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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

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

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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).

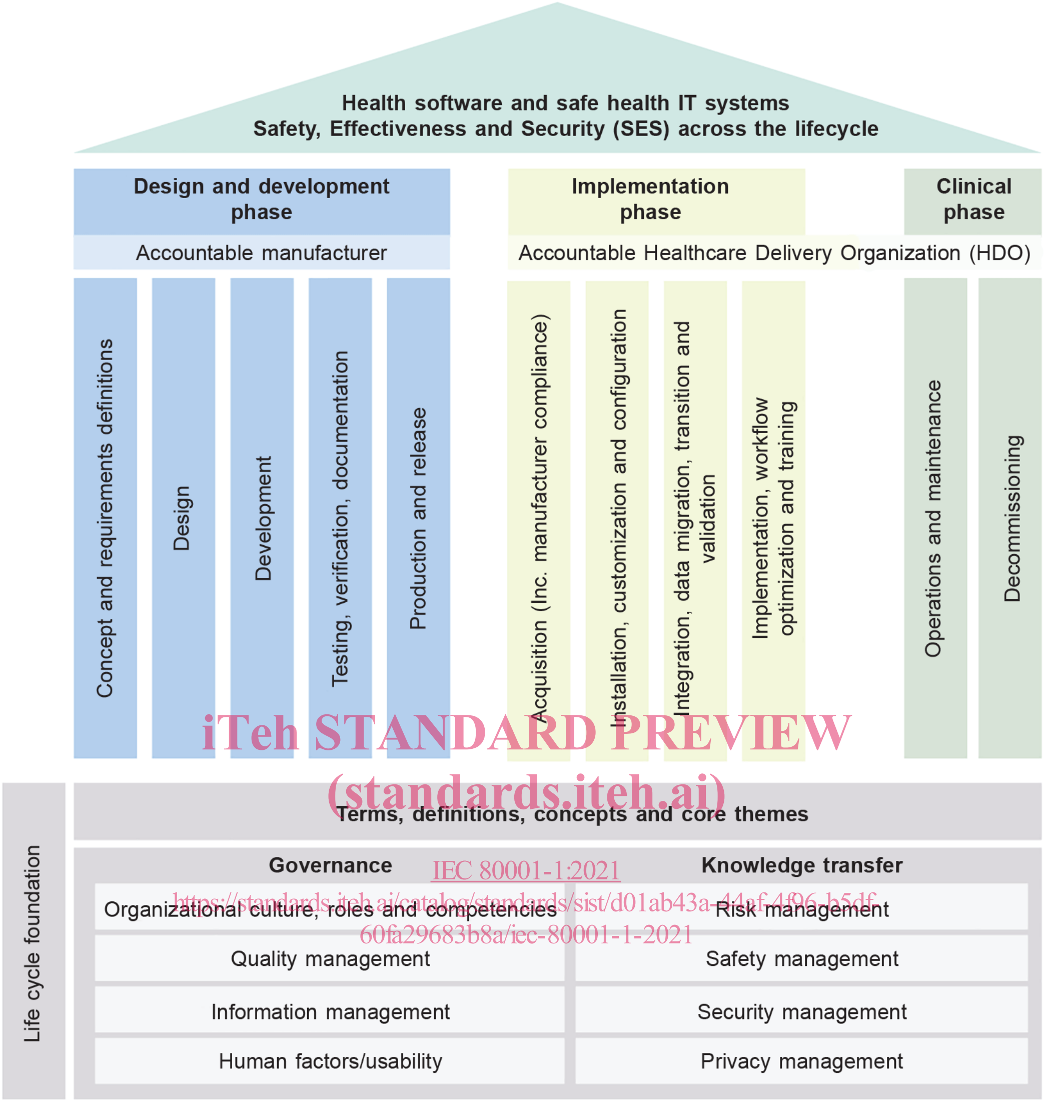
Health software and safe health IT systems
Safety, Effectiveness and Security (SES) across the lifecycle
Design and development phase
Accountable manufacturer
Implementation phase
Clinical phase
Accountable Healthcare Delivery Organization (HDO)
Concept and requirements definitions
Design
Development
Testing, verification, documentation
Production and release
Acquisition (Inc. manufacturer compliance)
Installation, customization and configuration
Integration, data migration, transition and validation
Implementation, workflow optimization and training
Operations and maintenance
Decommissioning
Life cycle foundation
Terms, definitions, concepts and core themes
Governance
Knowledge transfer
Organizational culture, roles and competencies
Risk management
Quality management
Safety management
Information management
Security management
Human factors/usability
Privacy management
IEC

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.

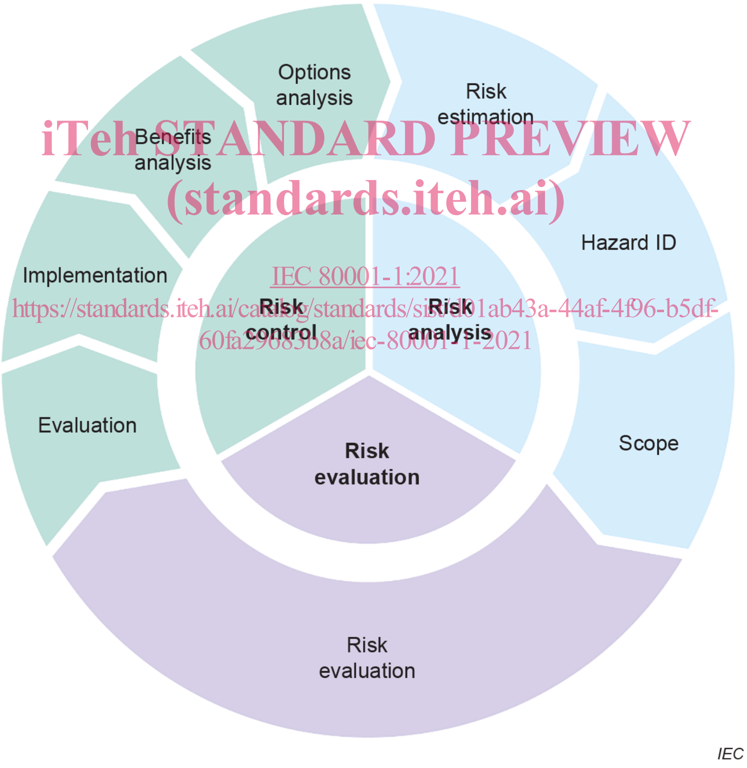

Figure 2 – RISK MANAGEMENT PROCESS

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;