TECHNICAL REPORT

ISO/TR 80001-2-7

First edition
2015-04-01

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

Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

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

Partie 2-7: Directives de prestation de soins de santé organisations sur la façon de s'auto-évaluer leur conformité avec la norme IEC 80001-1

Reference number
ISO/TR 80001-2-7:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/TC 215, *Heath informatics*.

ISO/IEC/TR 80001 consists of the following parts, under the general title *Application of risk management for IT-networks incorporating medical devices*:

— *Part 1: Roles, responsibilities and activities*

— *Part 2-1: Step-by-step risk management of medical IT-networks; Practical applications and Examples*

— *Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

— *Part 2-3: Guidance for wireless networks*

— *Part 2-4: General implementation guidance for Healthcare Delivery Organizations*

— *Part 2-5: Application guidance — Guidance for distributed alarm systems*

— *Part 2-6: Application guidance — Guidance for responsibility agreements*

— *Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*

The following parts are under preparation:

— *Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*

Introduction

This part of ISO/TR 80001 provides guidance for a Healthcare Delivery Organization (HDO) that wishes to self-assess its implementation of the processes of IEC 80001-1. This part of ISO/TR 80001 can be used to assess Medical IT-Network projects where IEC 80001-1 has been determined to be applicable. This part of ISO/TR 80001 provides an exemplar assessment method which includes a set of questions which can be used to assess the performance of risk management of a Medical IT-Network incorporating a medical device. This assessment method can be used in its presented form or can be tailored to meet the needs of a specific HDO. A Process Reference Model (PRM) and an example Process Assessment Model (PAM) that meet the requirements of ISO/IEC 15504-2 are included in the Appendices of this part of ISO/TR 80001. The PRM and PAM can be used to provide a standardized basis for tailoring the exemplar assessment method where required.

This part of ISO/TR 80001 can be used in a number of ways including the following.

a) The assessment method can be used to perform an assessment to determine conformance against IEC 80001-1.

b) In instances where conformance has been established, the assessment method can also be used to assess risk management processes and determine the capability level at which these processes are being performed.

c) Based on the context of the HDO being assessed, the assessment method can be tailored to address the individual HDO use, needs and concerns.

The results of the assessment will highlight any weaknesses within current risk management processes and can be used as a basis for the improvement of these processes. Where necessary, modification of the assessment method can be undertaken with reference to the PRM and PAM for IEC 80001-1 which are also included in this part of ISO/TR 80001. This approach allows for a lightweight assessment approach to which more rigour can be added if required. For example, a re-assessment may be required in instances where an initial assessment revealed weaknesses in the current risk management processes and improvements have subsequently been made which require re-assessment to assess their impact on conformance. A re-assessment may also be performed in instances where confirmation is required that process improvement measures which have been undertaken have resulted in the achievement of a higher capability level.

This part of ISO/TR 80001 provides the following:

— guidance for a HDO to self-assess implementation of the processes of IEC 80001-1;

— an exemplar assessment method which

  — includes a set of questions,

  — can be used to assess the performance of risk management of a Medical IT-Network incorporating a medical device,

  — can be used in its presented form, and

  — can be tailored on a standardised basis using the included PRM and PAM;

— a PRM that meet the requirements of ISO/IEC 15504-2;

— an example PAM that meet the requirements of ISO/IEC 15504-2.

NOTE This part of ISO/TR 80001 contains original material that is © 2013, Dundalk Institute of Technology, Ireland. Permission is granted to ISO and IEC to reproduce and circulate this material, this being without prejudice to the rights of Dundalk Institute of Technology to exploit the original text elsewhere.

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

Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

1 Scope

The purpose of this part of ISO/TR 80001 is to provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1.

The purpose of this part of ISO/TR 80001 is to

a) provide guidance to HDOs on self-assessment of their conformance against IEC 80001-1,

b) provide an exemplar assessment method which can be used by HDOs in varying contexts to assess themselves against IEC 80001-1,

c) define a PRM comprising a set of processes, described in terms of process purpose and outcomes that demonstrate coverage of the requirements of IEC 80001-1, and

d) define a PAM that meets the requirements of ISO/IEC 15504-2 and that supports the performance of an assessment by providing indicators for guidance on the interpretation of the process purposes and outcomes as defined in IEC 80001-1 (PRM) and the process attributes as defined in ISO/IEC 15504-2.

This part of ISO/TR 80001 does not introduce any requirements in addition to those expressed in IEC 80001-1.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Members of ISO and IEC maintain registers of currently valid International Standards.

IEC 80001-1:2010, *Application of Risk Management for IT-Networks incorporating Medical Devices — Part 1: Roles, responsibilities and activities*

ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

ISO/IEC 15504-2:2003, *Information technology — Process assessment — Part 2: Performing an assessment*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15504-1 and IEC 80001-1 apply.