Riskijuhtimise rakendamine meditsiiniseadmeid sisaldavates IT-võrkudes. Osa 1: Rollid, vastutus ja tegevused

Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities



EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 80001-1:2011 sisaldab Euroopa standardi EN 80001-1:2011	This Estonian standard EVS-EN 80001-1:2011 consists of the English text of the European					
ingliskeelset teksti.	standard EN 80001-1:2011.					
Standard on kinnitatud Eesti Standardikeskuse 31.03.2011 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 31.03.2011 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.					
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuopäev on 18.03.2011.	Date of Availability of the European standard text 18.03.2011.					
Standard on kättesaadav Eesti	The standard is available from Estonian					
ICS 11.040.01, 35.240.80						

Standardite reprodutseerimis- ja levitamisõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega: Aru 10 Tallinn 10317 Eesti; <u>www.evs.ee</u>; Telefon: 605 5050; E-post: <u>info@evs.ee</u>

Right to reproduce and distribute belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation: Aru str 10 Tallinn 10317 Estonia; <u>www.evs.ee</u>; Phone: 605 5050; E-mail: <u>info@evs.ee</u>

EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM

EN 80001-1

March 2011

ICS 11.040.01; 35.240.80

English version



© 2011 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Foreword

The text of document 62A/703/FDIS, future edition 1 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 was approved by CENELEC as EN 80001-1 on 2011-02-01.

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

The following dates were fixed:

-	latest date by which the EN has to be implemented at national level by publication of an identical national standard of by endorsement	(dop)	2011-11-01
-	latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2014-02-01

Terms defined in Clause 2 of this standard are printed in SMALL CAPITALS.

For the purposes of this standard:

- "shall" means that compliance with requirement is mandatory for compliance with this standard;
- "should" means that compliance with a requirement is recommended but is not mandatory for compliance with this standard;
- "may" is used to describe a permissible way achieve compliance with a requirement; and
- "establish" means to define, document, and implement.



The text of the International Standard IEC 80001-1:2010 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:

[1] IEC 60601-1:2005	NOTE	Harmonized as EN 60601-1:2006 (not movined)
[2] IEC 61907:2009	NOTE	Harmonized as EN 61907:2010 (not modified.
[3] IEC 62304:2006	NOTE	Harmonized as EN 62304:2006 (not modified).
[4] ISO 14971:2007	NOTE	Harmonized as EN ISO 14971:2009 (not modified).
[7] ISO 16484-2:2004	NOTE	Harmonized as EN ISO 16484-2:2004 (not modified).
[8] ISO 9000:2005	NOTE	Harmonized as EN ISO 9000:2005 (not modified).

CONTENTS

INTRODUCTION 6 1 Scope 9 2 Terms and definitions 9 3 Roles and responsibilities 14 3.1 General 14 3.2 RESPONSIBLE ORGANIZATION 14 3.3 TOP MARGEMENT responsibilities 15 3.4 MEDICALT NETWORK RISK MANAGER 16 3.5 MEDICAL DETERMORK RISK MANAGER 16 3.6 Providers of other information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANCOTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PLOCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 4.3.4 RISK relevant asset descoption 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RISK KONTROL 21 4.3.5 RI	FO	REWC	RD		4
1 Scope 9 2 Terms and definitions 9 3 Roles and responsibilities 14 3.1 General 14 3.2 RESPONENCE ORGANIZATION 14 3.3 TOP MAR CEMENT responsibilities 15 3.4 MEDICAL DEWER MANAGER 16 3.5 MEDICAL DEWER MANAGER 16 3.6 Providers of the information technology 17 3.6 Providers of the information technology 18 4 Life cycle RISK MANAGEMENT IN MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.1 Overview 19 4.1 Overview 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 4.3.2 RISK-relevant asset dependion 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RESPONSIBILI	INTRODUCTION		6		
2 Terms and definitions 9 3 Roles and responsibilities 14 3.1 General 14 3.2 RESPONSIBLE ORGANIZATION 14 3.3 Commended Market 15 3.4 MEDICAL PHONE MENT RESPONSIBILITIES 15 3.4 MEDICAL DEVICE manufacturer(s) 17 3.6 Providers of other information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT PROCESS 21 4.3.6 RISK MANAGEMENT 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 <td>1</td> <td>Scop</td> <td>e</td> <td></td> <td>9</td>	1	Scop	e		9
3 Roles and responsibilities 14 3.1 General 14 3.2 RESPONSIBLE ORGANIZATION 14 3.3 TOP MAY GEMENT responsibilities 15 3.4 MEDICAL DEVE emanufacturer(s) 17 3.6 Providers of other information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANECTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3.1 Overview 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset desemption 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 21 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.3.4 RESPONSIBILITY AGREEMENT 24 4.3.5 RISK MANAGEMENT <td>2</td> <td>Term</td> <td>s and d</td> <td>efinitions</td> <td>9</td>	2	Term	s and d	efinitions	9
3.1 General 14 3.2 RESPONSIBLE ORGANIZATION 14 3.3 TOP MARGEMENT responsibilities 15 3.4 MEDICAL DAVE MENT RESK MANAGER 16 3.5 MEDICAL DAVE manufacturer(s) 17 3.6 Providers of oper information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANENTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.1 4.3.3 MEDICAL IT-NETWORK documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the opicAL IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.3.5 RISK MANAGEMENT 22 4.3.6 RISK MANAGEMENT	3	Roles	and re	sponsibilities	14
3.1 Generative 14 3.2 RESPONSIBLE ORGANIZATION 14 3.3 TOP MARGEMENT RESPONSIBILITIES 15 3.4 MEDICAL DRAFE menufacturer(s) 17 3.5 MEDICAL DRAFE menufacturer(s) 17 3.6 Providers of other information technology 18 4 Life cycle RISK MANACEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.2 RESPONSIBLE ORGAN CATION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3.1 Overview 21 4.3.1 Overview 21 4.3.2 RISK-Relevant asset description 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RESPONSIBILITY A GREEMENT 22 4.3.5 RISK MANAGEMENT plan for the opicAL IT-NETWORK 22 4.3.4 RESPONSIBILITY A GREEMENT 24 4.4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RISK EVALUATION 22 <	Ũ	3 1	Genera		11
3.3 TOP MADE EMENT responsibilities 15 3.4 MEDICAL DEVICE MANAGER 16 3.5 MEDICAL DEVICE manufacturer(s) 17 3.6 Providers of oper information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.1 Overview 19 4.2 RESPONSIBLE ORGAN MOTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS. 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 4.3.3 MEDICAL IT-NETWORK AGEMENT planning and documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the COICAL IT-NETWORK 24 4.4 NEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK EVALUATION 25 4.4.4 RISK EVALUATION 25 4.4.5 RISK EVALUATI		3.2	RESPO		1 4 14
3.4 MEDICAL INSTRUCTION CONTINUES 16 3.5 MEDICAL DEVER MANAGEMENT (S) 17 3.6 Providers of their information technology 18 4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS. 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS. 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 4.3.3 MEDICAL IT-NETWORK GOCARGEMENT planning and documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the MOICAL IT-NETWORK 24 4.4 A.1 Overview 24 4.4.1 Overview 24 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK ANALYSIS 24 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5.1 CHANGE-RELEASE MANAGEMENT ANG CONFIGURATION MARAG		3.3		A CEMENT RESPONSIBILITIES	14
3.5 MEDICAL DIVE E manufacturer(s) 17 3.6 Providers of other information technology 18 4 Life cycle RISK MANACPUENT IN MEDICAL IT-NETWORKS. 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the motical IT-NETWORK 24 4.4 Nebical IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK CONTROL 25 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT PROCES		3.4			10
3.6 Providers of other information technology. 18 4 Life cycle RISK MANAGEMENT IN MEDICAL IT-NETWORKS. 19 4.1 Overview 19 4.2 RESPONSIBLE ORGAN OTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISC MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS. 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK ROK doct for intation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the report. 22 4.3.4 RESPONSIBILITY AGREEMENT 24 4.4.1 Overview 24 4.4.2 RISK MANAGEMENT plan for the report. 25 4.4.4 RISK CONTROL 25 4.5 RESIDUAL RISK VALUATION 25 4.4.4 RISK CONTROL 25 4.5 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS		3.5	MEDICA	AL DECE manufacturer(s).	
4 Life cycle RISK MANASCHENT IN MEDICAL IT-NETWORKS 19 4.1 Overview 19 4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset desorption 22 4.3.3 MEDICAL IT-NETWORK documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT Plan for the molical IT-NETWORK 24 4.4.1 Overview 24 4.4.2 RISK MANAGEMENT 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK EVALUATION 25 4.5.1 CHANGE-RELEASE MANAGEMENT AND CONFIGURATION MARCEMENT 27 4.5.2 DECICAL		3.6	Provide	ers of other information technology	
4.1 Overview 19 4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK RISK MANAGEMENT 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the MOICAL IT-NETWORK 24 4.4 RISK MANAGEMENT plan for the MOICAL IT-NETWORK 24 4.4.1 Overview 24 4.4.2 RISK MANAGEMENT 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT ANAGEMENT 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 <td>4</td> <td>Life c</td> <td>ycle RIS</td> <td>SK MANAGEMENT IN MEDICAL IT-NETWORKS</td> <td> 19</td>	4	Life c	ycle RIS	SK MANAGEMENT IN MEDICAL IT-NETWORKS	19
4.2 RESPONSIBLE ORGAN ATTION RISK MANAGEMENT 20 4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the molecular IT-NETWORK 24 4.4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.4 NEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.4 NEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-		4 1	Overvi	ew	19
4.2.1 POLICY FOR RISCHANAGEMENT for incorporating MEDICAL DEVICES 20 4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the ADDICAL IT-NETWORK 24 4.4.4 RISK EVALUATION 25 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK EVALUATION 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 RESIDUAL RISK evaluation and reporting 26 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29		4.2	RESPO	NSIBLE ORGAN	
4.2.2 RISK MANAGEMENT PROCESS 21 4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK documentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the indical IT-NETWORK 24 4.4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT AND CONFIGURATION MARGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5			4.2.1	POLICY FOR RISKMANAGEMENT for incorporating MEDICAL DEVICES	20
4.3 MEDICAL IT-NETWORK RISK MNAGEMENT planning and documentation 21 4.3.1 Overview 21 4.3.2 RISK-relevant asset deservation 22 4.3.3 MEDICAL IT-NETWORK doctmentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the topical IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 29 4.6 Live network RISK MANAGEMENT 29 4.6.2 EVENT MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1			4.2.2	RISK MANAGEMENT PROCESS	21
4.3.1 Overview 21 4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK doctmentation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the applicat IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MAY CEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGE		4.3	MEDICA	AL IT-NETWORK RISK MANAGEMENT planning and documentation	21
4.3.2 RISK-relevant asset description 22 4.3.3 MEDICAL IT-NETWORK docting nation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the redical IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.6.1 Monitoring 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Overview of RISK MANAGEMENT relationships 35 Annex A (informative) Overv			4.3.1	Overview	21
4.3.3 MEDICAL IT-NETWORK docting natation 22 4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the indical IT-network 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MAGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 27 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEM			4.3.2	RISK-relevant asset description	22
4.3.4 RESPONSIBILITY AGREEMENT 22 4.3.5 RISK MANAGEMENT plan for the indical IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 27 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on fiel			4.3.3	MEDICAL IT-NETWORK documentation	22
4.3.5 RISK MANAGEMENT plan for the indical IT-NETWORK 24 4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARAGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 27 4.6.2 EVENT MANAGEMENT 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.3.4	RESPONSIBILITY AGREEMENT	22
4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 24 4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.3.5	RISK MANAGEMENT plan for the notical IT-NETWORK	24
4.4.1 Overview 24 4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MAY GEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36		4.4	MEDICA	AL IT-NETWORK RISK MANAGEMENT	24
4.4.2 RISK ANALYSIS 24 4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MAY GEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.4.1	Overview	24
4.4.3 RISK EVALUATION 25 4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MAD GEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.4.2	RISK ANALYSIS	24
4.4.4 RISK CONTROL 25 4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARK GEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.4.3	RISK EVALUATION	25
4.4.5 RESIDUAL RISK evaluation and reporting 26 4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.4.4	RISK CONTROL	25
4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MARAGEMENT 27 4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 27 4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.4.5	RESIDUAL RISK evaluation and reporting	26
4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS. 27 4.5.2 Decision on how to apply RISK MANAGEMENT. 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT. 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure. 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale. 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36		4.5	CHANG	E-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT	27
4.5.2 Decision on how to apply RISK MANAGEMENT 27 4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.5.1	CHANGE-RELEASE MANAGEMENT PROCESS	27
4.5.3 Go-live 29 4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.5.2	Decision on how to apply RISK MANAGEMENT	27
4.6 Live network RISK MANAGEMENT 29 4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.5.3	Go-live	29
4.6.1 Monitoring 29 4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36		4.6	Live ne	etwork RISK MANAGEMENT	29
4.6.2 EVENT MANAGEMENT 29 5 Document control 30 5.1 Document control procedure 30 5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36			4.6.1	Monitoring	29
5 Document control 30 5.1 Document control procedure	_	_	4.6.2	EVENT MANAGEMENT	29
5.1 Document control procedure	5	Document control		30	
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 30 Annex A (informative) Rationale 31 Annex B (informative) Overview of RISK MANAGEMENT relationships 35 Annex C (informative) Guidance on field of application 36		5.1	Docum	ent control procedure	30
Annex A (informative) Rationale		5.2	MEDICA	AL IT-NETWORK RISK MANAGEMENT FILE	30
Annex B (informative) Overview of RISK MANAGEMENT relationships	Anr	iex A	(informa	ative) Rationale	31
Annex C (informative) Guidance on field of application	Anr	nex B	(informa	ative) Overview of RISK MANAGEMENT relationships	35
	Anr	nex C	(informa	ative) Guidance on field of application	36
Annex D (informative) Relationship with ISO/IEC 20000-2:2005 Information technology	Anr	nex D Service	(informa	ative) Relationship with ISO/IEC 20000-2:2005 Information technology	38
Bibliography 42	Bih	lioora	hv		

Figure 1 – Illustration of TOP MANAGEMENT responsibilities	16
Figure 2 – Overview of life cycle of MEDICAL IT-NETWORKS including RISK MANAGEMENT	20
Figure B.1 – Overview of roles and relationships	35
Figure D.1 – Service management processes	39

Table A.1 – Relationship between ISO 14971 and IEC 80001-1	33
Table C.1 – IT-NETWORK scenarios that can be encountered in a clinical environment	36
Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or	
ISO/IEC 20000-22005	40

ic FTWC ACOUNTING AT IS A DROWIG WORK OF A DROWIG WORK ACOUNTING AT IS A DROWIG WORK OF A DROWIG WORK ACOUNTING A DROWIG WORK OF A DROWIG WORK OF A DROWIG WORK ACOUNTING A DROWIG WORK OF A D

INTRODUCTION

An increasing number of MEDICAL DEVICEs are designed to exchange information electronically with other equipment in the user environment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature.

At the same time, IT-NETWORKS are becoming increasingly vital to the clinical environment and are now required to carry increasingly diverse traffic, ranging from life-critical patient data requiring immediate delivery and response, to general corporate operations data and to email containing potential malicious content (e.g. viruses).

For many jurisdictions, design and production of MEDICAL DEVICES is subject to regulation, and to standards recognized by the regulators. Traditionally, regulators direct their attention to MEDICAL DEVICE manufacturers, by requiring design features and by requiring a documented PROCESS for design and manufacturing. MEDICAL DEVICES cannot be placed on the market in these jurisdictions without evidence that those requirements have been met.

The use of the MEDICAL DEVICES by clinical staff is also subject to regulation. Members of clinical staff have to be appropriately trained and qualified, and are increasingly subject to defined PROCESSES designed to protect patients from unacceptable RISK.

In contrast, the incorporation of MEDVAL DEVICES into IT-NETWORKS in the clinical environment is a less regulated area. IEC 60601- 3005 [1]¹) requires MEDICAL DEVICE manufacturers to include some information in ACCOMPANYING DOCUMENTS if the MEDICAL DEVICE is intended to be connected to an IT-NETWORK. Standards are also in place covering common information technology activities including planning, Gesign and maintenance of IT-NETWORKS, for instance ISO 20000-1:2005 [9]. However, until the publication of this standard, no standard addressed how MEDICAL DEVICES can be connected to IT-NETWORKS, including general-purpose IT-NETWORKS, to achieve INTEROPERABILITY without compromising the organization and delivery of health care in terms of SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY.

There remain a number of potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, including:

- lack of consideration for RISK from use of IT-NETWORKS dating evaluation of clinical RISK;
- lack of support from manufacturers of MEDICAL DEVICE for the incorporation of their products into IT-NETWORKS, (e.g. the unavailability or inaded acy of information provided by the manufacturer to the OPERATOR of the IT-NETWORK);
- incorrect operation or degraded performance (e.g. incompatibility or improper configuration) resulting from combining MEDICAL DEVICES and other equipment on the same IT-NETWORK;
- incorrect operation resulting from combining MEDICAL DEVICE SOFTWARE and other software applications (e.g. open email systems or computer games) in the same II-NETWORK;
- lack of security controls on many MEDICAL DEVICES; and
- the conflict between the need for strict change control of MEDICAL DEVICES and the need for rapid response to the threat of cyberattack.

When these problems manifest themselves, unintended consequences frequently follow.

This standard is addressed to RESPONSIBLE ORGANIZATIONS, to manufacturers of MEDICAL DEVICES, and to providers of other information technology.

¹⁾ Numbers in square brackets refer to the Bibliography.

This standard adopts the following principles as a basis for its normative and informative sections:

- The incorporation or removal of a MEDICAL DEVICE or other components in an IT-NETWORK is a task which requires design of the action; this might be out of the control of the manufacturer of the MEDICAL DEVICE.
- RISK MANAGEMENT should be used before the incorporation of a MEDICAL DEVICE into an IT-NETWORK takes place, and for any changes during the entire life cycle of the resulting MEDICAL IT-NETWORK, to avoid unacceptable RISKS, including possible RISK to patients, resulting from the incorporation of the MEDICAL DEVICE into the IT-NETWORK. Many things are part of RISK decision, such as liability, cost, or impact on mission. These should be considered in determining acceptable RISK in addition to the requirements described in this standard.
- Aspects of removal, maintenance, change or modification of equipment, items or components should be addressed adequately in addition to the incorporation of MEDICAL DEVICES.
- The manufacturer of the MEDICAL DEVICE is responsible for RISK MANAGEMENT of the MEDICAL DEVICE during the design, implementation, and manufacturing of the MEDICAL DEVICE. This standard does not cover the RISK MANAGEMENT PROCESS for the MEDICAL DEVICE.
- The manufacturer of a MEDICAE DEVICE intended to be incorporated into an IT-NETWORK might need to provide information about the MEDICAL DEVICE that is necessary to allow the RESPONSIBLE ORGANIZATION to manage RISK according to this standard. This information can include, as part of the ACCOMPANYING DOCUMENTS, instructions specifically addressed to the person who incorporates a MEDICAL DEVICE into an IT-NETWORK.
- Such ACCOMPANYING DOCUMENTS should convey instructions about how to incorporate the MEDICAL DEVICE into the IT-NETWORK, how the MEDICAL DEVICE transfers information over the IT-NETWORK, and the minimum IT-NETWORK characteristics necessary to enable the INTENDED USE of the MEDICAL DEVICE when to is incorporated into the IT-NETWORK. The ACCOMPANYING DOCUMENTS should warn of possible hazardous situations associated with failure or disruptions of the IT-NETWORK, and the misuse of the IT-NETWORK connection or of the information that is transferred over the IT-NETWORK.
- RESPONSIBILITY AGREEMENTS can establish roles and responsibilities among those engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK, all aspects of the life cycle of the resulting MEDICAL IT-NETWORK and all activities that form part of that life cycle.
- The RESPONSIBLE ORGANIZATION is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of these roles. The most important of those roles is the MEDICAL IT-NETWORK RISK MANAGER. This role can be assigned to someone within the RESPONSIBLE ORGANIZATION or to an external contractor.
- The MEDICAL IT-NETWORK RISK MANAGER is responsible for ensuring that RISK MANAGEMENT is included during the PROCESSES of:
 - planning and design of new incorporations of MEDICAL DEVICES of changes to such incorporations;
 - putting the MEDICAL IT-NETWORK into use and the consequent use of the MEDICAL IT-NETWORK; and
 - CHANGE-RELEASE MANAGEMENT and change management of the IT-NETWORK during the IT-NETWORK's entire life cycle.
- RISK MANAGEMENT should be applied to address the following KEY PROPERTIES appropriate for the IT-NETWORK incorporating a MEDICAL DEVICE:
 - SAFETY (freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment);
- EFFECTIVENESS (ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION); and

• DATA AND SYSTEM 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).

this document is a preview denerated by EUS

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

Part 1: Roles, responsibilities and activities

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and the standard is described in Annex A.

This standard applies after a mEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-marker RISK MANAGEMENT.

n,

This standard applies throughout the life we of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 2000-2 and this standard is described in Annex D.

This standard applies where there is no single MEDICAL DEVICE manufacturer assuming responsibility for addressing the KEY PROPERTIES of the IT-NETWORK incorporating a MEDICAL DEVICE.

NOTE 4 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, the installation or assembly of the MEDICAL DEVICE according to the manufacturer's ACCORDANYING DOCUMENTS is not subject to the provisions of this standard regardless of who installs or assembles the MEDICAL DEVICE.

NOTE 5 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, additions to that MEDICAL DEVICE or modification of the configuration of that MEDICAL DEVICE other than as specified by the manufacturer, is subject to the provisions of this standard.

This standard applies to RESPONSIBLE ORGANIZATIONS, MEDICAL DEVCE manufacturers and providers of other information technology for the purpose of RISK MANAGEMENT of an IT-NETWORK incorporating MEDICAL DEVICES as specified by the RESPONSIBLE ORGANIZATION.

This standard does not apply to personal use applications where the patient person and RESPONSIBLE ORGANIZATION are one and the same person.

NOTE 6 In cases where a MEDICAL DEVICE is used at home under the supervision or instruction of the provider, that provider is deemed to be the RESPONSIBLE ORGANIZATION. Personal use where the patient acquires and uses a MEDICAL DEVICE without the supervision or instruction of a provider is out of scope of this standard.

This standard does not address regulatory or legal requirements.

2 Terms and definitions

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