mesures existantes de MAITRISE DU RISQUE afin de maintenir un niveau de RISQUE acceptable;

d) établir un PROCESSUS de gestion des INCIDENTS pour collecter et examiner les préoccupations et les incidents signalés pour le SYSTEME TI DE SANTE après son déploiement;

e) évaluer l'impact de tout incident sur la validité en cours du CAS D'ASSURANCE;

f) prendre des mesures correctives appropriées conformément au PLAN DE GESTION DES RISQUES lorsque l'INCIDENT porte atteinte au cas d'assurance;

g) tenir un registre des incidents, y compris de leur résolution; et

h) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

Il convient qu'un PROCESSUS de gestion des INCIDENTS:

– permette aux UTILISATEURS du SYSTEME TI DE SANTE de signaler les incidents qui ont causé ou qui ont été susceptibles de causer un dommage;

– prévoie un mécanisme de communication qui peut être utilisé par chaque ORGANISME RESPONSABLE et par chaque FABRICANT DE SYSTEMES TI DE SANTE;

– assure que l'ORGANISATION alloue des ressources appropriées et suffisantes pour gérer et résoudre les incidents signalés;

– permette à chaque ORGANISME RESPONSABLE de répondre à une alerte ou un bulletin quelconque émanant d'un FABRICANT DE SYSTEMES TI DE SANTE;

– prévoie un point de contact principal (centre d'assistance) où les incidents sont enregistrés;

– mette en place un moyen permettant d'effectuer une APPRECIATION DU RISQUE. Dans la pratique, il s'agit des mêmes critères que ceux définis dans le PLAN DE GESTION DES RISQUES;

– facilite l'examen du CAS D'ASSURANCE existant pour déterminer si les incidents signalés constituent un nouveau DANGER, une concrétisation d'un DANGER existant ou si les mesures de MAITRISE DU RISQUE ont échoué;

– inclue une analyse des causes profondes;

– accorde la permission aux autorités compétentes de déployer les modifications du SYSTEME TI DE SANTE, d'apporter des modifications aux PROCESSUS opérationnels et de résoudre les incidents;

– établisse des indicateurs de performance clés pour assurer une gestion efficace des INCIDENTS; et

– prévoie un moyen permettant à la communauté des UTILISATEURS d'être informée de la résolution d'un INCIDENT particulier.

Un SYSTEME TI DE SANTE peut être modifié ou mis à jour pendant sa durée de vie. Un tel changement peut être motivé par la suppression des corrections, l'introduction de nouvelles fonctionnalités ou une réponse à une menace à la sécurité. L'ORGANISATION doit également examiner les méthodes d'exécution des activités planifiées, telles que l'application de correctifs, la sauvegarde de données et les mises à jour automatiques.

L'ORGANISATION doit

i) documenter le PROCESSUS DE GESTION DU DECLENCHEMENT DES MODIFICATIONS qui inclut la GESTION DES RISQUES.

Lorsqu'un SYSTEME TI DE SANTE est modifié, l'ORGANISATION doit:

j) appliquer la GESTION DES RISQUES à tout changement ou toute modification introduit(e) dans le SYSTEME TI DE SANTE.

Lorsqu'un SYSTEME TI DE SANTE est modifié par l'ORGANISME RESPONSABLE, avec le consentement du FABRICANT DU SYSTEME TI DE SANTE, l'ORGANISME RESPONSABLE doit:

k) confirmer que la modification a été effectuée conformément aux instructions du FABRICANT DU SYSTEME TI DE SANTE;

Il est fortement recommandé qu'un ORGANISME RESPONSABLE n'apporte aucune modification à un SYSTEME TI DE SANTE sans le consentement documenté du FABRICANT DE SYSTEMES TI DE SANTE. Si une telle modification est entreprise, l'ORGANISME RESPONSABLE doit:

l) notifier le changement à l'ORGANISATION DU FABRICANT; et

m) lorsque la modification est apportée à un DISPOSITIF MEDICAL, suivre toutes les étapes réglementaires nécessaires à la mise en service d'un tel SYSTEME TI DE SANTE modifié (par exemple, une configuration selon les instructions d'utilisation du fabricant peut constituer un consentement implicite).

L'ORGANISATION doit:

n) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

6.2.7 Mise hors service

Les SYSTEMES TI DE SANTE mis hors service sont soumis aux mêmes activités de GESTION DES RISQUES que lors de leur premier déploiement. À ce stade du cycle de vie, l'accent est mis sur la MAITRISE DU RISQUE des DANGERS associés au retrait de service du SYSTEME TI DE SANTE.

L'ORGANISME RESPONSABLE doit:

a) satisfaire aux exigences de 6.1.2, 6.2.4 et 6.2.5;

b) appliquer son PROCESSUS DE GESTION DES RISQUES pour prendre en charge le déploiement de tout autre SYSTEME TI DE SANTE ultérieur;

c) examiner l'impact de la suppression des fonctionnalités du SYSTEME TI DE SANTE de l'ORGANISME RESPONSABLE sur la prestation de soins;

d) le cas échéant, introduire des PROCESSUS opérationnels nouveaux ou modifiés et/ou des formations pour pallier la perte du SYSTEME TI DE SANTE ou pour venir à l'appui d'un autre SYSTEME TI DE SANTE;

e) veiller à ce que la GESTION DES RISQUES prenne en considération la migration des données entre le SYSTEME TI DE SANTE mis hors service et le SYSTEME TI DE SANTE ultérieur;

f) prendre les dispositions appropriées pour la conservation et la récupération des informations médicales après la mise hors service;

g) lorsqu'aucun DANGER n'est identifié, enregistrer cette conclusion et sa justification dans le DOSSIER DE GESTION DES RISQUES; et

h) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément aux exigences du présent paragraphe, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.

Annexe A
(informative)

Tableau de correspondance des exigences de l'IEC 80001-1

Le Tableau A.1 met en correspondance les exigences de la présente édition de l'IEC 80001-1 avec les paragraphes de la norme.

Tableau A.1 – Tableau des exigences de l'IEC 80001-1

Paragraphe	Exigence
5.2 Leadership et engagement	**L'ORGANISATION doit:** a) établir et adhérer à un PROCESSUS défini pour la GESTION DES RISQUES.
5.4.2 DOSSIER DE GESTION DES RISQUES	**L'ORGANISATION doit:** a) établir, au début d'un projet, un DOSSIER DE GESTION DES RISQUES du SYSTEME TI DE SANTE; b) maintenir le DOSSIER DE GESTION DES RISQUES tout au long du cycle de vie du SYSTEME TI DE SANTE; et c) assurer que le DOSSIER DE GESTION DES RISQUES est récupérable en cas de défaillance.
5.4.3 Comprendre l'ORGANISATION et l'ECOSYSTEME SOCIOTECHNIQUE	**L'ORGANISATION doit:** a) établir et maintenir une liste définie d'ÉLEMENTS D'ACTIFS qui se connectent au SYSTEME TI DE SANTE ou en font partie.
5.4.4 Articulation de l'engagement en matière de GESTION DES RISQUES	**La DIRECTION de l'ORGANISATION doit:** a) être chargée de veiller à ce que l'ORGANISATION adhère au PLAN DE GESTION DES RISQUES du SYSTEME TI DE SANTE; b) être chargée de veiller à ce que l'ORGANISATION se conforme au présent document; et c) être chargée d'autoriser la vente ou le déploiement du SYSTEME TI DE SANTE.
5.4.5 Attribution de rôles, autorités, responsabilités et imputabilités dans l'organisation	**La DIRECTION de l'ORGANISATION doit:** a) identifier un GESTIONNAIRE DES RISQUES TI DE SANTE qui possède les qualifications, les connaissances et les compétences nécessaires pour appliquer la GESTION DES RISQUES aux SYSTEMES TI DE SANTE; b) assurer que les rôles et responsabilités du personnel impliqué dans les activités de GESTION DES RISQUES, y compris les rôles de ceux qui peuvent examiner et approuver les artéfacts de GESTION DES RISQUES, sont définis et consignés; c) assurer que tous les membres du personnel remplissant ces rôles sont conscients de leurs responsabilités en ce qui concerne le respect du PROCESSUS DE GESTION DES RISQUES de l'ORGANISATION; **Le GESTIONNAIRE DES RISQUES TI DE SANTE doit:** d) être chargé de veiller au respect du PROCESSUS DE GESTION DES RISQUES; e) de rendre compte du PROCESSUS DE GESTION DES RISQUES à la DIRECTION. **L'ORGANISATION doit:** f) incorporer les résultats des activités de GESTION DES RISQUES, effectuées conformément à ces exigences, dans le CAS D'ASSURANCE et les consigner dans le DOSSIER DE GESTION DES RISQUES.
5.4.6 Allocation de ressources	**La DIRECTION de l'ORGANISATION doit:** a) fournir des ressources suffisantes pour soutenir la GESTION DES RISQUES; b) assurer que le personnel impliqué dans la GESTION DES RISQUES est dûment qualifié et expérimenté.