SEK Teknisk rapport 80001-2-4

Utgiven	Utgåva	Sida	Ansvarig kommitté
2014-02-19	1	1 (1+21)	SEK TK 62

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

(IEC Technical Report 80001-2-4:2012)

Denna publikation ingår i en serie med tekniska rapporter som ansluter till standarden SS-EN 80001-1, Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter – Del 1: Roller, ansvar och aktiviteter. Den är avsedd att ge vårdgivare vägledning beträffande grunderna för riskhantering för ett medicintekniskt IT-nätverk.

För närvarande finns fyra tekniska rapporter i serien. De är:

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

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

Part 2-3: Guidance for wireless networks

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

ISSN 1651-1417

ICS 11.040.01; 35.240.80

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

CONTENTS

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.*