

Medizintechnik und Informationstechnologie im Krankenhaus

Dr. Andreas Zimolong

DIN EN 80001-1:2011

Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten

Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten

➤ Netzwerke mit Medizinprodukten

- Medizinprodukte nach MPG § 3 Nr. 1
- Zubehör nach MPG §2 Abs. 1 und § 3 Nr. 9
- Für die Vernetzung notwendige Systeme und Komponenten

➤ Gültig für den gesamten Lebenszyklus von Netzwerken mit Medizinprodukten:

- Projektierung und Planung
- Implementierung
- Betrieb und Fehlermanagement
- Änderungen

- 2 -

80001-1 © IEC:2010

CONTENTS	
INTRODUCTION	
1 Scope	4
2 Terms and definitions	6
3 Roles and responsibilities	9
3.1 General	9
3.2 RESPONSIBLE ORGANIZATION	9
3.3 TOP MANAGEMENT responsibilities	14
3.4 MEDICAL IT-NETWORK RISK MANAGER	14
3.5 MEDICAL DEVICE manufacturer(s)	14
3.6 Providers of other information technology	15
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS	17
4.1 Overview	17
4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT	18
4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES	19
4.2.2 RISK MANAGEMENT PROCESS	19
4.3 MEDICAL IT-NETWORK RISK MANAGEMENT	20
4.3.1 Overview	20
4.3.2 RISK-relevant asset description	21
4.3.3 MEDICAL IT-NETWORK documentation	21
4.3.4 RESPONSIBILITY AGREEMENT	21
4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK	21
4.4 MEDICAL IT-NETWORK RISK MANAGEMENT	22
4.4.1 Overview	22
4.4.2 RISK ANALYSIS	22
4.4.3 RISK EVALUATION	24
4.4.4 RISK CONTROL	24
4.4.5 RESIDUAL RISK evaluation and reporting	24
4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT	25
4.5.1 CHANGE-RELEASE MANAGEMENT	25
4.5.2 Decision on how to apply RISK MANAGEMENT	25
4.5.3 Go-live	28
4.6 Live network RISK MANAGEMENT	27
4.6.1 Monitoring	27
4.6.2 EVENT MANAGEMENT	27
5 Document control	29
5.1 Document control procedure	29
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE	29
Annex A (informative) Rationale	29
Annex B (informative) Overview of RISK MANAGEMENT relationships	30
Annex C (informative) Guidance on field of application	30
Annex D (informative) Relationship with ISO/IEC 20000-2:2005 information technology - Service management - Part 2: Code of practice	31
Bibliography	35

Kap. 4: Lebenszyklus-Risikomanagement für medizinische IT Netzwerke



4.1 Übersicht

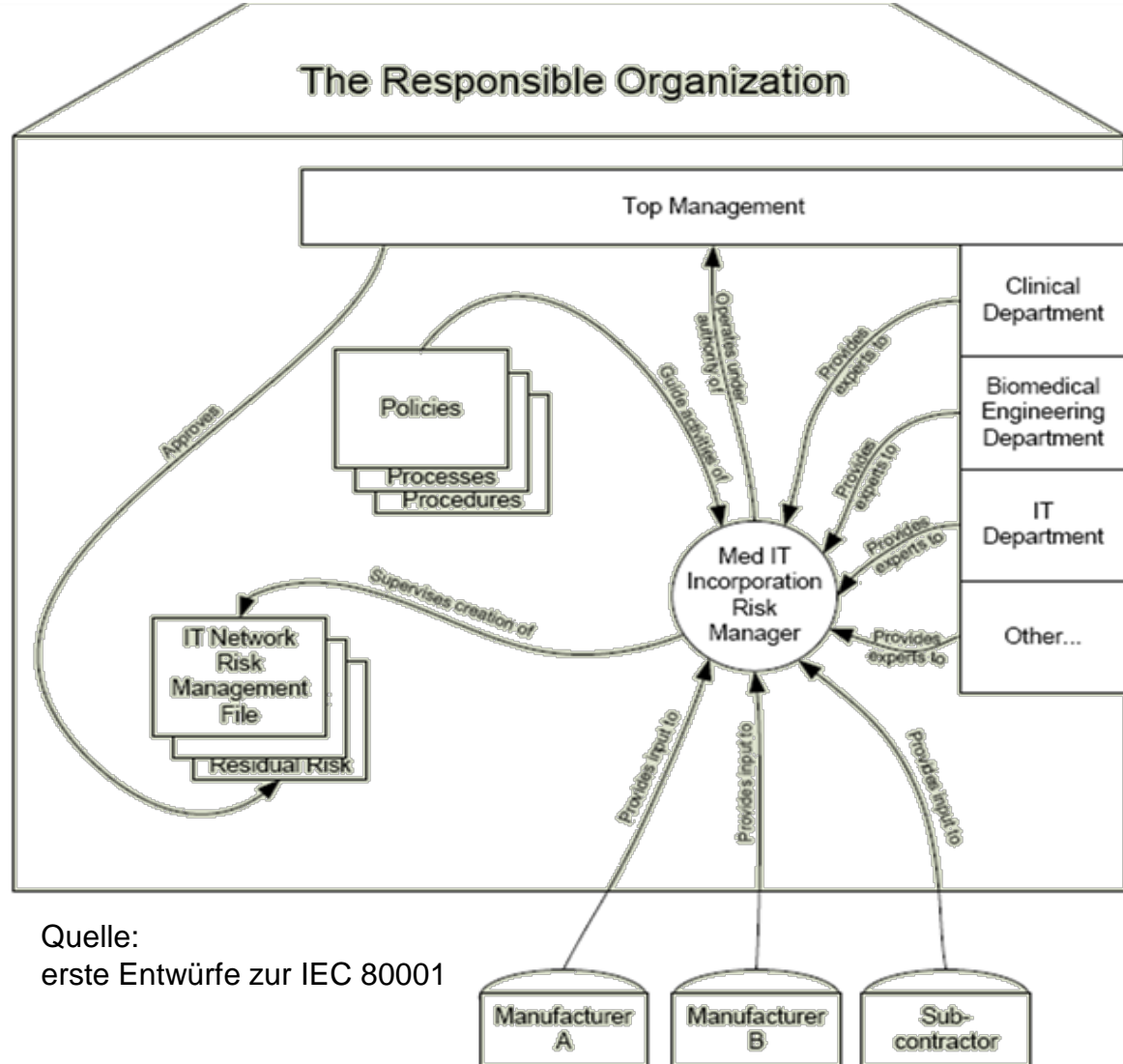
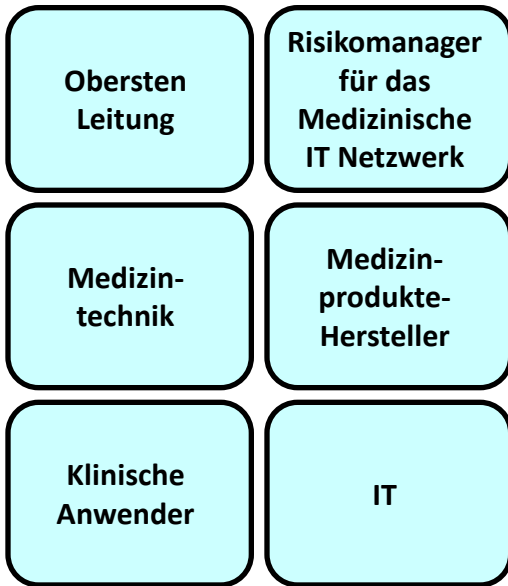
4.2 Risikomanagement der verantwortlichen Organisation

4.3 Planung und Dokumentation des Risikomanagements für medizinische IT Netzwerke

4.5 Management der Änderungsfreigabe und Konfigurationsmanagement

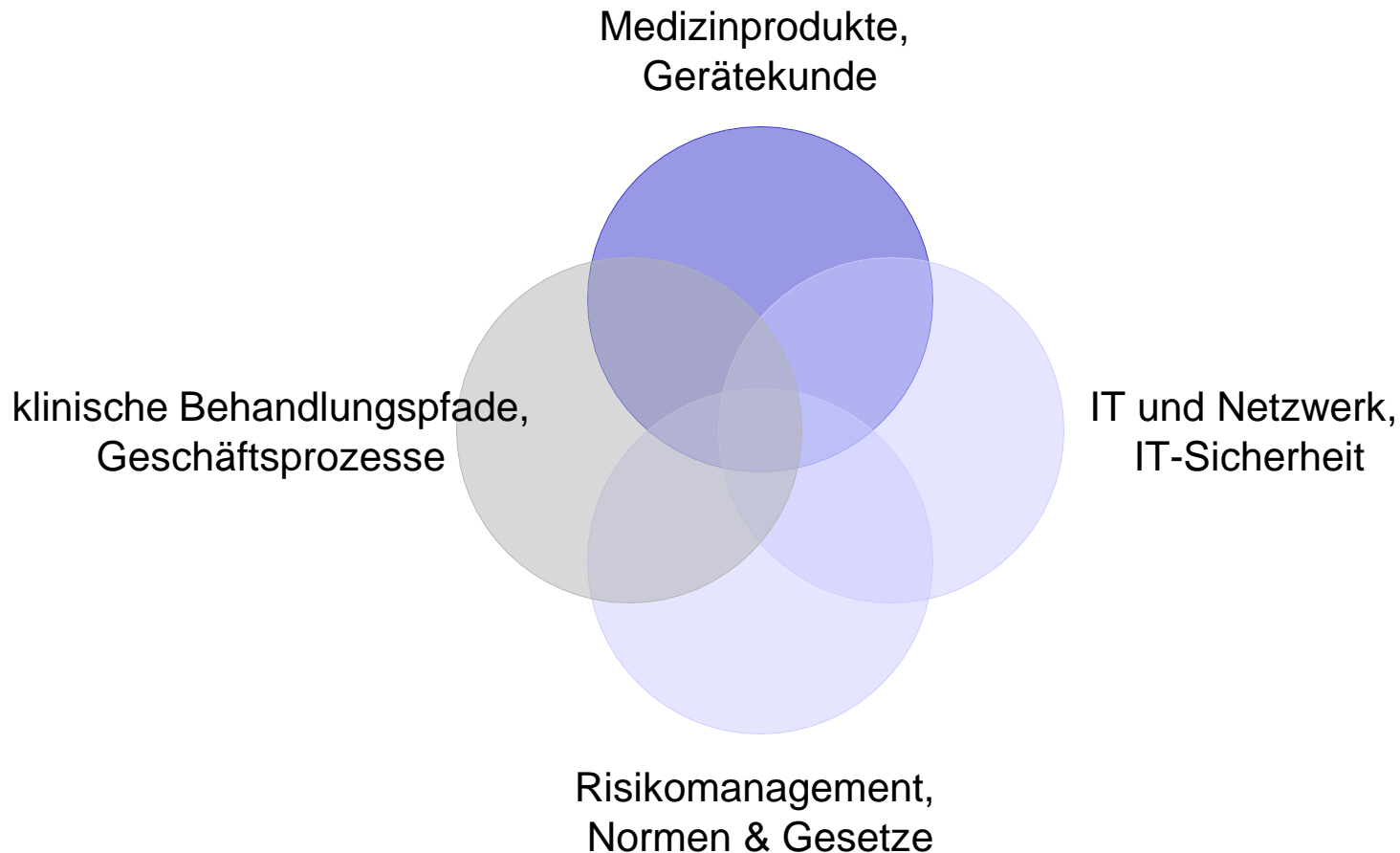
4.6 Risikomanagement für das funktionierende Netzwerk

Aufgaben und Verantwortlichkeiten



Schlüsselrolle: Risikomanager für das Medizinische IT Netzwerk

Risikomanager
für das
Medizinische
IT Netzwerk



Risikomanager für das Medizinische IT Netzwerk



- Risikomanagement von Medizinischen IT Netzwerken:
 - Gesamt-Management des Risikomanagement-Prozesses,
 - Berichte an die oberste Leitung über den Risikomanagement-Prozess,
 - Lenkung der erforderlichen Kommunikation zwischen den internen und externen Teilnehmern am Risikomanagement.

- Durchführung des Risikomanagement-Prozesses:
 - Sammeln aller für Risiken wichtigen Informationen über Medizinprodukte,
 - Planung der Einbindung der Medizinprodukte,
 - Durchführung des Risikomanagement-Prozesses,
 - wenn ein Medizinprodukt zu einem IT Netzwerk hinzugefügt wird,
 - wenn ein eingebundenes Medizinprodukt oder das Medizinische IT Netzwerk verändert wird;
 - Autorisierung für das in Betrieb gehen nach einer Änderung am Medizinischen IT Netzwerk;
 - Information an die Verantwortliche Organisation über unvermeidbare Risiken und die möglichen Gefährdungen infolge von Änderungen an der Konfiguration,
 - Überwachung aller Projekte oder Änderungen des Medizinischen IT Netzwerks.

- Anweisungen für die Durchführung der Einbindung geben:
 - a) der **Zweck** seines in ein IT-Netzwerk eingebundenen Medizinprodukts;
 - b) die **geforderten Leistungsmerkmale des IT-Netzwerks**, in das sein Medizinprodukt eingebunden wird;
 - c) die **geforderte Konfiguration des IT-Netzwerks**, in das sein Medizinprodukt eingebunden wird;
 - d) die **technischen Spezifikationen des Netzwerkanschlusses** des Medizinprodukts, einschließlich der Sicherheitsspezifikationen;
 - e) der **beabsichtigte Informationsfluss** zwischen dem Medizinprodukt, dem medizinischen IT-Netzwerk und anderen Geräten im medizinischen IT-Netzwerk; wenn es für die wesentlichen Eigenschaften relevant ist, muss auch das beabsichtigte Routing durch das medizinische IT-Netzwerk angegeben werden.
 - f) Eine **Liste der Gefährdungssituationen**, die resultieren, wenn ein IT-Netzwerk nicht die Leistungsmerkmale liefert, die erforderlich sind, um den Zweck der Einbindung des Medizinproduktes in das IT-Netzwerk zu erfüllen.

- Pflicht zur Dokumentation und Bereitstellung von
 - allen für das Risikomanagement Medizinische IT-Netzwerk relevante Informationen, insbesondere
 - alle bekannten Gefährdungssituationen, die von der Verantwortlichen Organisation gehandhabt werden müssen.
- Für die Zuständigkeitsvereinbarung benötigte Dokumente und Informationen mit folgenden Inhalten:
 - Umfang der Tätigkeiten in allen Phasen des Lebenszyklus des medizinischen IT Netzwerks
 - Anweisungen für die Einbindung in ein, oder Herauslösung aus einem IT Netzwerk,
 - Für die Durchführung einer Risikoanalyse des Medizinischen IT-Netzwerks notwendigen technischen Informationen.

Wesentliche Eigenschaften nach DIN EN 80001

1. Sicherheit (safety)
→ ableitbar aus RA Konformitätsbewertung
2. Wirksamkeit (effectiveness)
→ neu für den Medizinproduktehersteller
3. Daten & System Sicherheit (security)
(Vertraulichkeit, Integrität, Verfügbarkeit)
→ neu für den Medizinproduktehersteller



Fragestellung für das Forschungsprojekt

TP 5 - Betreibermodelle

- Wie können für das Risikomanagement wichtige Informationen an die Betreiber fließen, ohne dass schutzwürdige Informationen zu den einzelnen Medizinprodukten offenbart werden müssen?
- Wie kann der Hersteller zusammen mit dem Betreiber eine Liste von Gefährdungssituationen bei nicht nach den Spezifikationen arbeitenden IT-Netzwerken liefern?
- Welche Informationen lassen sich nur Projekt-individuell erarbeiten und welche Maßnahmen können für einen Grundschutz spezifiziert werden?
- Welche Organisationsformen für interne und externe Betriebsleistungen erlauben einen zuverlässigen und effizienten Betrieb sicherer Medizinproduktenetzwerke?
- Welche Dienstleistungen können die Hersteller anbieten?
- Welche betriebswirtschaftlichen Modelle bzw. Geschäftsmodelle können identifiziert werden?
- Welche technischen Voraussetzungen müssen für die einzelnen Organisationsformen und betriebswirtschaftlichen Modelle erfüllt werden?
- Durch welche Maßnahmen hinsichtlich des Datenschutzes müssen die einzelnen Organisationsformen und betriebswirtschaftlichen Modelle flankiert werden?

Vorgehen

TP 5 - Betreibermodelle

- Risikoanalysen ausgewählter Referenzsysteme und Risikokontrollmaßnahmen
- Entwicklung Anforderungskatalog (Betreibersicht)
- Entwicklung Leitungskatalog (Anbietersicht)
 - Umsetzung der Anforderungen der Betreiber in spezifische System- und Dienstleistungen (Leistungsscheine)
 - Zusammenstellung der Leistungsscheine zu einem Leistungsportfolio (Leistungskatalog)
- Erstellung Marktübersicht zum Leistungskatalog
- Ausarbeitung Vertragsmuster zum Leistungskatalog

Vielen Dank!

Dr. Andreas Zimolong

Synagon GmbH

Im Süsterfeld 6, 52072 Aachen

Tel: 02441 / 7010 3133

eMail: Andreas.Zimolong@Synagon.de

www.Synagon.de

