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 It also gives information on projects, replaced and withdrawn publications.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

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).

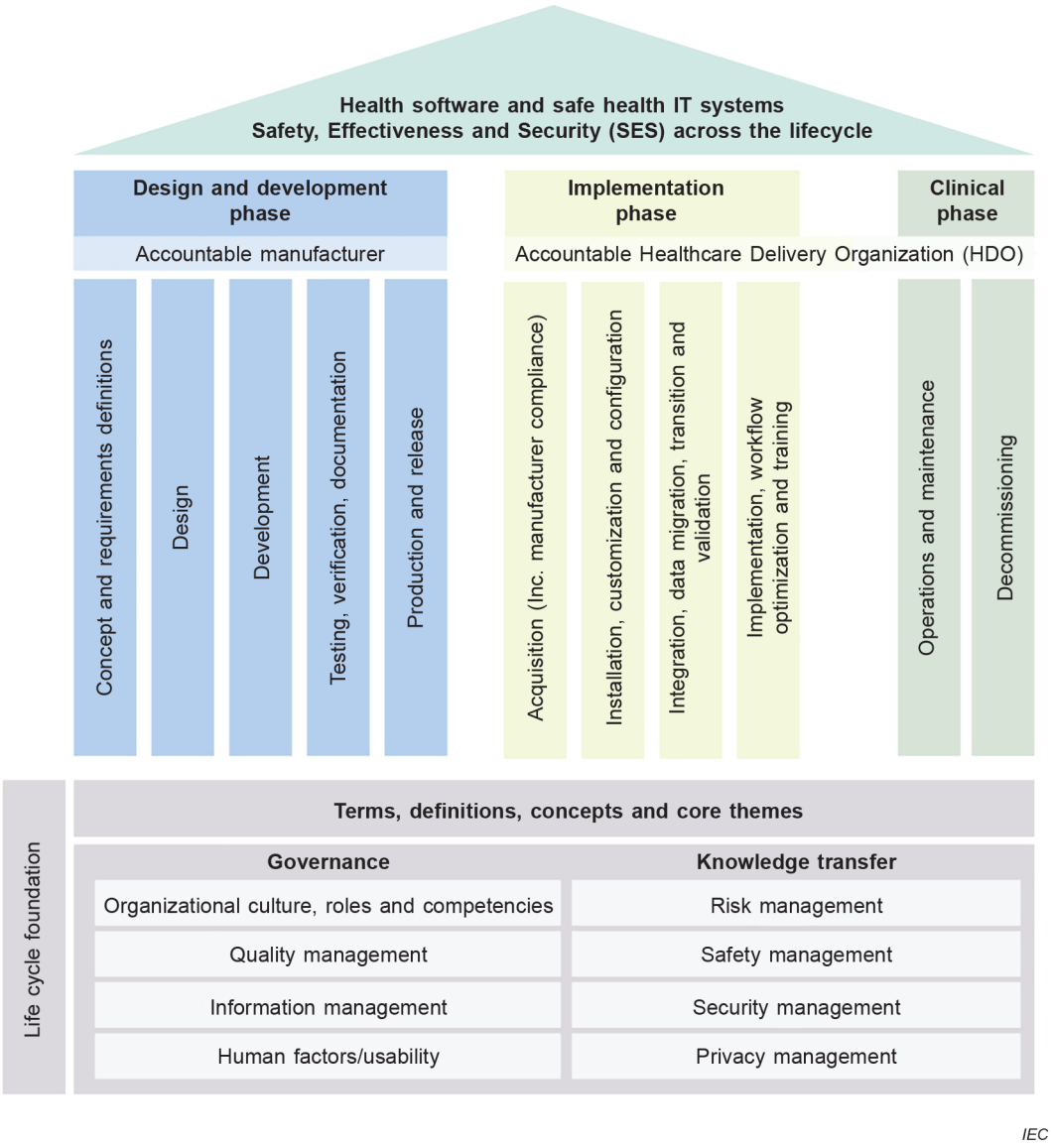

Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health software and health IT systems

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.]