BS EN IEC 80001-1:2021

BSI Standards Publication

# 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

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

# National foreword

This British Standard is the UK implementation of EN IEC 80001-1:2021. It is identical to IEC 80001-1:2021. It supersedes BS EN 80001-1:2011, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice.

A list of organizations represented on this committee can be obtained on request to its committee manager.

**Contractual and legal considerations**

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 580 98363 4

ICS 11.040.01; 35.240.80

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2021.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN IEC 80001-1

October 2021

ICS 11.040.01; 35.240.80

Supersedes EN 80001-1:2011 and all of its amendments and corrigenda (if any)

English Version

# 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 (IEC 80001-1:2021)

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)

Sicherheit, Effektivität und Daten- und Systemsicherheit bei Implementierung und Gebrauch von eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware - Teil 1: Anwendung von Risikomanagement (IEC 80001-1:2021)

This European Standard was approved by CENELEC on 2021-10-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

© 2021 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 80001-1:2021 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

# European foreword

The text of document 62A/1434/FDIS, future edition 2 of IEC 80001-1, prepared by SC 62A “Common aspects of electrical equipment used in medical practice” of IEC/TC 62 “Electrical equipment in medical practice” was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 80001-1:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2022–07–26
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2024–10–26

This document supersedes EN 80001-1:2011 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

## Endorsement notice

The text of the International Standard IEC 80001-1:2021 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

ISO 14971:2019 NOTE Harmonized as EN ISO 14971:2019 (not modified)

ISO 13940:2015 NOTE Harmonized as EN ISO 13940:2016 (not modified)

IEC 60601-1:2005 NOTE Harmonized as EN 60601-1:2006 (not modified) +A11:2011



Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

# 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.**

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

CONTENTS

FOREWORD ..... 4
INTRODUCTION ..... 7
1 Scope ..... 9
2 Normative references ..... 9
3 Terms and definitions ..... 9
4 Principles ..... 10
5 Framework ..... 11
5.1 General ..... 11
5.2 Leadership and commitment ..... 11
5.3 Integrating RISK MANAGEMENT ..... 11
5.4 Design/planning ..... 12
5.4.1 General ..... 12
5.4.2 RISK MANAGEMENT FILE ..... 13
5.4.3 Understanding the organization and the SOCIOTECHNICAL ECOSYSTEM ..... 13
5.4.4 Articulating RISK MANAGEMENT commitment ..... 13
5.4.5 Assigning organizational roles, authorities, responsibilities and accountabilities ..... 13
5.4.6 Allocating resources ..... 14
5.4.7 Establishing communication and consultation ..... 14
5.5 Implementation ..... 15
5.6 Evaluation ..... 15
5.7 Improvement ..... 15
6 RISK MANAGEMENT PROCESS ..... 15
6.1 Generic requirements ..... 15
6.1.1 General ..... 15
6.1.2 RISK ANALYSIS ..... 16
6.1.3 RISK EVALUATION ..... 18
6.1.4 RISK CONTROL ..... 19
6.2 Lifecycle specific requirements ..... 21
6.2.1 General ..... 21
6.2.2 Acquisition ..... 21
6.2.3 Installation, customization and configuration ..... 22
6.2.4 Integration, data migration, transition and validation ..... 22
6.2.5 Implementation, workflow optimization and training ..... 22
6.2.6 Operation and maintenance ..... 23
6.2.7 Decommission ..... 24
Annex A (informative) IEC 80001-1 requirements mapping table ..... 25
Annex B (informative) Guidance for accompanying document Information ..... 31
B.1 Foreword ..... 31
B.2 Information system categorization ..... 32
B.3 Overview ..... 32
B.4 Reference documents ..... 32
B.5 System level description ..... 32
B.5.1 Environment description ..... 32
B.5.2 Network ports, protocols and services ..... 33
B.5.3 Purpose of connection to the health IT infrastructure ..... 33

AVA Documents
Document Sharing Hub

B.5.4 Networking requirements ..... 33
B.5.5 Required IT-network services ..... 33
B.5.6 Data flows and protocols ..... 33
B.6 Security and user access ..... 34
B.6.1 General ..... 34
B.6.2 Malware / antivirus / allow-list ..... 34
B.6.3 Security exclusions ..... 34
B.6.4 System access ..... 34
B.7 RISK MANAGEMENT ..... 36
Bibliography ..... 37

Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health software and health IT systems ..... 8
Figure 2 – RISK MANAGEMENT PROCESS ..... 12

Table A.1 – IEC 80001-1 requirements table ..... 25
Table B.1 – Organization name and location ..... 31
Table B.2 – Cybersecurity device characterization level ..... 32
Table B.3 – Ports, protocols and services ..... 33
Table B.4 – Information system name and title ..... 34
Table B.5 – Roles and privileges ..... 35

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

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;

AVA Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

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.**

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

# 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).

Documents
Document Sharing Hub

Full document details: BS EN IEC 80001-1:2021

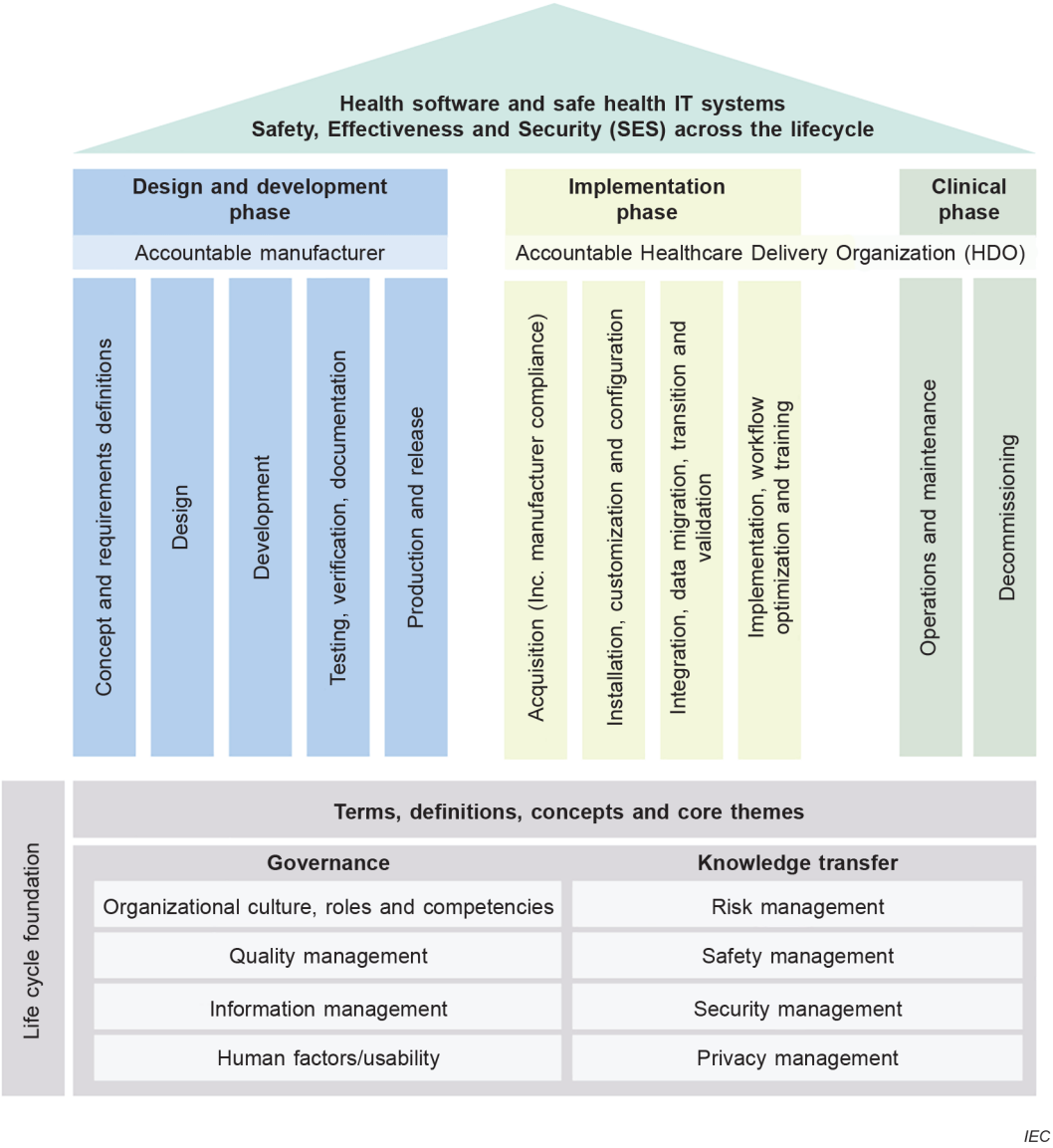


**Figure 1 – Lifecycle framework addressing safety, effectiveness and security of health software and health IT systems**

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 80001-1:2021

# 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.]

AVA Documents
Document Sharing Hub