Sana Klinik Service

SKS Webinar
24.04.2024

Sana Medizintechnisches Servicezentrum

Umsetzung des Risikomanagements bei der MedIT

Zusammenfassung der Normengeber und strategisches Vorgehen

Sana Klinik
Service

Medworx

Sana Sterilgut
Service

ROESER

Sana Medizintechnisches
Servicezentrum

Revitech

Sana Medizintechnisches Servicezentrum

Kompetenzbereich Technische Services
IT-Sicherheit von Medizinprodukten

CHRISTIAN SULZBERGER

- Teamleitung Kompetenzbereich IT-Sicherheit von Medizinprodukten
- Mitglied im EK Cybermed
- Normengremium DIN EN 62353 und Cybersecurity von Medizinprodukten

c.sulzberger@sana-mtsz.de

Motivation

Sana Medizintechnisches Servicezentrum

“IT-Sicherheit von Kliniken mangelhaft.” [kma-online.de]

Überwachung des Betriebs von vernetzten Medizinprodukten [AGMP: Formblatt 206]

KritisV, SGB V, DIN EN IEC 80001-1, NIS-2, KHZG etc.

Anwender: “Meine Geräte sollen vernetzt sein.”

veränderte Lage:

- Bedrohungslage
- Regulatorik
- Produkte (höherer Vernetzungsgrad)

80001-Normenreihe

Sana Medizintechnisches Servicezentrum

Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten

Teil 2-1 (10/2012): Schritt-für-Schritt-Risikomanagement von medizinischen IT-Netzwerken

Teil 2-2 (10/2012): Leitfaden zur Angabe von Bedingungen für die Kommunikations-sicherheit

Teil 2-3 (10/2012): Leitfaden für drahtlose Netzwerke

Teil 2-4:General implementation guidance for Healthcare Delivery Organizations

Teil 2-5 (03/2016): Anleitung für verteilte Alarmsysteme

Teil 2-6 (12/2014): Anleitung für Verantwortungs-vereinbarungen

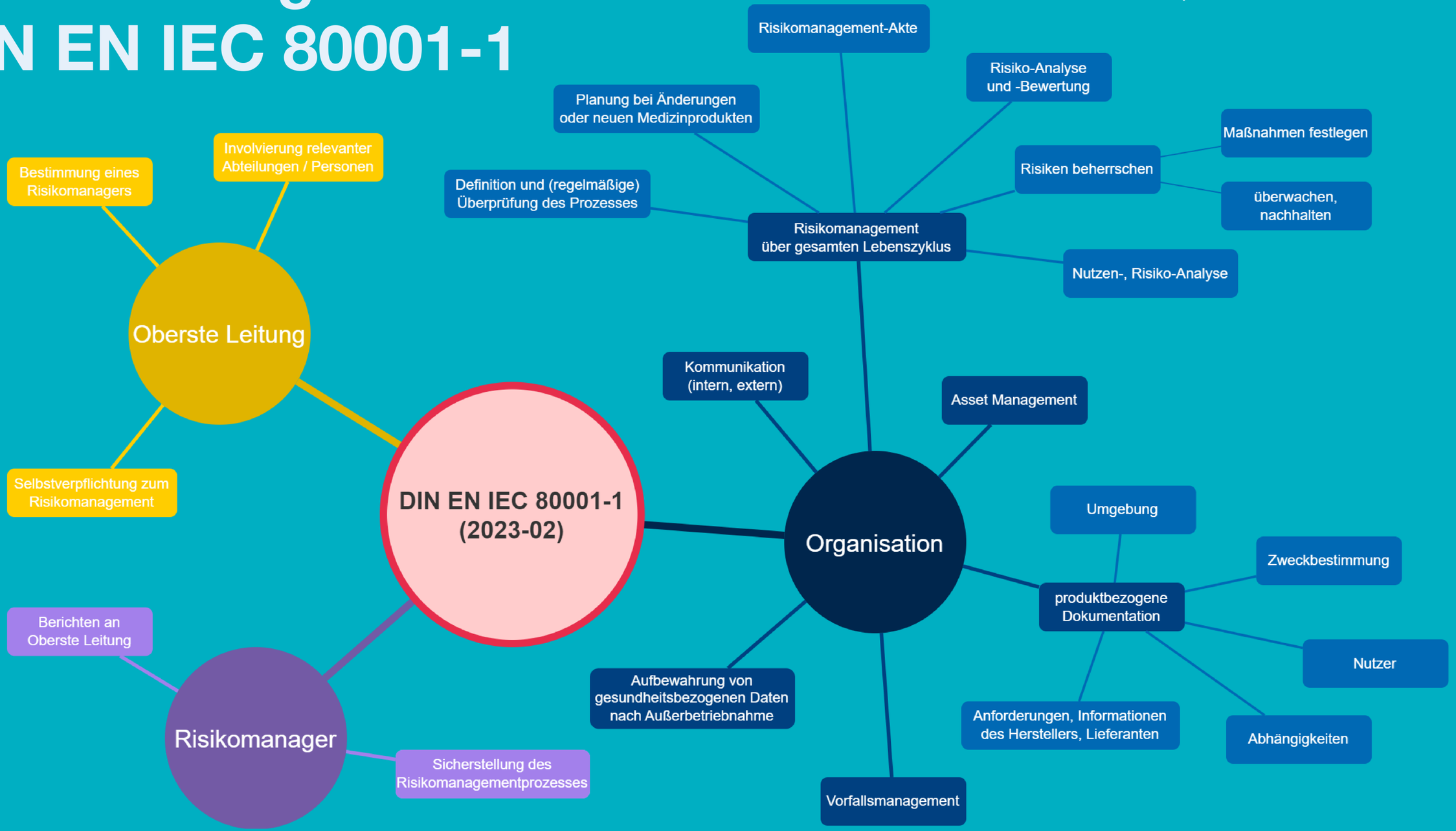
Teil 2-7 (04/2015): Selbsteinschätzung ihrer Übereinstimmung mit IEC 80001-1

Teil 2-8 (05/2016): Anleitung für den technischen Informations-austausch für Zulieferer

Teil 2-9 (02/2017): Verwendung von Assurance Cases zur Bestätigung der Übereinstimmung mit IEC/TR 80001-2-2

Anforderungen der DIN EN IEC 80001-1

Sana Medizintechnisches Servicezentrum



Sana Medizintechnisches Servicezentrum

Schutzziele verschiedener Regularien

Regularien / Schutzziele	BSIG	SGB V	B3S Gesundheit	DIN EN IEC 80001-1
Verfügbarkeit	✓	✓	✓	✓
Integrität	✓	✓	✓	✓
Vertraulichkeit	✓	✓	✓	✓
Authentizität	✓		✓	
Patienten-sicherheit		Sicherheit der Patienten-informationen	✓	Sicherheit für Patienten, Anwender, Dritte
Effektivität		Funktions-fähigkeit des Krankenhauses	Behandlungs-effektivität	Wirksamkeit

- unterschiedliche Vorgaben, jedoch das selbe Ziel; teilweise mit unterschiedlichem Scope
- „VIV“ sind die Grundziele, aus denen sich die anderen Schutzziele abstützen (können).
- Betrachtung der Einzelgeräte als auch der gesamten Systeme erforderlich.
- Forderung nach Risikomanagement: Gefährdungen aus B3S Gesundheit, BSI-IT-Grundschutz oder spezifischeren Normen

vom Detail zum Groben, vom Groben zum Detail

Sana Medizintechnisches Servicezentrum

IT, Netzwerk-Infrastruktur, Medizinprodukte, Personal

(Konzern-, Krankenhaus-) Informationssicherheit

ca. 110.000 Medizinprodukte

einzelne vernetzte Systeme

Vorgehen zur Umsetzung

Sana Medizintechnisches Servicezentrum

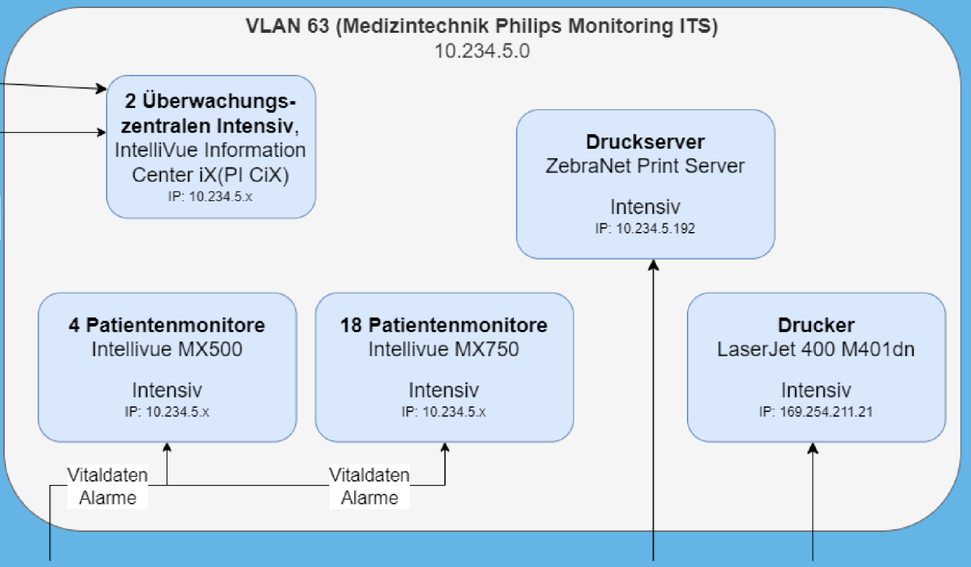
Verständnis Transparenz	**1 – Vorbereitung**		Schutzbedarfsanalyse Abstimmung System und Umfang Involvierung relevanter Personen
	2 – Erhebung MIT-System		Einholung des Geräteprofils (MDS-2), Verständnis des Systems mit der dazugehörigen Infrastruktur und Anwendung
	3 – Risiko-Analyse & -Bewertung		Identifikation möglicher Risikoszenarien Durchführung der Risiko-Analyse
Finden von Lösungen	**4 – Ableiten von Maßnahmen**		Eruierung von Maßnahmen
Erhöhung der Sicherung	**5 – Risikobeherrschung**		Umsetzung und Nachverfolgung von Maßnahmen

Softwareunterstützung für ISMS und Risikomanagement

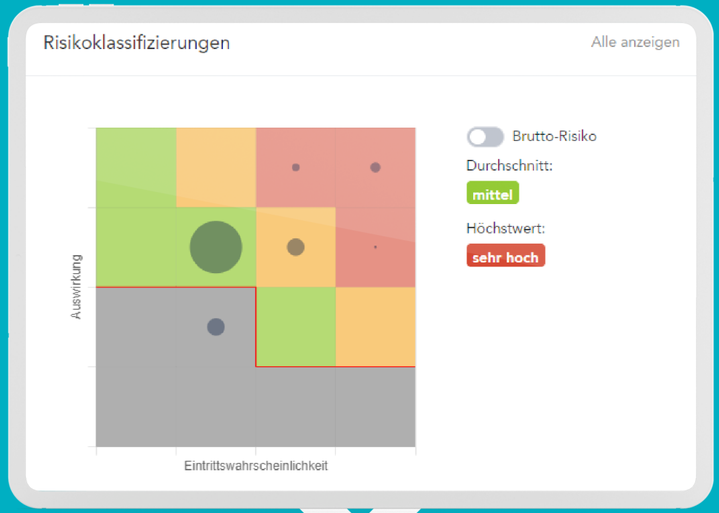
Sana Medizintechnisches Servicezentrum

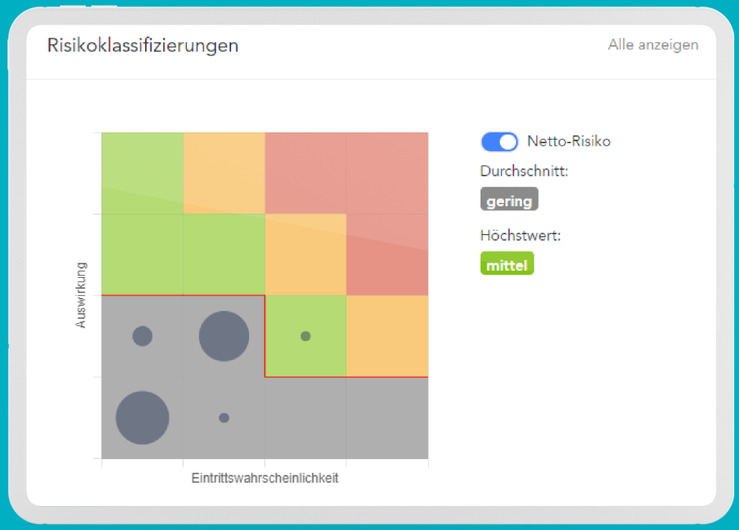
einzelne vernetzte Systeme

einzelne vernetzte Systeme



einzelne vernetzte Systeme





Lösungen für vernetzte Medizinprodukte

Sana Medizintechnisches Servicezentrum

MEDIGATE asimily ARMIS ordr CyberMDX paloalto NETWORKS

Sana Medizintechnisches Servicezentrum

Fazit

1. Betreiber müssen auf die veränderte Lage reagieren.

2. Es bestehen viele Regularien, welche in der Auswirkung auf Medizinprodukte größtenteils redundant sind: Betreiber sollen risikobasiert und abteilungsübergreifend vorgehen.

3. Eine Umsetzung ist sowohl mit üblichen Tools (wie Excel, Lansweeper etc.) als auch mit spezifischerer Tool-Unterstützung (IoT-Security, ISMS) möglich.

Sana Medizintechnisches Servicezentrum

Module zum Risikomanagement vernetzter Medizinprodukte

(nach DIN EN IEC 80001 innerhalb KritisV bzw. SGB V)

Module im Detail

Sana Medizintechnisches Servicezentrum

Modul	A Check-up	B Schulung	C Strategieberatung	D Umsetzungsprojekt
Inhalte	• Durchführung des Risikomanagements • Erstellung einer Dokumentation inkl. eines Maßnahmenkataloges zur Risikominimierung • hands-on bei Umsetzung • Möglichkeit eines Reviews der empfohlenen Maßnahmen	• Durchführung des Risikomanagements • Erstellung einer Dokumentation inkl. eines Maßnahmenkataloges zur Risikominimierung • hands-on bei Umsetzung • Möglichkeit eines Reviews der empfohlenen Maßnahmen	• Durchführung des Risikomanagements • Erstellung einer Dokumentation inkl. eines Maßnahmenkataloges zur Risikominimierung • hands-on bei Umsetzung • Möglichkeit eines Reviews der empfohlenen Maßnahmen	• Durchführung des Risikomanagements • Erstellung einer Dokumentation inkl. eines Maßnahmenkataloges zur Risikominimierung • hands-on bei Umsetzung • Möglichkeit eines Reviews der empfohlenen Maßnahmen
Ziele	1. Transparenz zum Umsetzungsstand der DIN EN IEC 80001 im Krankenhaus 2. Ableitung von Maßnahmen	1. Verständnis der Norm 2. Kenntnisse zu Werkzeugen 3. Befähigung zur Entwicklung einer Umsetzungsstrategie durch das Krankenhaus	1. Verständnis der Norm 2. Befähigung der Verantwortlichen zur Erfüllung der regulatorischen Anforderungen	1. Normkonformität erfüllt 2. aufzeigen und umsetzen von Risiken und risiko-minimierenden Maßnahmen 3. Nachweis für mögliche Audits