DRAFT INTERNATIONAL STANDARD

IEC/DIS 80001-1

ISO/TC **215** | Secretariat: **ANSI**

Voting begins on: **2020-01-23** | Voting terminates on: **2020-04-16**

Application of risk management for IT-networks incorporating medical devices —

Part 1: Roles, responsibilities and activities

Application du management du risque aux réseaux des technologies de l'information contenant les dispositifs médicaux —

Partie 1: Rôles, responsabilités et activités

ICS: 11.040.01; 35.240.80

Member bodies are requested to consult relevant national interests in IEC/SC 62A before casting their ballot to the e-Balloting application.

This document is circulated as received from the committee secretariat.

Reference number
IEC/DIS 80001-1:2020(E)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE

Part 1: Application of RISK MANAGEMENT

FOREWORD

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

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

It is published as a double logo standard.

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 and guidance for an ORGANIZATION in the application of RISK MANAGEMENT;

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 International Standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this International Standard 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 document 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 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 permission (e.g. a permissible way to achieve compliance with a requirement or test);
- “can” is used to describe a possibility or capability;

- "must" is used to express an external constraint that is not a requirement of the document; and
- "establish" means to define, document, and implement.

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 health IT systems or connected health software,* can be found on the IEC website.

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

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

The National Committees are requested to note that for this document the stability date is 2026.

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

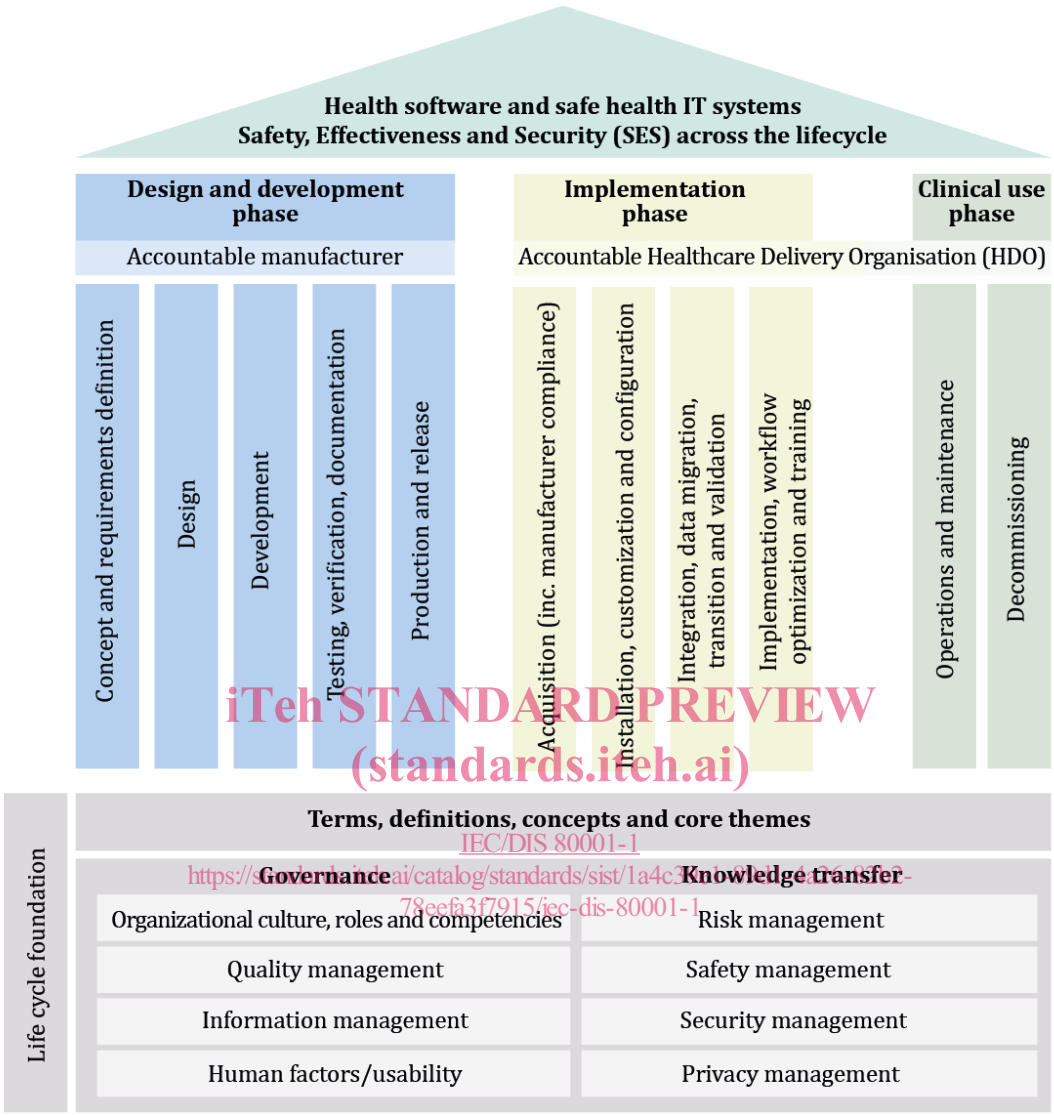
INTRODUCTION

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 and guidance 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 & clinical use" (see the lifecycle diagram in Figure 1).

176



177

178 **Figure 1: Lifecycle framework addressing safety, security & effectiveness of health IT**
179 **software and health IT systems**

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

186 The RISK MANAGEMENT requirements of this document are based upon existing concepts adapted
187 and extended for use by all stakeholders supporting implementation and clinical use of connected
188 HEALTH IT SYSTEMS or HEALTH SOFTWARE. This document aligns with ISO 81001-1, ISO Guide 63,
189 IEC Guide 120. It also builds upon ISO 31000 and ISO 14971.

SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE –

Part 1: Application of risk management

1 Scope

This document specifies a framework of general requirements, guidance, 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

ISO 81001-1 ED2, *Health informatics – Health software and health IT systems safety, effectiveness and security – Part 1: Foundational principles, concepts and terms*.

3 Terms and Definitions

With the exception of the terms and definitions listed in this section all terms and definitions used in this document are taken from ISO 81001-1 ED2.

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

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

3.1
CONSEQUENCE
outcome of an event affecting objectives

[BS ISO 31000:2018, definition 3.6]

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.

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

[BS ISO 13940:2015, definition 3.1.1]

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.

3.3
INITIAL RISK
The RISK derived during risk estimation taking into consideration any retained RISK control measures.

[ISO/IEC/IEEE 15026-1:2019, definition 3.3.3]

231

232 **3.4**
233 **LIKELIHOOD**
234 chance of something happening

235 [BS ISO 31000:2018, definition 3.7]

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

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

243 **3.5**
244 **PROCESS**
245 set of interrelated or interacting activities which transforms inputs into outputs

246 [IEC 80001-1 2010, definition 2.19]

247 NOTE The term “activities” covers use of resources

248 **3.6**
249 **RISK MANAGER**
250 person accountable for RISK MANAGEMENT of a HEALTH IT SYSTEM.

251 [IEC 80001-1 2010, definition 2.17]

252 **3.7**

253 **RISK MANAGEMENT PLAN**
254 A description of how the elements and resources of the risk management process will be
255 implemented within an organization or project

256 [BS ISO/IEC 16085:2006, definition 3.1.1]

257

258 ## 4 Principles

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

263 - RISK MANAGEMENT is an integral part of an ORGANIZATION’S activities at all stages of the
264 HEALTH IT SYSTEM lifecycle;

265 - Accountability for the RISK MANAGEMENT PROCESS remains with the HEALTHCARE DELIVERY
266 ORGANIZATION;

267 - A HEALTHCARE DELIVERY ORGANIZATION may assign responsibility for RISK MANAGEMENT of the
268 HEALTH IT SYSTEM and or HEALTH IT INFRASTRUCTURE to a different ORGANIZATION such as
269 providers of HEALTH IT SYSTEMS, HEALTH IT INFRASTRUCTURE or a collaboration of
270 HEALTHCARE DELIVERY ORGANIZATIONS.

271 RISK MANAGEMENT creates and protects value. It contributes to the demonstrable maintenance
272 or/and improvement of SAFETY, EFFECTIVENESS and SECURITY in the implementation and use of
273 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 needs to 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 ORGANIZATION resilience and supports the ORGANIZATION'S business needs and objectives.

NOTE 1 Risk should be 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 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:

a) 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. RISK is managed in every part of the ORGANIZATION'S structure. Everyone in an ORGANIZATION has responsibility for managing RISK.
Integrating RISK MANAGEMENT is a dynamic and iterative process that can be customised to the ORGANIZATION'S culture and objectives. RISK MANAGEMENT should be part of, and not separate

317 from, organizational purpose, governance, leadership, commitment, strategy, objectives and
318 operations.
319
320 **5.4 Design/planning**

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