CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

ISMS und Medizintechnik im Kontext KRITIS

Michael Römling
CISO / Informationssicherheitsbeauftragter
Stabsstelle Informationssicherheit

Charité – Universitätsmedizin Berlin

Informationssicherheit in Kritischen Infrastrukturen

Ransomware WannaCry befällt Rechner der Deutschen Bahn

13.05.2017 11:22 Uhr – Volker Briegleb

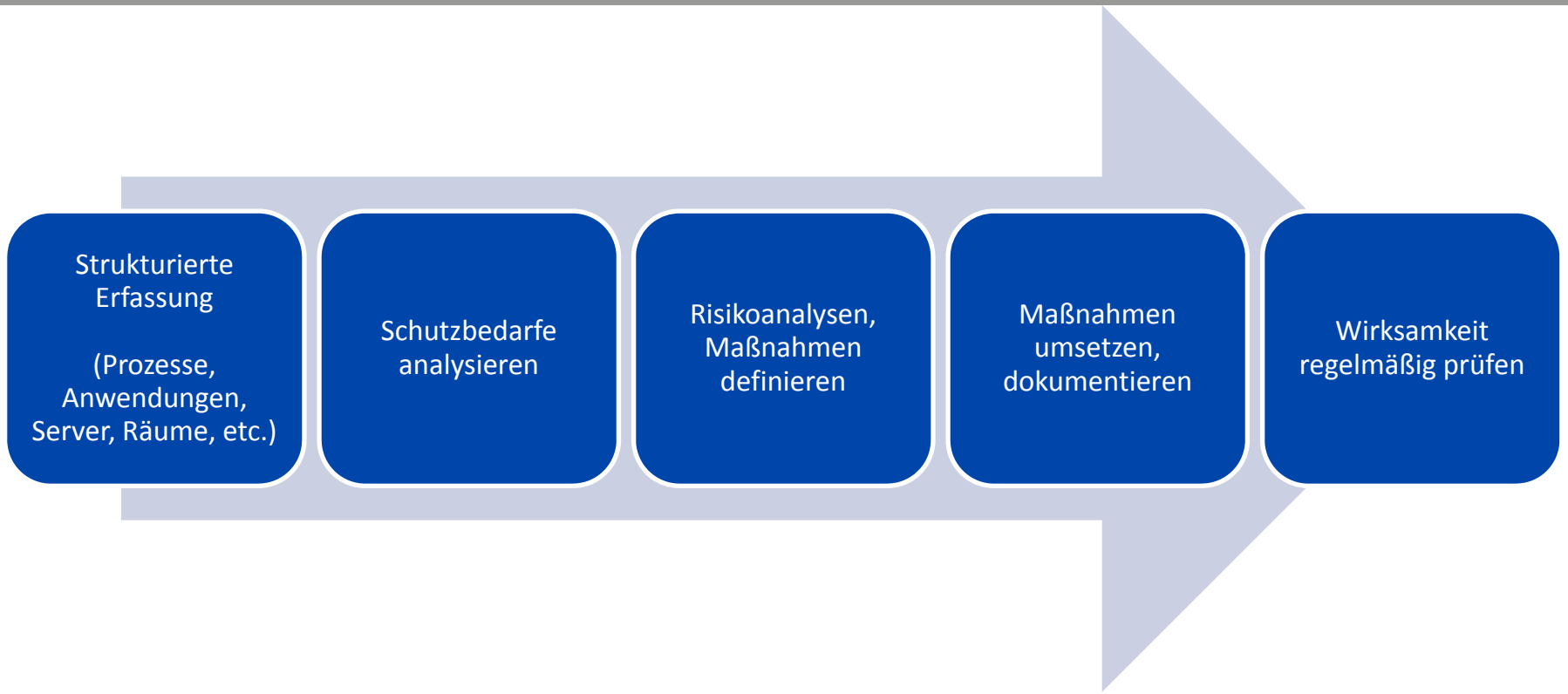
vorlesen

(Bild: Martin Wiesner)

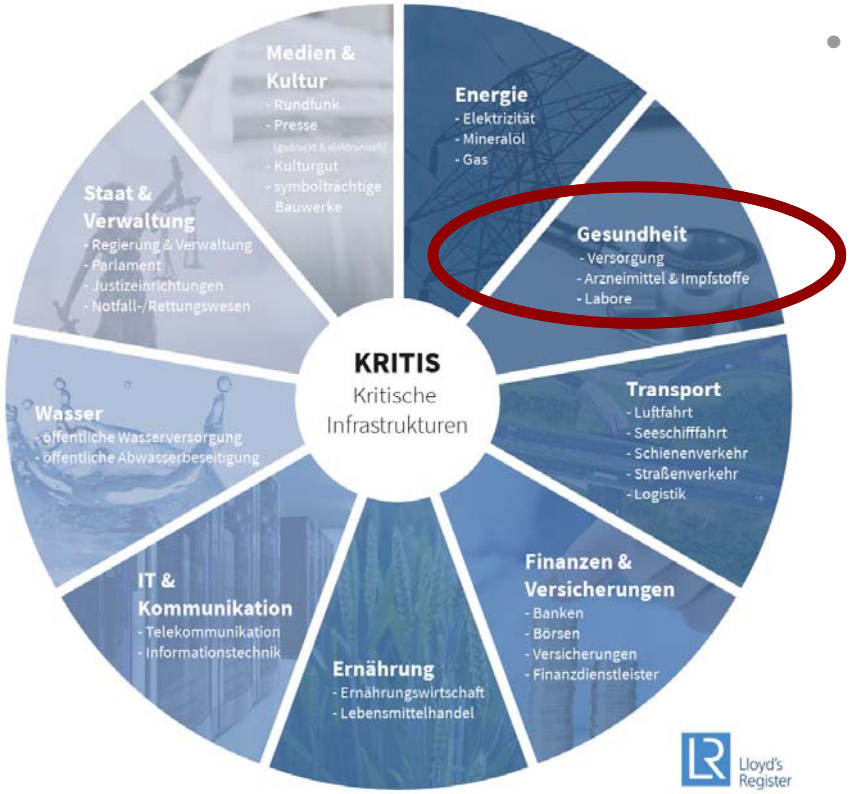
Ausgangslage: IT-Sicherheitsgesetz

- Gesetz zur **Erhöhung der Sicherheit** informationstechnischer Systeme (IT-SiG)
- gültig seit 2015, § 10 IT-SiG: Welche Unternehmen dies betrifft, regelt der Gesetzgeber in sog. Rechtsverordnungen „zur Bestimmung kritischer Infrastrukturen“ (KRITIS)
- **Organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der informationssicherheitstechnischen Systeme, Komponenten, Prozesse
- Übergangsfrist von zwei Jahren, um die Auflagen nachzuweisen
- Wirksamkeit der Maßnahmen **sind danach alle zwei Jahre** nachzuweisen (durch Audits oder Zertifizierung)

Ausgangslage: ISM-Vorgehensweise allgemein

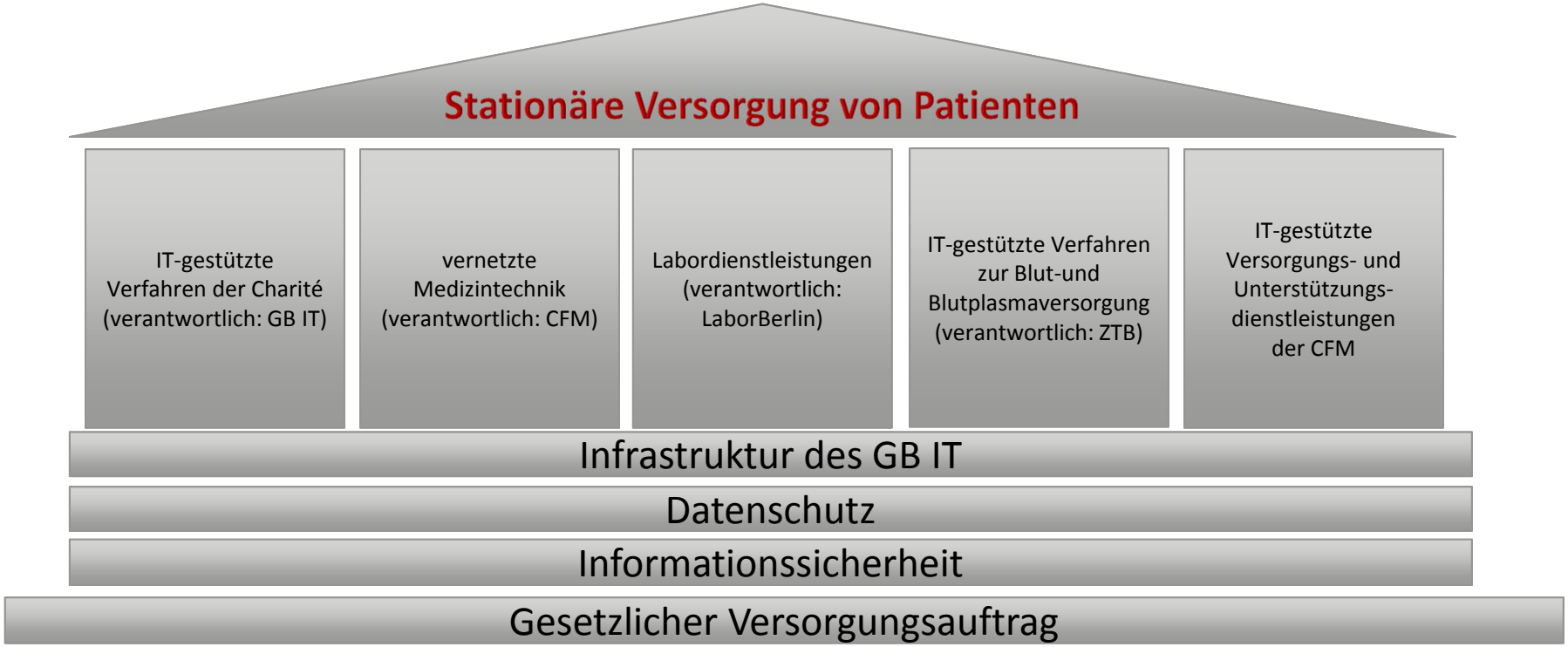


KRITIS Sektoren



- Sektor Gesundheit
  - Nachweispflicht nach §8a(3) BSIG/IT-SiG bis Juni 2019
  - Beinhaltet die Strukturen für
    - Stationäre Versorgung
    - Arzneimittel & Impfstoffe
    - Labore

kDL der Charité (technische Sichtweise)



Was ist „die IT“ der Charité?

Töchter und Beteiligungen

2

Rechen-zentren

Forschung & Lehre, Studien

ca. 30.000

Identitäten

ca.15.000

Klinische Arbeitsplätze

ca. 8.000

Vernetzte Medizinprodukte

Informationssicherheit bei Gesundheitsversorgern
Szenario: Totalausfall durch Schadsoftware per Mail – Teil 1

- "Betrifft: Einladung zum Kongress Gastroenterologie in Hamburg" Unter dieser Überschrift erreicht eine E-Mail das Büro der Klinik-Leitung.
- Solche Einladungen sind nichts Ungewöhnliches. Also öffnet ein Mitarbeiter die Mail.
- Kurz darauf wird der Bildschirm schwarz und auf dem Display erscheint ein Hinweis.
- Die Botschaft: Die Daten des Empfängers sind verschlüsselt. Ein Entschlüsselungscode wird nur gegen die Zahlung von 0,5 Bitcoins (damals ca. EUR 3.000 Euro) geliefert.

Informationssicherheit bei Gesundheitsversorgern
Szenario: Totalausfall durch Schadsoftware per Mail – Teil 2

- Tatsächlich werden in den nächsten Minuten immer mehr Teile des IT Netzes der Klinik unbrauchbar.
- Die Klinikleitung entscheidet daraufhin, die IT vollständig abzuschalten.
- Noch am selben Tag muss die Notaufnahme der Klinik geschlossen werden.
- Operationen werden verschoben, die Bestrahlung von Krebspatienten ausgesetzt.
- Es können keine Medikamente mehr bestellt werden, denn auch das läuft vollständig digital.
- Erst nach einer Woche Ausnahmezustand kann die Klinik ihre bereinigte IT wieder hochfahren.

Informationssicherheit in Kritischen Infrastrukturen

heise online ⟩ News ⟩ 03/2018 ⟩ **Sicherheitslücken: Medizinische Geräte können gehackt werden**

28.03.2018 12:30 Uhr

Sicherheitslücken: Medizinische Geräte können gehackt werden

Medizinische Geräte wie Herzschrittmacher oder Insulinpumpen können gehackt werden – auch wenn die Gefahr gering ist. Anfälliger ist eher die IT in Krankenhäusern, die ein Einfallstor für Hacker zu medizinischen Überwachungsgeräten sein kann.

von **Andrea Barthélémy, dpa**

36

(Bild: Pixabay / CC0)

16.11.2018 14:47 Uhr

Fürstenfeldbruck: Malware legt Klinikums-IT komplett lahm

Im bayerischen Fürstenfeldbruck muss die örtliche Klinik seit Tagen fast komplett ohne Computer auskommen; verantwortlich ist Malware.

Von **Martin Holland**

762

Das Klinikum Fürstenfeldbruck (Bild: Klinikum FFB)

Das Klinikum Fürstenfeldbruck in Bayern muss seit einer Woche ohne Computer auskommen, nachdem offenbar ein per Mail empfangener Trojaner die IT-Systeme infiziert hat. Das meldet der *Münchner Merkur* unter Berufung auf Verantwortliche des Krankenhauses in der Kreisstadt westlich von München. Noch immer werden demnach fast alle der 450 vorhandenen Computer überprüft und die Angelegenheiten des Hauses müssen weitgehend ohne IT-Unterstützung erledigt werden. Erst in den kommenden Tagen sollten alle Geräte wieder funktionieren.

Informationssicherheit bei Gesundheitsversorgern
Szenario: Totalausfall durch Schadsoftware per USB (Stabsübung 2019)

- **08:20 Uhr:** bei Routine-Wartungsarbeiten eines externen Dienstleisters wird Schadsoftware unbemerkt in die IT-Infrastruktur des Krankenhauses eingeschleust (infizierter USB-Stick)
- **09:45 Uhr:** zunächst fallen nur einige Befundarbeitsplätze (RIS/PACS-Workstations) im CT und Röntgenbereich und in der zentralen Notaufnahme aus
- **10:25 Uhr:** der Vorfall wird bemerkt, die betroffenen Rechner werden isoliert
- **11:10 Uhr:** nach und nach werden weitere Radiologie-Arbeitsplätze infiziert, sodass keine Notfallpatienten mehr versorgt werden können
- **13:15 Uhr:** nach vergeblichen Korrekturversuchen werden die Notaufnahmen nach und nach abgemeldet
- **…**

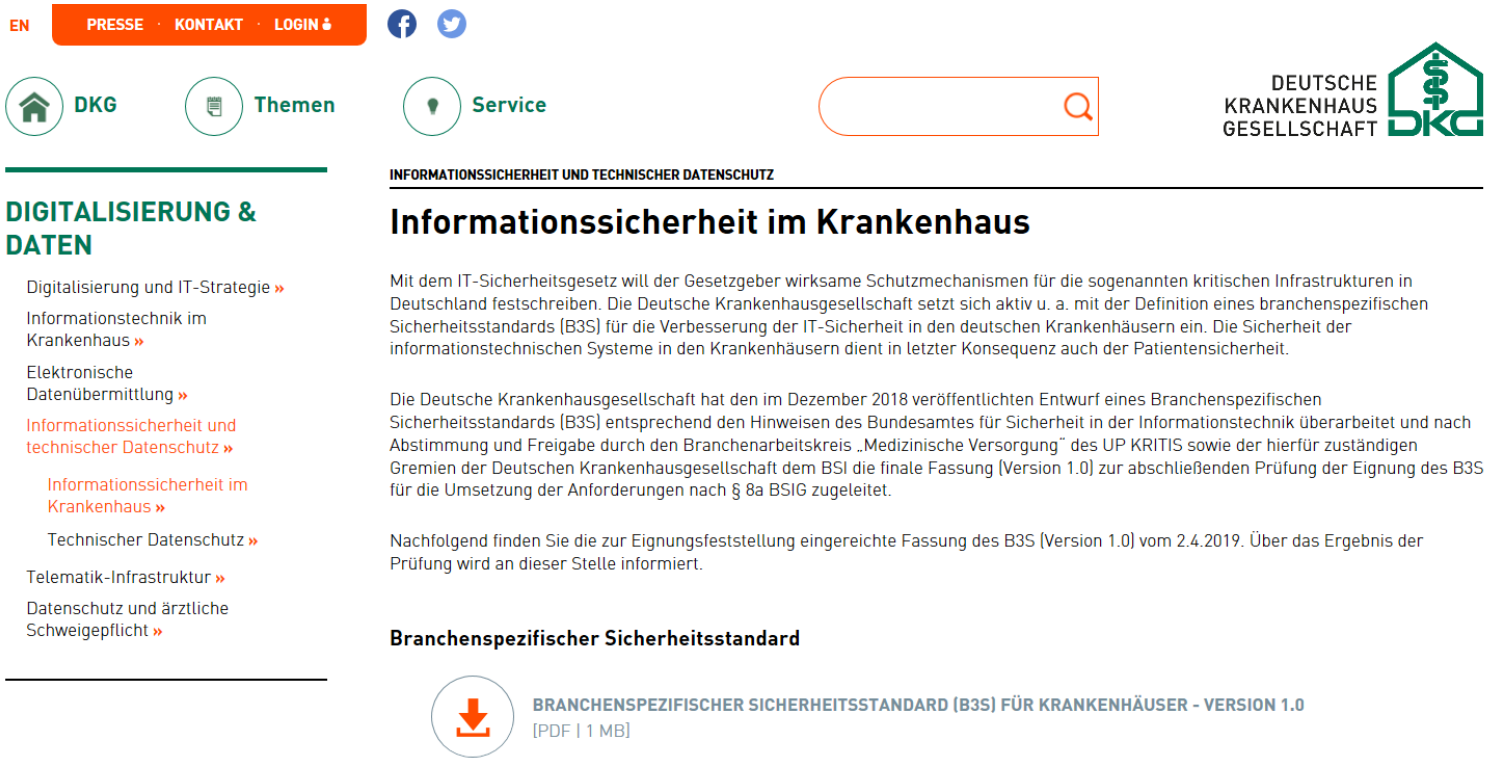
BSI: Bundesamt für Sicherheit in der Informationstechnik

„ Krankenhäuser, die gemäß BSI-Gesetz als Kritische Infrastruktur eingestuft wurden, sind verpflichtet, dem BSI **bis spätestens Juni 2019 nachzuweisen, dass sie IT-Sicherheitsmaßnahmen nach dem Stand der Technik erfolgreich implementiert haben**.“

„Der zunehmende **Einsatz netzwerkfähiger Medizinprodukte ist dabei ein zentraler Aspekt**.“

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/sicherheitsanforderung_medizinprodukte_09052018.html

KRITIS-Prüfnachweis auf Basis B3S



EN PRESSE · KONTAKT · LOGIN

DKG Themen Service

DEUTSCHE KRANKENHAUS GESELLSCHAFT

DIGITALISIERUNG & DATEN

- Digitalisierung und IT-Strategie »
- Informationstechnik im Krankenhaus »
- Elektronische Datenübermittlung »
- Informationssicherheit und technischer Datenschutz »
  - Informationssicherheit im Krankenhaus »
  - Technischer Datenschutz »
- Telematik-Infrastruktur »
- Datenschutz und ärztliche Schweigepflicht »

INFORMATIONSSICHERHEIT UND TECHNISCHER DATENSCHUTZ

Informationssicherheit im Krankenhaus

Mit dem IT-Sicherheitsgesetz will der Gesetzgeber wirksame Schutzmechanismen für die sogenannten kritischen Infrastrukturen in Deutschland festschreiben. Die Deutsche Krankenhausgesellschaft setzt sich aktiv u. a. mit der Definition eines branchenspezifischen Sicherheitsstandards (B3S) für die Verbesserung der IT-Sicherheit in den deutschen Krankenhäusern ein. Die Sicherheit der informationstechnischen Systeme in den Krankenhäusern dient in letzter Konsequenz auch der Patientensicherheit.

Die Deutsche Krankenhausgesellschaft hat den im Dezember 2018 veröffentlichten Entwurf eines Branchenspezifischen Sicherheitsstandards (B3S) entsprechend den Hinweisen des Bundesamtes für Sicherheit in der Informationstechnik überarbeitet und nach Abstimmung und Freigabe durch den Branchenarbeitskreis „Medizinische Versorgung" des UP KRITIS sowie der hierfür zuständigen Gremien der Deutschen Krankenhausgesellschaft dem BSI die finale Fassung (Version 1.0) zur abschließenden Prüfung der Eignung des B3S für die Umsetzung der Anforderungen nach § 8a BSIG zugeleitet.

Nachfolgend finden Sie die zur Eignungsfeststellung eingereichte Fassung des B3S (Version 1.0) vom 2.4.2019. Über das Ergebnis der Prüfung wird an dieser Stelle informiert.

Branchenspezifischer Sicherheitsstandard

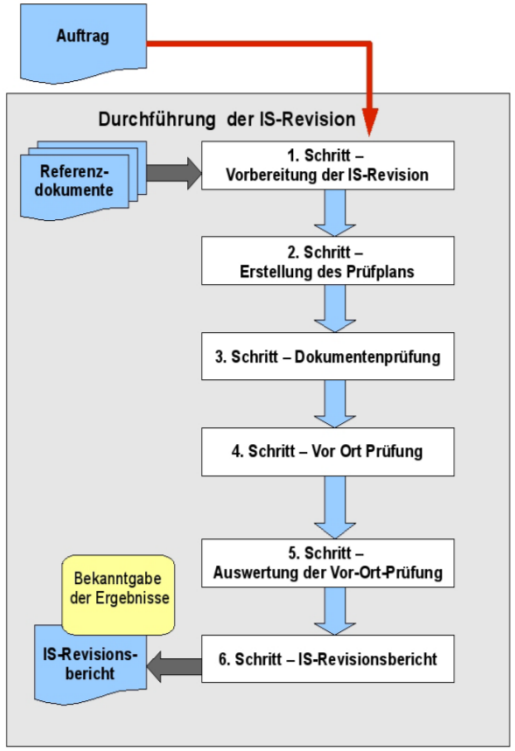
BRANCHENSPEZIFISCHER SICHERHEITSSTANDARD (B3S) FÜR KRANKENHÄUSER - VERSION 1.0
[PDF | 1 MB]

Nachweise gemäß § 8a BSIG

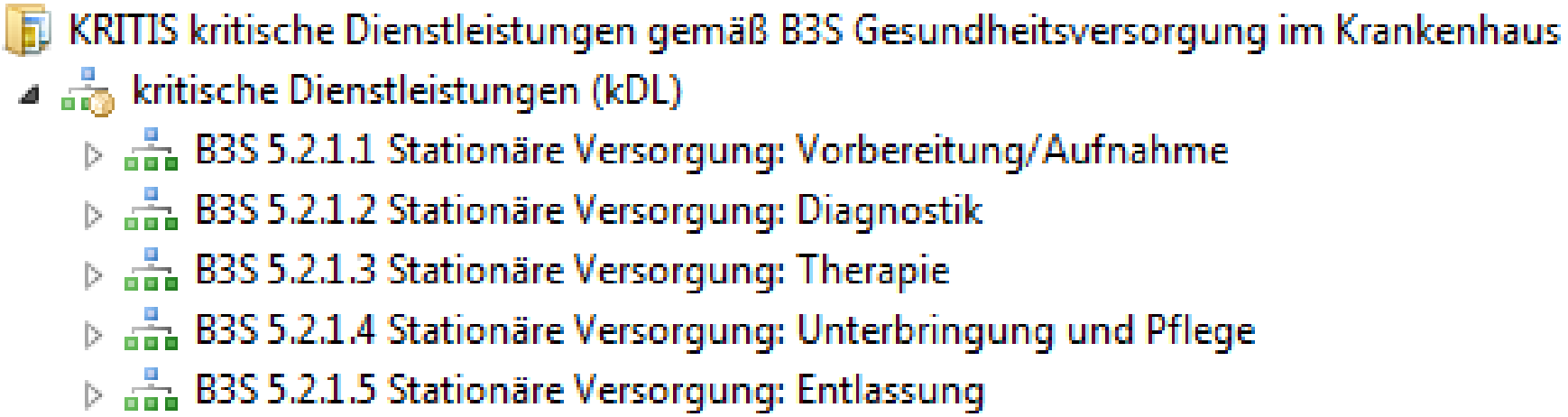
- Sicherheitsniveau feststellen durch unabhängige Instanz
- Hinweise zu bestehenden Sicherheitslücken und -mängel

Besonderheiten für Institutionen im KRITIS-Umfeld

- Nachweispflichten gemäß § 8a BSIG
- Ziel: Vermeidung von Versorgungs-Engpässen
- **Begrenzte** Wirtschaftlichkeitsbetrachtung
- **Risikoakzeptanz und -übernahme nicht zulässig**
- Dialog statt formale Vorgaben und Strafen
- Nachweise bspw. durch ISO 27001-basiertes Managementsystem (Regelungs- und Nachweisdokumente) -> Charité: ISMS-Handbuch und das Tool Verinice

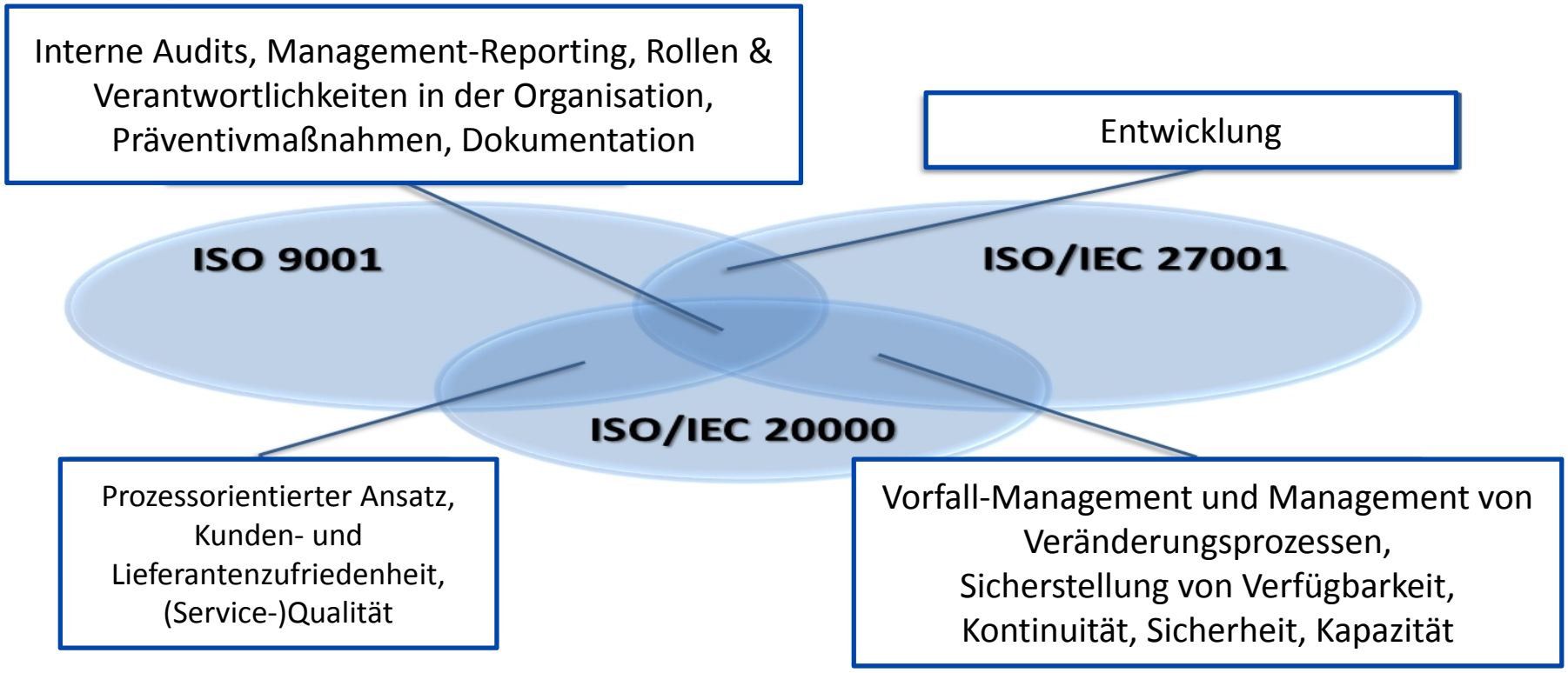


Kritische Dienstleistungen nach B3S Kapitel 5.2.1



kDL umfassen alle relevanten Aufgaben und Infrastrukturen zur Aufrechterhaltung wesentlicher Prozesse der stationären Versorgung

Übergreifende Standards



Wie dokumentieren?

- QM-Handbuch, SOP
- ISMS-Handbuch
- ISMS-Tool
- Zentrale TOM
- DMS
- Regelungs-/Nachweisdokumente
- Intranet / Dateiablagen

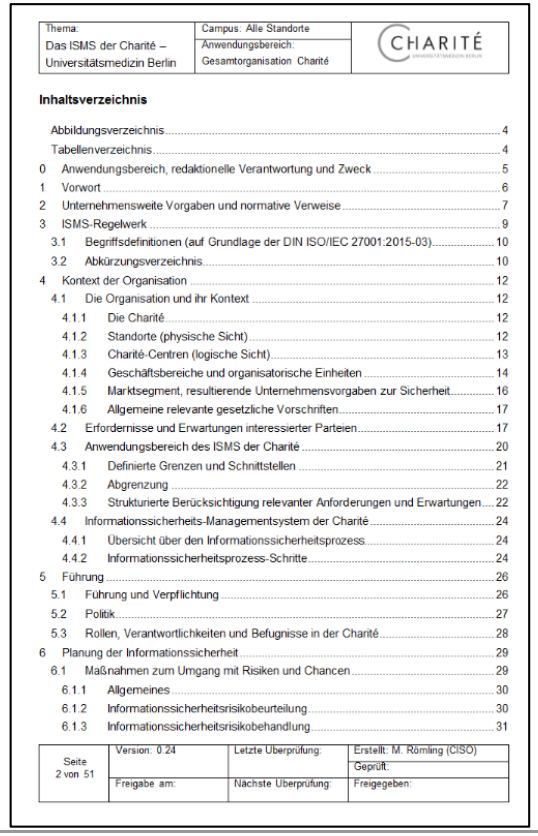
ISMS-Handbuch

Thema: Das ISMS der Charité – Universitätsmedizin Berlin	Campus: Alle Standorte Anwendungsbereich: Gesamtorganisation Charité	CHARITÉ

CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

Das ISMS der
Charité – Universitätsmedizin Berlin

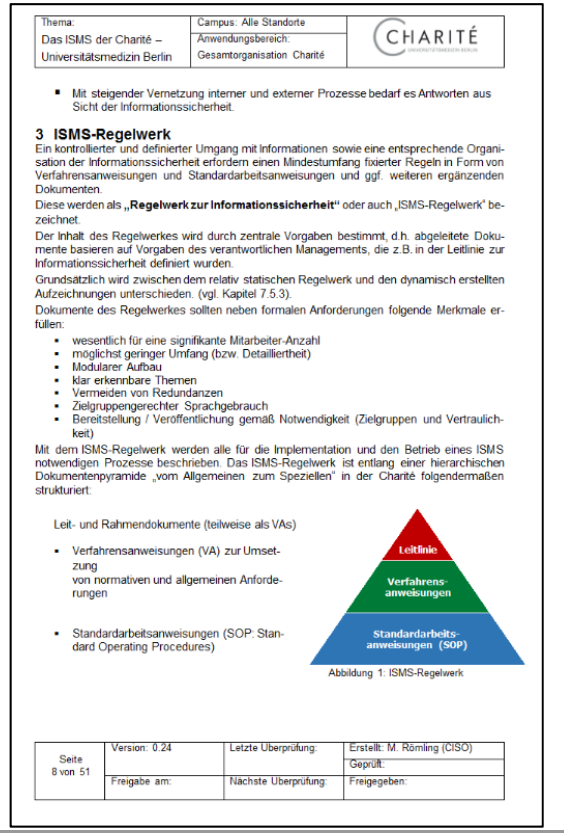
Seite 1 von 51	Version: 0.24	Letzte Überprüfung:	Erstellt: M. Römling (CISO)
			Geprüft:
	Freigabe am:	Nächste Überprüfung:	Freigegeben:



Thema: Das ISMS der Charité – Universitätsmedizin Berlin	Campus: Alle Standorte Anwendungsbereich: Gesamtorganisation Charité	CHARITÉ

Inhaltsverzeichnis

Seite 2 von 51	Version: 0.24	Letzte Überprüfung:	Erstellt: M. Römling (CISO)
			Geprüft:
	Freigabe am:	Nächste Überprüfung:	Freigegeben:



Thema: Das ISMS der Charité – Universitätsmedizin Berlin	Campus: Alle Standorte Anwendungsbereich: Gesamtorganisation Charité	CHARITÉ

- Mit steigender Vernetzung interner und externer Prozesse bedarf es Antworten aus Sicht der Informationssicherheit.

3 ISMS-Regelwerk

Ein kontrollierter und definierter Umgang mit Informationen sowie eine entsprechende Organisation der Informationssicherheit erfordern einen Mindestumfang fixierter Regeln in Form von Verfahrensanweisungen und Standardarbeitsanweisungen und ggf. weiteren ergänzenden Dokumenten.

Diese werden als **„Regelwerk zur Informationssicherheit"** oder auch „ISMS-Regelwerk" bezeichnet.

Der Inhalt des Regelwerkes wird durch zentrale Vorgaben bestimmt, d.h. abgeleitete Dokumente basieren auf Vorgaben des verantwortlichen Managements, die z.B. in der Leitlinie zur Informationssicherheit definiert wurden.

Grundsätzlich wird zwischen dem relativ statischen Regelwerk und den dynamisch erstellten Aufzeichnungen unterschieden. (vgl. Kapitel 7.5.3).

Dokumente des Regelwerkes sollten neben formalen Anforderungen folgende Merkmale erfüllen:

- wesentlich für eine signifikante Mitarbeiter-Anzahl
- möglichst geringer Umfang (bzw. Detailliertheit)
- Modularer Aufbau
- klar erkennbare Themen
- Vermeiden von Redundanzen
- Zielgruppengerechter Sprachgebrauch
- Bereitstellung / Veröffentlichung gemäß Notwendigkeit (Zielgruppen und Vertraulichkeit)

Mit dem ISMS-Regelwerk werden alle für die Implementation und den Betrieb eines ISMS notwendigen Prozesse beschrieben. Das ISMS-Regelwerk ist entlang einer hierarchischen Dokumentenpyramide „vom Allgemeinen zum Speziellen" in der Charité folgendermaßen strukturiert:

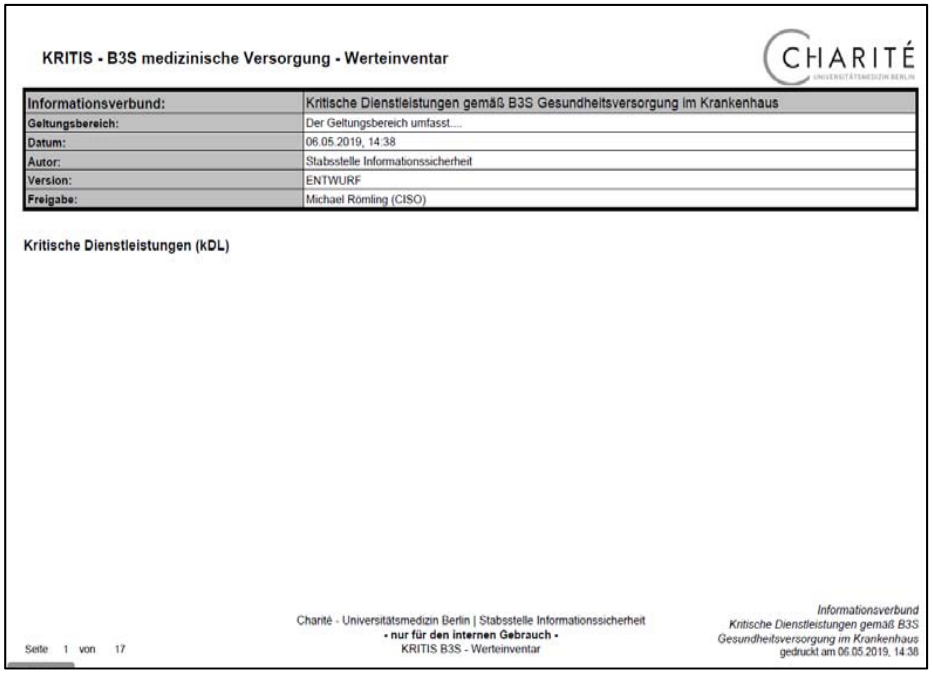
Leit- und Rahmendokumente (teilweise als VAs)

- Verfahrensanweisungen (VA) zur Umsetzung von normativen und allgemeinen Anforderungen
- Standardarbeitsanweisungen (SOP: Standard Operating Procedures)

Abbildung 1: ISMS-Regelwerk

Seite 8 von 51	Version: 0.24	Letzte Überprüfung:	Erstellt: M. Römling (CISO)
			Geprüft:
	Freigabe am:	Nächste Überprüfung:	Freigegeben:

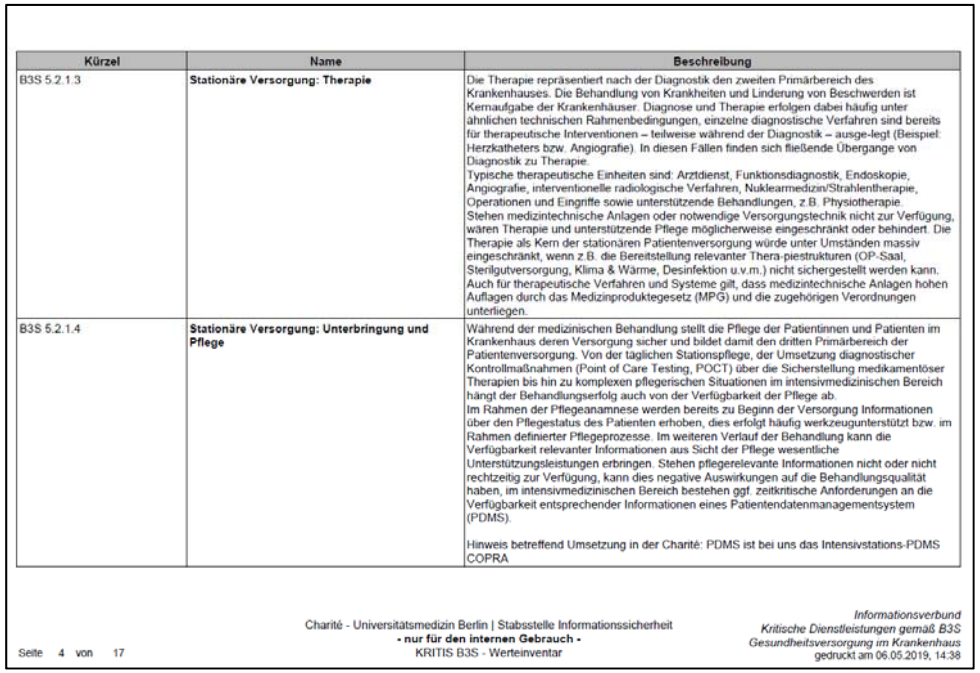
Reports aus dem ISMS-Tool



KRITIS - B3S medizinische Versorgung - Werteinventar

Informationsverbund:	Kritische Dienstleistungen gemäß B3S Gesundheitsversorgung im Krankenhaus
Geltungsbereich:	Der Geltungsbereich umfasst....
Datum:	06.05.2019, 14:38
Autor:	Stabsstelle Informationssicherheit
Version:	ENTWURF
Freigabe:	Michael Römling (CISO)

Kritische Dienstleistungen (kDL)

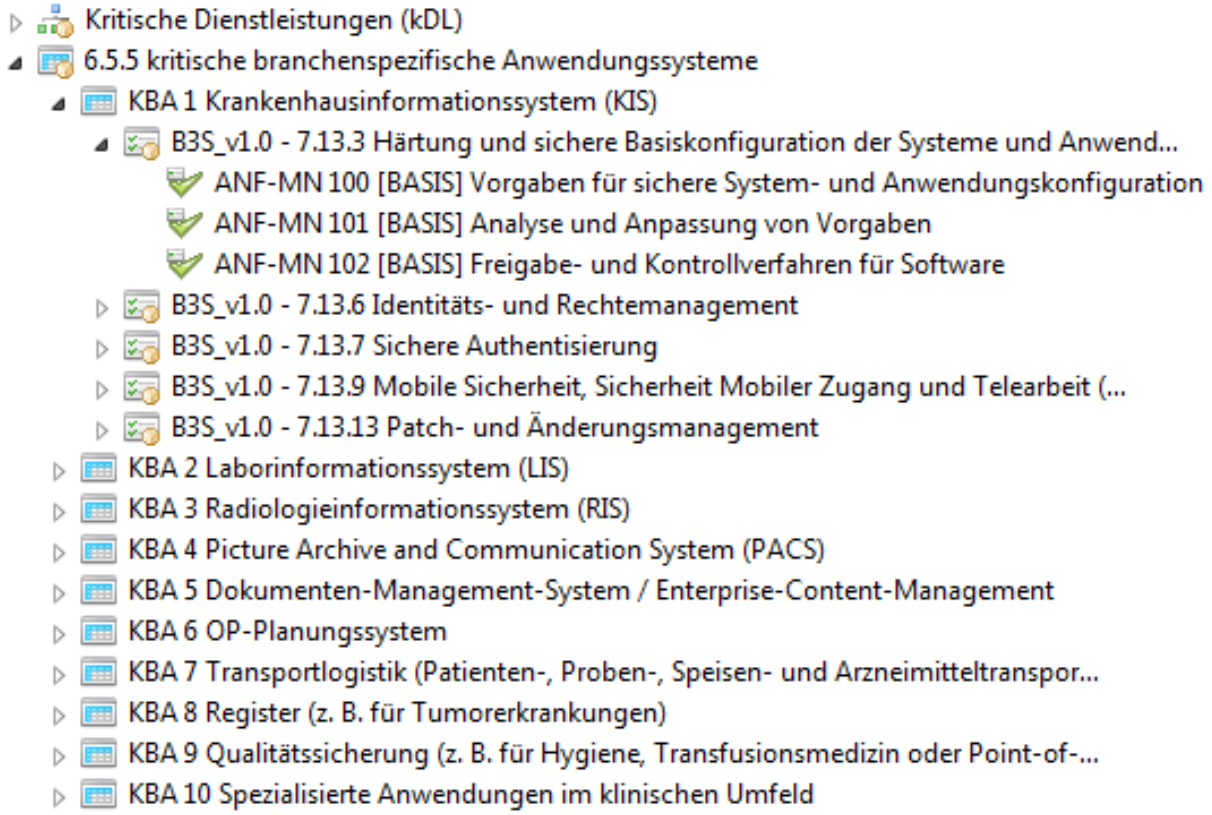


Kürzel	Name	Beschreibung
B3S 5.2.1.3	**Stationäre Versorgung: Therapie**	Die Therapie repräsentiert nach der Diagnostik den zweiten Primärbereich des Krankenhauses. Die Behandlung von Krankheiten und Linderung von Beschwerden ist Kernaufgabe der Krankenhäuser. Diagnose und Therapie erfolgen dabei häufig unter ähnlichen technischen Rahmenbedingungen, einzelne diagnostische Verfahren sind bereits für therapeutische Interventionen – teilweise während der Diagnostik – ausge-legt (Beispiel: Herzkatheters bzw. Angiografie). In diesen Fällen finden sich fließende Übergange von Diagnostik zu Therapie. Typische therapeutische Einheiten sind: Arztdienst, Funktionsdiagnostik, Endoskopie, Angiografie, interventionelle radiologische Verfahren, Nuklearmedizin/Strahlentherapie, Operationen und Eingriffe sowie unterstützende Behandlungen, z.B. Physiotherapie. Stehen medizintechnische Anlagen oder notwendige Versorgungstechnik nicht zur Verfügung, wären Therapie und unterstützende Pflege möglicherweise eingeschränkt oder behindert. Die Therapie als Kern der stationären Patientenversorgung würde unter Umständen massiv eingeschränkt, wenn z.B. die Bereitstellung relevanter Thera-piestrukturen (OP-Saal, Sterilgutversorgung, Klima & Wärme, Desinfektion u.v.m.) nicht sichergestellt werden kann. Auch für therapeutische Verfahren und Systeme gilt, dass medizintechnische Anlagen hohen Auflagen durch das Medizinproduktegesetz (MPG) und die zugehörigen Verordnungen unterliegen.
B3S 5.2.1.4	**Stationäre Versorgung: Unterbringung und Pflege**	Während der medizinischen Behandlung stellt die Pflege der Patientinnen und Patienten im Krankenhaus deren Versorgung sicher und bildet damit den dritten Primärbereich der Patientenversorgung. Von der täglichen Stationspflege, der Umsetzung diagnostischer Kontrollmaßnahmen (Point of Care Testing, POCT) über die Sicherstellung medikamentöser Therapien bis hin zu komplexen pflegerischen Situationen im intensivmedizinischen Bereich hängt der Behandlungserfolg auch von der Verfügbarkeit der Pflege ab. Im Rahmen der Pflegeanamnese werden bereits zu Beginn der Versorgung Informationen über den Pflegestatus des Patienten erhoben, dies erfolgt häufig werkzeugunterstützt bzw. im Rahmen definierter Pflegeprozesse. Im weiteren Verlauf der Behandlung kann die Verfügbarkeit relevanter Informationen aus Sicht der Pflege wesentliche Unterstützungsleistungen erbringen. Stehen pflegerelevante Informationen nicht oder nicht rechtzeitig zur Verfügung, kann dies negative Auswirkungen auf die Behandlungsqualität haben, im intensivmedizinischen Bereich bestehen ggf. zeitkritische Anforderungen an die Verfügbarkeit entsprechender Informationen eines Patientendatenmanagementsystem (PDMS). Hinweis betreffend Umsetzung in der Charité: PDMS ist bei uns das Intensivstations-PDMS COPRA

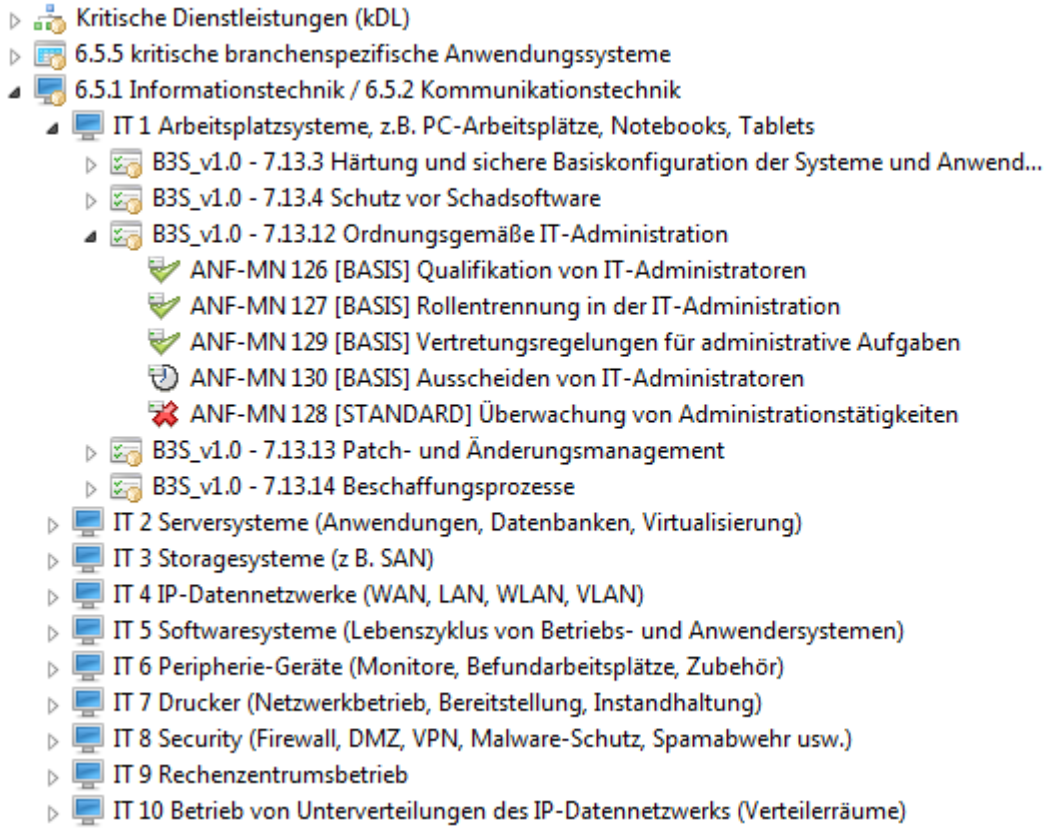
Wie dokumentieren?

Kürzel	Name	Beschreibung
B3S 5.2.1.3	**Stationäre Versorgung: Therapie**	Die Therapie repräsentiert nach der Diagnostik den zweiten Primärbereich des Krankenhauses. Die Behandlung von Krankheiten und Linderung von Beschwerden ist Kernaufgabe der Krankenhäuser. Diagnose und Therapie erfolgen dabei häufig unter ähnlichen technischen Rahmenbedingungen, einzelne diagnostische Verfahren sind bereits für therapeutische Interventionen – teilweise während der Diagnostik – ausge-legt (Beispiel: Herzkatheters bzw. Angiografie). In diesen Fällen finden sich fließende Übergange von Diagnostik zu Therapie. Typische therapeutische Einheiten sind: Arztdienst, Funktionsdiagnostik, Endoskopie, Angiografie, interventionelle radiologische Verfahren, Nuklearmedizin/Strahlentherapie, Operationen und Eingriffe sowie unterstützende Behandlungen, z.B. Physiotherapie. Stehen medizintechnische Anlagen oder notwendige Versorgungstechnik nicht zur Verfügung, wären Therapie und unterstützende Pflege möglicherweise eingeschränkt oder behindert. Die Therapie als Kern der stationären Patientenversorgung würde unter Umständen massiv eingeschränkt, wenn z.B. die Bereitstellung relevanter Thera-piestrukturen (OP-Saal, Sterilgutversorgung, Klima & Wärme, Desinfektion u.v.m.) nicht sichergestellt werden kann. Auch für therapeutische Verfahren und Systeme gilt, dass medizintechnische Anlagen hohen Auflagen durch das Medizinproduktegesetz (MPG) und die zugehörigen Verordnungen unterliegen.
B3S 5.2.1.4	**Stationäre Versorgung: Unterbringung und Pflege**	Während der medizinischen Behandlung stellt die Pflege der Patientinnen und Patienten im Krankenhaus deren Versorgung sicher und bildet damit den dritten Primärbereich der Patientenversorgung. Von der täglichen Stationspflege, der Umsetzung diagnostischer Kontrollmaßnahmen (Point of Care Testing, POCT) über die Sicherstellung medikamentöser Therapien bis hin zu komplexen pflegerischen Situationen im intensivmedizinischen Bereich hängt der Behandlungserfolg auch von der Verfügbarkeit der Pflege ab. Im Rahmen der Pflegeanamnese werden bereits zu Beginn der Versorgung Informationen über den Pflegestatus des Patienten erhoben, dies erfolgt häufig werkzeugunterstützt bzw. im Rahmen definierter Pflegeprozesse. Im weiteren Verlauf der Behandlung kann die Verfügbarkeit relevanter Informationen aus Sicht der Pflege wesentliche Unterstützungsleistungen erbringen. Stehen pflegerelevante Informationen nicht oder nicht rechtzeitig zur Verfügung, kann dies negative Auswirkungen auf die Behandlungsqualität haben, im intensivmedizinischen Bereich bestehen ggf. zeitkritische Anforderungen an die Verfügbarkeit entsprechender Informationen eines Patientendatenmanagementsystem (PDMS). Hinweis betreffend Umsetzung in der Charité: PDMS ist bei uns das Intensivstations-PDMS COPRA

Kritische Anwendungen nach B3S Kapitel 6.5.5



Medizintechnik/-produkte nach B3S Kapitel 6.5



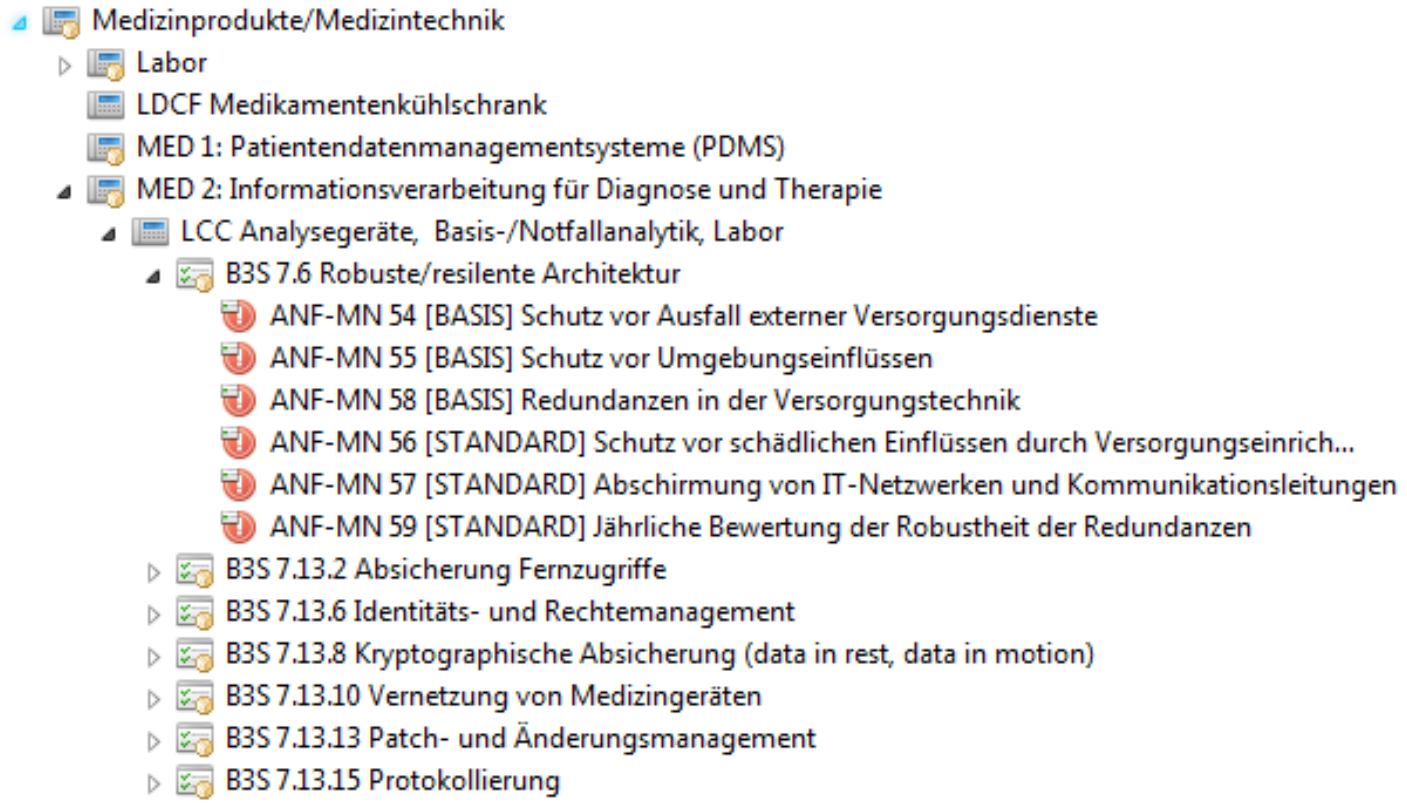
Schnittstelle KRITIS / emtec Katalog Medizintechnik

- Medizinprodukte/Medizintechnik
  - Labor
    - LDCF Medikamentenkühlschrank
    - MED 1: Patientendatenmanagementsysteme (PDMS)
    - MED 2: Informationsverarbeitung für Diagnose und Therapie
      - LCC Analysegeräte, Basis-/Notfallanalytik, Labor
      - LCDB POCT-Blutzuckeranalysegerät
      - LECA Bilderfassungssystem
      - WBD Infusionsapparate
      - WBDQ Dockingstation für Infusionsapparate
      - WCA Neurologie-Messgeräte
      - WCB Elektrokardiographen
      - WCDJ Gefäßdoppler, nicht bildgebend
      - WCH Lungenfunktions-Messgeräte
      - WCQE Drucker, medizinischer Einsatz
      - WCQK Rechnereinheit, medizinischer Einsatz
      - WCSB Elektrophysiologischer Messplatz, kardiologisch
      - WCSC Elektrophysiologisches Mappingsystem, kardiologisch
      - WF Bildgebende Systeme
      - WGAB Afterloadinggerät
      - WGDB Linearbeschleuniger
      - WGDH Tomotherapiegerät
      - WJUC Navigationssystem, chirurgisch
    - MED 3: Telemedizinische Systeme / Telemetriesysteme
      - WDKF Telemetrieanlage

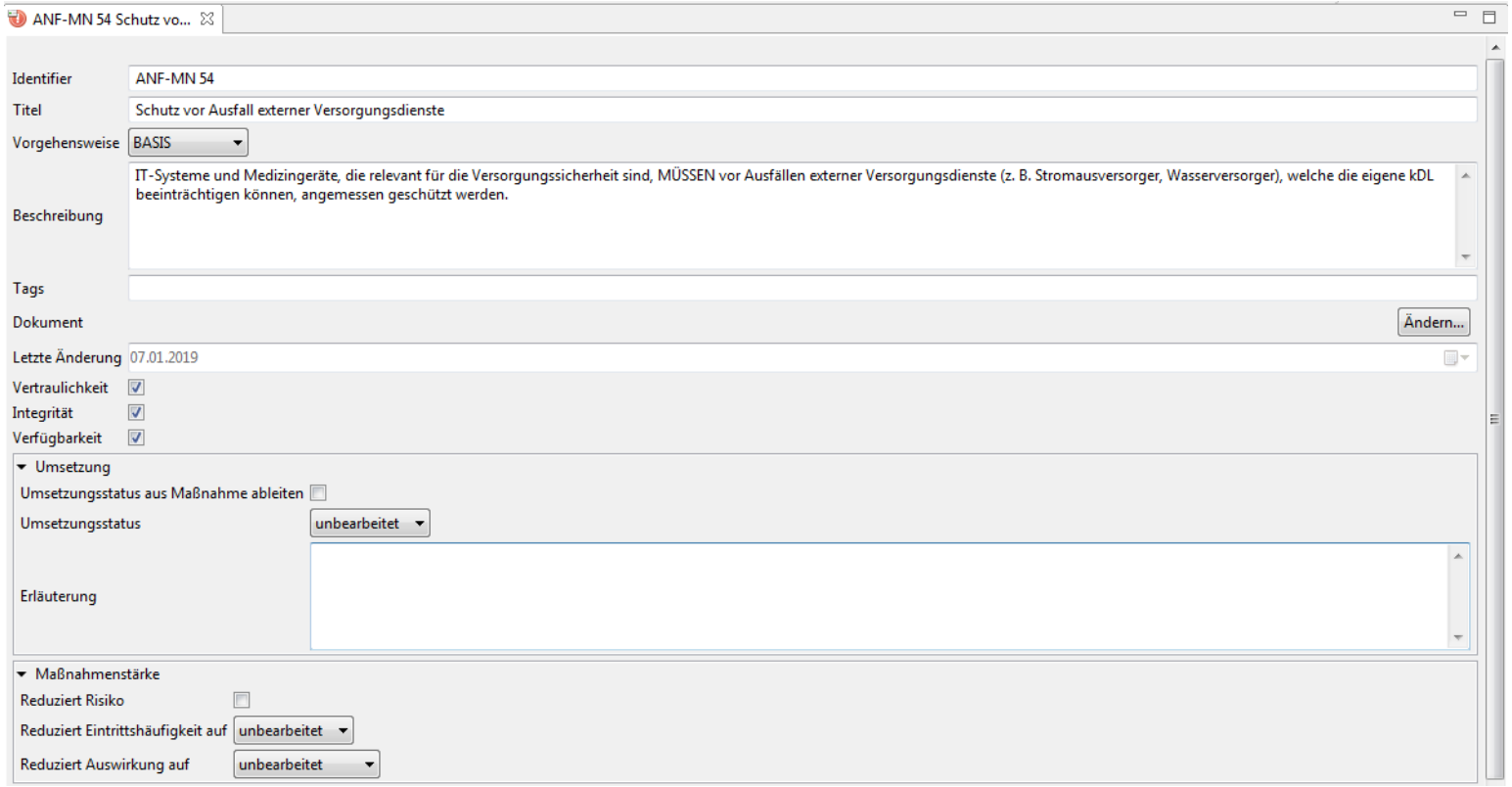
MT/-produkte – ANF-MN nach B3S Kapitel 7 (direkt)

- 6.5.4 Medizintechnik/-produkte
  - MED 1 Einsatz von Patientendatenmanagementsystemen (PDMS)
    - B3S 7.6 Robuste/resilente Architektur
      - ANF-MN 54 [BASIS] Schutz vor Ausfall externer Versorgungsdienste
      - ANF-MN 55 [BASIS] Schutz vor Umgebungseinflüssen
      - ANF-MN 58 [BASIS] Redundanzen in der Versorgungstechnik
      - ANF-MN 56 [STANDARD] Schutz vor schädlichen Einflüssen durch Versorgungseinrich...
      - ANF-MN 57 [STANDARD] Abschirmung von IT-Netzwerken und Kommunikationsleitungen
      - ANF-MN 59 [STANDARD] Jährliche Bewertung der Robustheit der Redundanzen
    - B3S 7.13.2 Absicherung Fernzugriffe
    - B3S 7.13.3 Härtung und sichere Basiskonfiguration der Systeme und Anwendungen
    - B3S 7.13.6 Identitäts- und Rechtemanagement
    - B3S 7.13.7 Sichere Authentisierung
    - B3S 7.13.13 Patch- und Änderungsmanagement
    - B3S 7.13.15 Protokollierung
    - B3S 7.13.18 Softwaretests und Freigaben
    - B3S 7.13.19 Datenschutz
  - MED 2 Informationsverarbeitung für diagnostische bzw. therapeutische Zwecke
  - MED 3 Telemedizinische Systeme / Telemetriesysteme
  - MED 4 patientengebundene Alarmierungssysteme
  - MED 5 Steuerung der Instandhaltung medizintechnischer Anlagen für Diagnostik un...
  - MED 6 Instandhaltung und Austausch von Einzelgeräten (z. B. "Kleingeräte", wie ...

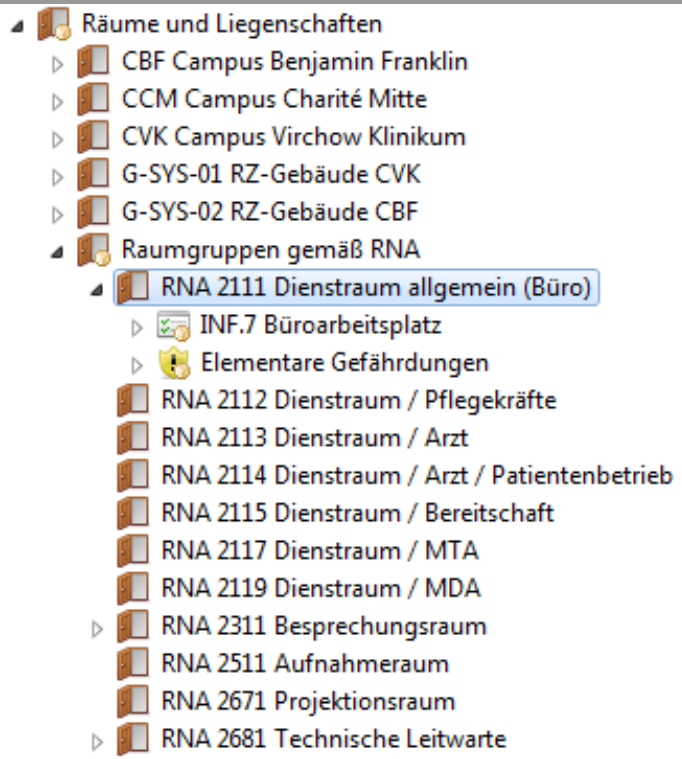
MT/-produkte – ANF-MN nach B3S Kapitel 7 (indirekt)



Medizintechnik/-produkte – Umsetzungsstatus nach B3S



Schnittstelle KRITIS / RNA*



*Raumnutzungsarten (RNA) sind eine weitere Aufteilung der zweistelligen DIN 277 Teil 1 und 2

Wiederverwendbarkeit dokumentierter Informationen

Überwachungs-bereiche (14)	Hauptkategorien ("Kontrollziele") (35)	Sicherheitsmaßnahmen (114)	IT-Grundschutz	B3S: Anforderungen (auf Grundschutz)	B3S: Kapitel/Abschnitte	B3S: Anforderungen (auf ISO)	SDM: Maßnahmen (auf ISO)	SDM: Bausteine
1 Scope			BSI-Standard 200-2, Kapitel 1 Einleitung					
2 Normative references			BSI-Standard 200-1, Kapitel 11.1 Literaturverzeichnis					
3 Terms and definitions			BSI-Glossar der Cyber-Sicherheit,					
4 Context of the organization	4.1 Understanding the organization and its context		BSI-Standard 200-2, Kapitel 3.2.1 Ermittlung von Rahmenbedingungen ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie					
	4.2 Understanding the needs and		BSI-Standard 200-2, Kapitel 3.2 Konzeption und Planung des Sicherheitsprozesses					
	4.3 Determining the scope of the information security management system		BSI-Standard 200-2, Kapitel 3.3.4					
	4.4 Information security management system		BSI-Standard 200-1, Kapitel 3 ISMS-Definition und Prozessbeschreibung BSI-Standard 200-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz ISMS.1 Sicherheitsmanagement					
5 Information security policies (Informations-sicherheits-	5.1 Management direction for information security (Vorgaben der	5.1.1 Policies for information security (Informationssicherheits-richtlinien)	ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherhei BSI-Standard 200-2, Kapitel 3 Initiierung des Sicherheitsproze ISMS.1 Sicherheitsmanagement ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsr		?	ANF-MN 1, ANF-MN 167 (SOLL)	M42.18 (Sicherheitsrichtlinie)	42 **"Dokumentation"** (Maßnahmen M42.1 - M42.37)
		5.1.2 Review of the policies for information	BSI-Standard 200-2, Kapitel 3.4.5 Aktualisierung der Sicherhei					

Zusammenfassung

- Prüfkriterien im Audit:
  - Aktualität (der Dokumentationslage)
  - Nachvollziehbarkeit (der Dokumentationslage)
  - Vollständigkeit (der Dokumentationslage)
  - Korrektheit (der Dokumentationslage)

- Strukturierte Dokumentationslage, frei von Redundanzen
- Mitnutzung existierender Inventarisierungen
- Skalierbarkeit / Nachnutzung der dokumentierter Informationen