IEC/TR 80001-2-4

Edition 1.0 2012-11

TECHNICAL REPORT

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

IEC/TR 80001-2-4

Edition 1.0 2012-11

TECHNICAL REPORT

colour inside

Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE T

ICS 11.040.01; 35.240.80

ISBN 978-2-83220-525-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-4, which is a technical report, 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.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
62A/818/DTR	62A/835/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table. In ISO, the technical report has been approved by 15 P-members out of 16 having cast a vote.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

A list of all parts of the IEC 80001 series, published under the general title *Application of risk management for IT-networks incorporating medical devices,* can be found on the IEC website.

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

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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

This technical report is a guide to help a HEALTHCARE DELIVERY ORGANIZATION (see 1.2) fulfilling its obligations as a RESPONSIBLE ORGANIZATION in the application of IEC 80001-1, in conjunction with other technical reports in this series. Specifically, this guide helps the HEALTHCARE DELIVERY ORGANIZATION assess the impact of the standard on the organization and establish a series of business as usual PROCESSES to manage RISK in the creation, maintenance and upkeep of its MEDICAL IT-NETWORKS. Whilst this document is aimed solely at HEALTHCARE DELIVERY ORGANIZATIONS, the term RESPONSIBLE ORGANIZATION is used throughout this document to ensure consistency with IEC 80001-1. In this respect the two terms are synonymous.

This technical report will be useful to those responsible for establishing an IEC 80001-1 compliant RISK MANAGEMENT framework within a RESPONSIBLE ORGANIZATION that is expecting to establish one or more MEDICAL IT-NETWORKS. In particular, the RISK MANAGEMENT framework should address the KEY PROPERTIES – SAFETY, DATA AND SYSTEM SECURITY and EFFECTIVENESS – as defined in IEC 80001-1. The purpose of the framework is to ensure that the potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, identified in IEC 80001-1, are avoided.

Defining and implementing the RISK MANAGEMENT framework and the business change that can result, will require the RESPONSIBLE ORGANIZATION to draw upon a range of skills from within the organization, managerial, clinical and technical. Where such skills are not available within the RESPONSIBLE ORGANIZATION, consideration should be given to collaboration with similar organizations or through experts in the field. It is important that the RESPONSIBLE ORGANIZATION be able to draw upon expertise with respect to appropriate standards and their corresponding technical reports.

In establishing a RISK MANAGEMENT framework, a RESPONSIBLE ORGANIZATION will need to take account of:

– the size and capabilities of the organization;

– the extent of its IT operations and the complexity of its current infrastructure and systems; and

– the cost of implementing IEC 80001-1.

It is expected that some of the above factors, for example size of IT operations and complexity of the networks, will be proportionate to the size of the organization. It is important that the framework itself does not create patient RISK by placing unnecessary demands on clinical staff, yet at the same time this workload should not introduce avoidable new RISKS when implementing a new technology.

In taking a RESPONSIBLE ORGANIZATION through the key decisions and steps required to successfully establish a RISK MANAGEMENT framework for MEDICAL IT-NETWORKS this document refers to small and large organizations. These are subjective terms, for which no precise measures are given, though:

- a small organization could be a doctor's practice with:
  - a few clinicians, or
  - with many clinicians, a consolidated IT function and a highly centralised governance structure
- a large organization could be:
  - a multi-hospital conglomerate, or
  - an organisation with distributed clinics and a mixture of in-house and outsourced clinical and IT governance.

Small organisations may also find the guidance identified under large organisation relevant.

The RISK MANAGEMENT framework developed by a RESPONSIBLE ORGANIZATION following the guidance in this technical report needs to fit into the formal management systems that are

routinely used for normal business: the business as usual PROCESSES. Such business as usual PROCESSES need to ensure RISK MANAGEMENT is part of the on-going requirement when systems are changed or new systems are deployed by:

– including the RISK MANAGEMENT PROCESSES in the existing management PROCESSES, for example the organization's Quality Management System;
– ensuring that the internal audit schedule includes the RISK MANAGEMENT PROCESSES;
– making sure RISK MANAGEMENT training is included on induction of new staff and provided to existing staff; and
– ensuring RISK MANAGEMENT is undertaken for both new work and changes to existing MEDICAL IT-NETWORKS.

Having established a RISK MANAGEMENT framework, the RESPONSIBLE ORGANIZATION will be ready to undertake a detailed RISK ASSESSMENT (see IEC/TR 80001-2-1 [1]).

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

1 Scope

1.1 Purpose

This technical report helps a RESPONSIBLE ORGANIZATION through the key decisions and steps required to establish a RISK MANAGEMENT framework, before the organization embarks on a detailed RISK ASSESSMENT of an individual instance of a MEDICAL IT-NETWORK. The steps are supported by a series of decision points to steer the RESPONSIBLE ORGANIZATION through the PROCESS of understanding the MEDICAL IT-NETWORK context and identifying any organizational changes required to execute the responsibilities of TOP MANAGEMENT as defined in Figure 1 of IEC 80001-1:2010.

1.2 HEALTHCARE DELIVERY ORGANIZATION

This technical report is addressed to all HEALTHCARE DELIVERY ORGANIZATIONS. A HEALTHCARE DELIVERY ORGANIZATION includes hospitals, doctors' offices, community care homes and clinics.

In the provision of a MEDICAL IT-NETWORK containing a MEDICAL DEVICE within a HEALTHCARE DELIVERY ORGANIZATION there can be a number of RESPONSIBLE ORGANIZATIONS. For the purpose of this document the focus is the HEALTHCARE DELIVERY ORGANIZATION and its obligations with respect to IEC 80001-1.

It is important for the HEALTHCARE DELIVERY ORGANIZATION to identify the RESPONSIBLE ORGANIZATION(S) responsible for any aspect of the network which is subject to IEC 80001-1. This allows a clear assignment of the roles and responsibilities of that standard.

1.3 Field of application

This technical report details the steps to be undertaken by the RESPONSIBLE ORGANIZATION in implementing the requirements of 3.1 to 3.3 and 4.1 to 4.6 of IEC 80001-1:2010.

NOTE It is assumed that the RESPONSIBLE ORGANIZATION will consider IEC/TR 80001-2-1 [1] for detailed advice in satisfying 4.4 of IEC 80001-1:2010.

1.4 Prerequisites

The International Standard IEC 80001-1:2010 is prerequisite to this technical report. The guidance in this technical report is intended to help a RESPONSIBLE ORGANIZATION establish a RISK MANAGEMENT framework to satisfy the underlying requirements of IEC 80001-1, ensuring:

– RISK MANAGEMENT policy and PROCESSES are in place;

– probability, severity, and RISK acceptability scales are specified; and

– MEDICAL IT-NETWORKS are well defined.

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.

IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities.*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

3.1
ACCOMPANYING DOCUMENT
a document accompanying a MEDICAL DEVICE or an accessory and containing information for the RESPONSIBLE ORGANIZATION or OPERATOR, particularly regarding SAFETY

Note 1 to entry: Adapted from IEC 60601-1:2005, definition 3.4.

[SOURCE: IEC 80001-1:2010, 2.1]

3.2
CHANGE-RELEASE MANAGEMENT
PROCESS that ensures that all changes to the IT-NETWORK are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with CONFIGURATION MANAGEMENT

Note 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclauses 9.2 (change management) and 10.1 (release management).

[SOURCE: IEC 80001-1:2010, 2.2]

3.3
CONFIGURATION MANAGEMENT
a PROCESS that ensures that configuration information of components and the IT-NETWORK are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the IT-NETWORK

Note 1 to entry: Adapted from ISO/IEC 20000-1:2005, Subclause 9.1.

[SOURCE: IEC 80001-1:2010, 2.4]

3.4
DATA AND SYSTEMS SECURITY
an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

Note 1 to entry: Security, when mentioned in this technical report, should be taken to include DATA AND SYSTEMS SECURITY.

Note 2 to entry: DATA AND SYSTEMS SECURITY is assured through a framework of policy, guidance, infrastructure, and services designed to protect information assets and the systems that acquire, transmit, store, and use information in pursuit of the organization's mission.

[SOURCE: IEC 80001-1:2010, 2.5]