

IEC 80001-1:2010-10 (E/F)

Application of risk management for IT-networks incorporating medical devices_ Part_1: Roles, responsibilities and activities

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux_ - Partie_1: Fonctions, responsabilités et activités

CONTENTS

FOREWORD.....	4
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 MANAGEMENT responsibilities.....	15
3.4 MEDICAL IT-NETWORK RISK MANAGER	16
3.5 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 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 MEDICAL 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 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
Annex D (informative) Relationship with ISO/IEC 20000-2:2005 <i>Information technology</i> – <i>Service management</i> – <i>Part 2: Code of practice</i>	38
Bibliography.....	42

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 20000-2:2005	40

SOMMAIRE

AVANT-PROPOS.....	46
INTRODUCTION.....	48
1 Domaine d'application	51
2 Termes et définitions	52
3 Fonctions et responsabilités	56
3.1 Généralités.....	56
3.2 ORGANISME RESPONSABLE.....	57
3.3 Responsabilités de la DIRECTION.....	57
3.4 GESTIONNAIRE DES RISQUES DU RÉSEAU TI MÉDICAL.....	59
3.5 Fabricant(s) de DISPOSITIFS MÉDICAUX.....	60
3.6 Fournisseurs d'autres équipements de technologies de l'information.....	61
4 GESTION DES RISQUES du cycle de vie des RÉSEAUX TI MÉDICAUX.....	62
4.1 Vue d'ensemble.....	62
4.2 GESTION DES RISQUES DE L'ORGANISME RESPONSABLE.....	63
4.2.1 POLITIQUE DE GESTION DES RISQUES pour l'incorporation des DISPOSITIFS MÉDICAUX.....	63
4.2.2 PROCESSUS DE GESTION DES RISQUES	64
4.3 Planification et documentation de la GESTION DES RISQUES DU RÉSEAU TI MÉDICAL	64
4.3.1 Vue d'ensemble.....	64
4.3.2 Description des avantages liés aux RISQUES	65
4.3.3 Documentation relative au RÉSEAU TI MÉDICAL.....	65
4.3.4 ACCORD DE RESPONSABILITÉ	66
4.3.5 Plan de GESTION DES RISQUES pour le RÉSEAU TI MÉDICAL	67
4.4 GESTION DES RISQUES DU RÉSEAU TI MÉDICAL	67
4.4.1 Vue d'ensemble.....	67
4.4.2 ANALYSE DU RISQUE.....	68
4.4.3 ÉVALUATION DU RISQUE.....	68
4.4.4 MAÎTRISE DU RISQUE.....	68
4.4.5 Evaluation et compte-rendu du RISQUE RÉSIDUEL	70
4.5 GESTION DU DÉCLENCHEMENT DES MODIFICATIONS et GESTION DE LA CONFIGURATION	71
4.5.1 PROCESSUS DE GESTION DU DÉCLENCHEMENT DES MODIFICATIONS.....	71
4.5.2 Décision relative à l'application de la GESTION DES RISQUES.....	71
4.5.3 Mise en service	73
4.6 GESTION DES RISQUES du réseau en service	73
4.6.1 Surveillance.....	73
4.6.2 Gestion des événements	74
5 Contrôle des documents.....	74
5.1 Procédure de contrôle des documents.....	74
5.2 DOSSIER DE GESTION DES RISQUES DU RÉSEAU TI MÉDICAL	74
Annexe A (informative) Justifications	75
Annexe B (informative) Vue d'ensemble des relations entre les intervenants dans la GESTION DES RISQUES.....	79
Annexe C (informative) Directive relative au champ d'application	80
Annexe D (informative) Relation avec l'ISO/CEI 20000-2:2005, <i>Technologies de l'information – Gestion des services – Partie 2: Code de pratique</i>	82

Bibliographie.....	86
Figure 1 – Illustration des responsabilités de la direction	59
Figure 2 – Vue d’ensemble du cycle de vie des RÉSEAUX TI MÉDICAUX y compris la gestion des risques.....	63
Figure B.1 – Vue d’ensemble des fonctions et des relations.....	79
Figure D.1 – Processus de gestion des services	83
Tableau A.1 – Relations entre l’ISO 14971 et la CEI 80001-1	77
Tableau C.1 – Scénarios de réseaux TI pouvant être rencontrés dans un environnement clinique	80
Tableau D.1 – Relations entre la CEI 80001-1 et l’ISO/CEI 20000-1:2005 ou l’ISO/CEI 20000-2:2005	84