Hosp.DO.IT
Hospitalgemeinschaft

Heute geht es um die

Network & Information Security Directive-2 (NIS2)

der Europäischen Union

Was sind die kritischen Punkte von NIS2

Formalitäten Pflichten

- Das Krankenhaus (MVZ) ist beim BSI zu registrieren.
- Geschäftsleitung muss sich kontinuierlich schulen lassen und dafür Nachweis beibringen.
- Ein ISMS das NIS2 genügt ist zu institutionalisieren.
- Geschäftsleitung hat Institutionalisierung zu überwachen.
- Schadensfälle sind BSI, Gesellschafter und der Öffentlichkeit zu melden – mind. WebSeite.
- Geschäftsleitung haftet mit Privatvermögen bei Pflichtverletzung. Verantwortung ist nicht delegierbar.

Haftungsrechtliche Absicherung Individuum

- Die Geschäftsführung, Vorstände und Geschäftsleitung (IKMVT, Einkauf, Apotheke, QRM, etc.) tragen eine hohe persönliche Verantwortung und haften mit Privatvermögen bei Organisationsverschulden.
- Geschäftsleitung haftet persönlich bei Datenschutzverstößen (DSGVO), Patientendatenlecks und unzureichenden Cyber- bzw. IT-Sicherheitsmaßnahmen nach NIS2
- Geschäftsleitung muss sich kontinuierlich schulen lassen und dafür Nachweis beibringen.
- Ein ISMS das NIS2 genügt ist zu institutionalisieren.

Haftungsrechtliche Absicherung des Unternehmens ➔ mittelbar Individium

- Die Geschäftsleitung hat die Institutionalisierung zu überwachen. Ist die Institutionalisierung nicht gegeben und es kommt zum Schadensfall, so wird der Versicherungsträger nicht zahlen. De facto liegt dann ein Organisationsverschulden vor.

Institutionalisierung meint

- ➔ Risikomanagementsystem (H-ISMS-Matrix)
- ➔ Business Continuity Management (H-ISMS-QBerichte)
- ➔ Cybersicherheitsstrategie (Hosp-Be-Notfall)
- ➔ Sicherer Betrieb kritischer Systeme (Hosp-Be-Notfall)
- ➔ Incident-Response-Plan & Meldungen (IHosp-Be-Notfal)
- ➔ Notfallmanager – CISO - Chief Information Security Officer (Hosp-Be-Notfall)
- ➔ Schulung der Mitarbeitenden in IT-Sicherheit & Awareness-Kampagnen (H-ISMS-Qberichte & Hosp-Be-Notfal)
- ➔ Durchführung von regelmäßigen Penetrationstests und Security-Audits (H-ISMS-Qberichte & Hosp-Be-Notfal)

Was ist für das Krankenhaus zu tun?

➔ ISMS, Lieferkettengesetz, Registrierung & BCM

Ein Informationssicherheits-Managementsystem (ISMS) ist zu institutionalisieren bzw. erweitern, siehe Lieferketten und BCM.

Im Rahmen des ISMS sind u.a. die
- ➔ Lieferketten zu prüfen bzw. weiter organisatorische Maßnahmen vorzunehmen.
- ➔ Cybersicherheitszertifikate zu prüfen und Maßnahmen zu ergreifen.

Es ist die Registrierung beim BSI vorzunehmen und sich auf kontinuierliche Kommunikation mit dem BSI und dem Landesamt einzustellen.

Es ist ein BCM (Business Continuity) aufzubauen.

Die Geschäftsführung und -leitung muss sich schulen lassen, darüber ein Zertifikat ablegen und das Zertifikat ist dem BSI vorzulegen.

Das Zertifikat bzw. die Schulungsinhalte müssen dem Gesetz genügen !

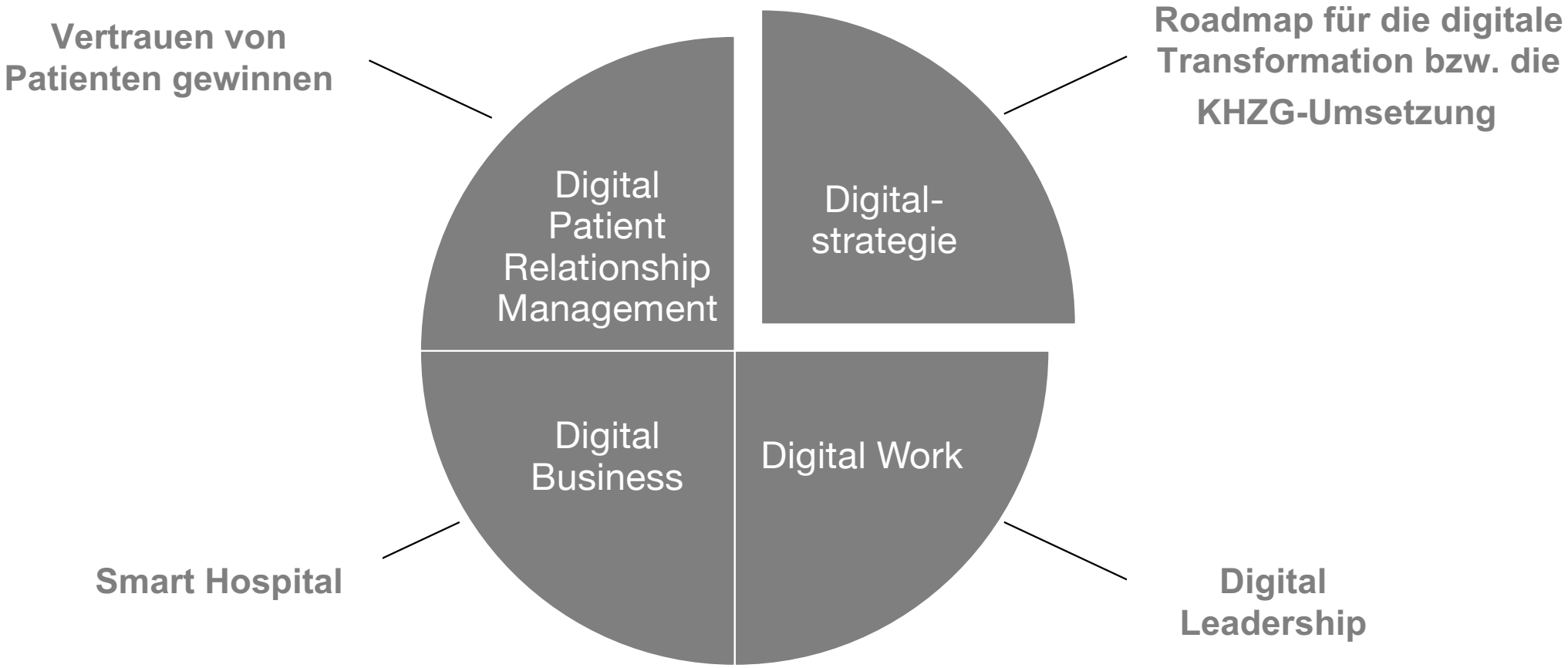
Matrix zur Digitalisierung der Organisation Krankenhaus

Strukturen, Aufgaben, Fähigkeiten, Rollen und Verantwortlichkeiten

Unternehmen Krankenhaus	Geschäftsfeld Medizin	Geschäftsfeld Digitalisierung	...	Geschäftsfeld Health-IT	Verantwortung
Vision	Regionale medizinische Exzellenz	Digitale Agenda	...	Health Information Management	Executive Board, d.h. CEO, CFO, CIO, CMO, CNO, COO plus CDO (CDO auch als Stabsstelle von CEO oder COO)
Mission	Bezogen auf gewisse med. Indikationen dominierender Taktgeber der Region	Digitale Transformation (vom Struktur- zum Prozesskrankenhaus)	...	Management der "7" CIO Kompetenzfelder inkl. Security !	CIO mit Executive Board und CIO-Führungsteam
Werte	So viel Spezialisierung wie möglich und so viel Notfallversorgung wie nötig	Einführung neuer Verhaltensweisen	…	Innovation, Flexibilität, Serviceorientierung und -standardisierung	CIO mit CIO-Führungsteam (CINO, CMIO, CNIO und CTO)
Strategie	Medizinstrategie	Digitalstrategie	...	Health-IT Strategie	CIO mit CIO-Führungsteam
Ziele (Taktische Vorgaben)	Ziele (Taktische Vorgaben)	Ziele (Taktische Vorgaben)	Ziele (Taktische Vorgaben)	Ziele (Taktische Vorgaben)	CIO mit CIO-Führungsteam
Planung & Kontrolle (Operative Maßnahmen)	Planung & Kontrolle (Operative Maßnahmen)	Planung & Kontrolle (Operative Maßnahmen)	Planung & Kontrolle (Operative Maßnahmen)	Planung & Kontrolle (Operative Maßnahmen)	CIO-Führungsteam

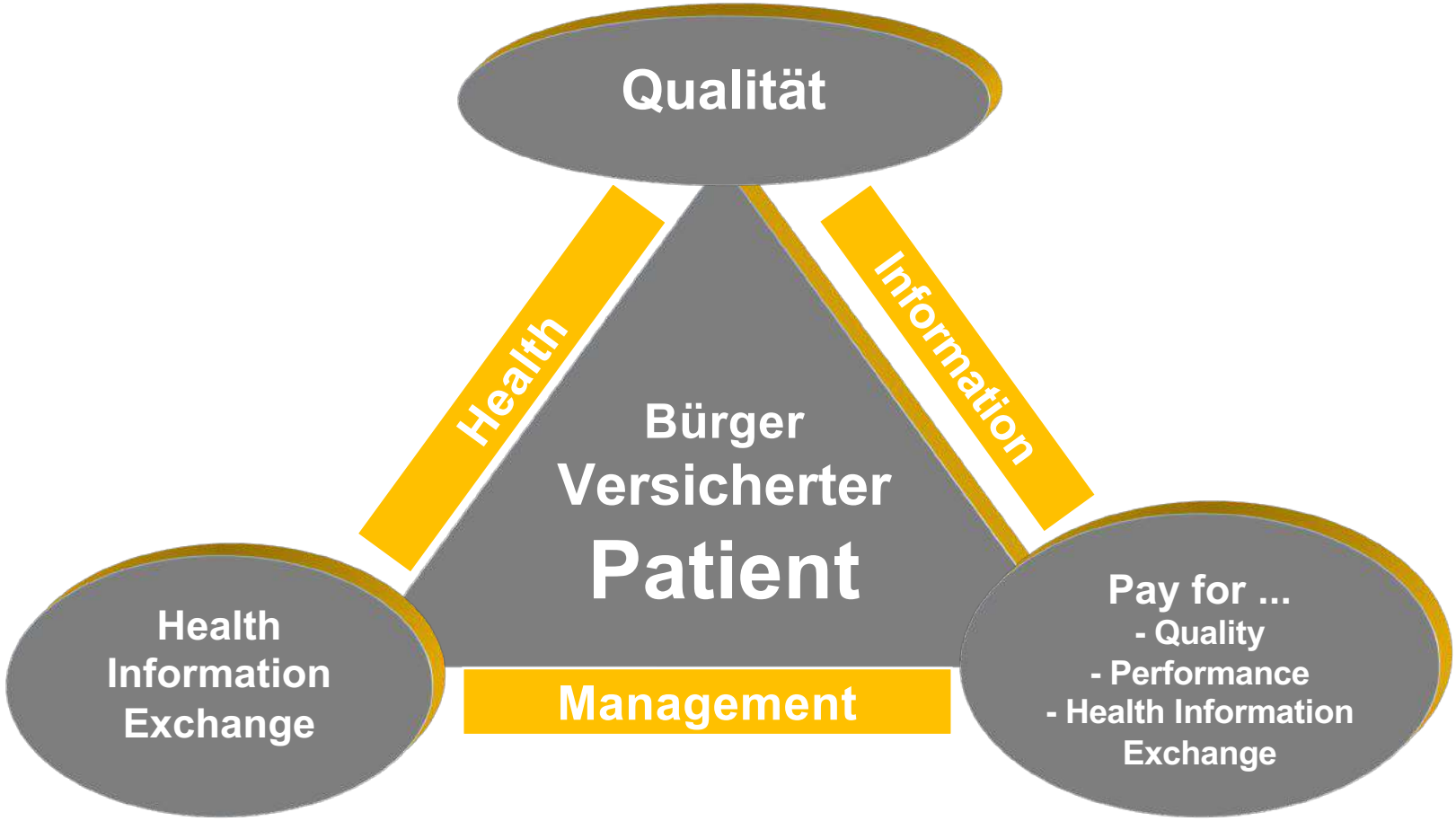
Quelle: Pierre-Michael Meier, Healthcare CIO, 2022

Ohne Digitale Agenda kein Erfolg!



Ohne Digitalstrategie kein Erfolg:

Was ist unser Managements Fokus?



Zur IT-Strategie ...

Mit skalierbarer Software- und Hardwarelandschaft unter folgenden Bedingungen die Zukunftssicherheit gewährleisten:

- **Interoperabilität und**
- **Revisionssicherheit**

für das

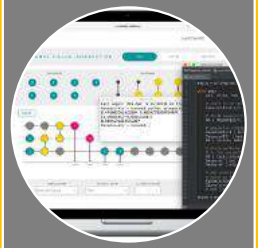
„Consumer KIS“

Erfolgreiches Management der Digital-/KHZG-Strategie mit Competence Centern

- **„Cloud“ und„KIS - Prozesse“**

Digitalisierungs- und **IT-Strategie**

Informationssicherheit Management System

							
Herr der Daten werden, Abhängigkeiten reduzieren und Best Practice integrieren	IOPs einführen und Revisionssicher-heit und Interoperabilität erreichen	Digitalisierung von Papier	Medizingeräte Output Integration	**AI & Big Data** durch Clinical Data Repository Management (Art, Umfang, Lokalisierung, etc.)	Digitale Interaktion & Kommunikation zw. Health Professional (EPA) und Patient (EGA)	Cloud Readiness oder Automatisierung durch Software	An der Digital-/ IT-Strategie ausgerichtete Nutzung von Cloud Speichern

Informationssicherheitsmanagementsystem (ISMS)

Ziel:

Sicherstellung der Informationssicherheit durch

- **strukturiertes Management,**
- **„lebende“ Dokumente** (Dokumente, die einer stetigen Veränderungen unterliegen)
- **nicht veränderbare und somit revisionssichere Dokumente** (Absicherung des Unternehmen Krankenhaus, der Geschäftsführung und des ISB)

Unser ISMS basiert auf fünf zentralen Bestandteilen.

1. **Management: Strukturierte Quartalsprotokoll**
2. **ISMS-Kompendium**
3. **Matrix Risiko- und Schutzbedarfsfeststellung**
4. **Datenschutzkonzept**
5. **IT-Betriebsführungs- und Notfallhandbuch**

Das **ISMS - Informationssicherheit** Managementsystem

Sicherheitsziele
➔ Vertraulichkeit
➔ Integrität
➔ Verfügbarkeit
➔ Behandlungseffektivität
➔ Patientensicherheit

ISMS-Kompendium
mit
Links zu ...

Kernprozesse der Wertschöpfung
* Aufnahme-administrativ – elektiv
* Aufnahme-administrativ – Notfall
* Aufnahme-medizinisch – elektiv
* Aufnahme-medizinisch – Notfall
* Aufnahme-pflegerisch – elektiv
...

Datenschutzkonzept

Informationssicherheit Managementsystem mit Quartalsprotokollen

IT-Betriebsführungs- u. -Notfallhandbuch

Matrix Risiko- und Schutzbedarfsfeststellung mit Auswirkungswert zu Assets nach akt. B3S
* kritische branchenspezifische Anwendungssysteme
* Informationstechnik
* Medizintechnik/-produkte
* Kommunikationstechnik
* Versorgungstechnik

NIS2 Compliance Zertifikat

➔ **Wir sichern unsere Geschäftsführung & -leitung ab!**

Hosp.DO.IT
Hospitalgemeinschaft

Die Hospitalgemeinschaft Hosp.DO.IT *bestätigt, dass*

Namen

den Lehrgang zur NIS2-Compliance *erfolgreich abgeschlossen hat*
und wird hiermit als NIS2-Compliance Executive *anerkannt.*

NIS2compliance executive

Düsseldorf, 14.02.2025 Prof. Dr. Pierre-Michael Meier, CHCDO, CHCIO

Durch den erfolgreichen Abschluss des Lehrgangs haben die Teilnehmenden ausreichende Kenntnisse und Fähigkeiten
- zur Erkennung und Bewertung von Risiken, Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und
- bezogen auf die Auswirkungen von Risiken, Risikomanagementpraktiken auf die Versorgung von Patientinnen und Patienten gemäß BSIG-2025 erworben.

Bundesrepublik Deutschland

Urkunde

über die Eintragung der
Marke Nr. 30 2024 108 389

Az.: 30 2024 108 389.8

NIS2-compliance executive

02.08.2024

Die Präsidentin des Deutschen Patent- und Markenamtes

Eva Schewior

München, 02.08.2024

... die teilnehmenden haben ausreichend Kenntnisse und Fähigkeiten
** zur Erkennung und Bewertung von Risiken, Risikomanagementpraktiken im Bereich der Sicherheit der Informationstechnik und*
** bezogen auf die Auswirkungen von Risiken, Risiko-managementpraktiken für die Versorgung von Patientinnen und Patienten gemäß BSIG-2025 erworben*

Initialschulung mit Zertifikat

Wort-/Bildmarkenanmeldung Patentamt

B C M

Besser Clever Managen!

➢Business Continuity Management

BCM - Begriffsklärung

BCM meint die Aufrechterhaltung der Betriebsfähigkeit:

„Fähigkeit einer Organisation die Belieferung mit Produkten und Dienstleistungen innerhalb akzeptabler Zeiträume mit zuvor festgelegter Kapazität während einer Störung fortzusetzen“
(Sicherheit und Resilienz — Business Continuity Management System — Anforderungen (ISO 22301:2019))

BSI - BSI-Standard 200-4: Hilfsmittel (bund.de)

Im Fokus des BCM liegen die **zeitkritischen Geschäftsprozesse** der Institution, die gegen **Ausfälle** abgesichert werden sollen.

Unter **BC-Lösungen** fallen alle Maßnahmen, die im Vorfeld erarbeitet und umgesetzt werden, um eine Geschäftsfortführung im Notfall zu ermöglichen.

- Leitlinie
- Beispiel für eine BCM -Organisation
- Präsentationsvorlage zur Business-Impact-Analyse
- Übersicht über Schadensszenarien und -kategorien
- Bewertungstabelle BC -Strategien
- Notfallvorsorgekonzept
- Notfallhandbuch
- Beispiel Verhaltenskodex
- Schaubild Eskalations- und Alarmierungspfade
- Geschäftsfortführungsplan (GFP)
- Wiederanlauf- / Wiederherstellungsplan (WAP / WHP)
- Übungskonzept
- BCM -Maßnahmenplan
- Grundanforderungskatalog für Outsourcing und Lieferketten

BCM - Begriffsklärung

BCM bietet Mehrwerte:

finanzielle Sicht:

- Verringerung rechtlicher und finanzieller Gefahren
- Reduzierung direkter und indirekter Kosten von Störungen

Sicht der internen Prozesse:

- Reduzierung der Störanfälligkeit
- proaktive Kontrolle der Risiken
- Erkennen und Behandeln betrieblicher Anfälligkeiten

geschäftliche Sicht:

- Unterstützung der strategischen Zielsetzungen
- Erzeugen von Wettbewerbsvorteilen
- Verbessern der Glaubwürdigkeit
- Belastbarkeit der Organisation erhöhen

Vgl. Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019

Business Continuity Management

Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das BCMS Führung und Verpflichtung zeigen, ….

(Sicherheit und Resilienz — Business Continuity Management System — Anforderungen (ISO 22301:2019))

Ein BCMS muss von der Institutionsleitung initiiert werden, weil die zu treffenden Entscheidungen weitreichende Konsequenzen haben.

BSI-Standard 200-4

Business Continuity Management

Führung und Verpflichtung- im B3S

ANF-0034 Innerhalb des B3S-Geltungsbereichs MUSS die Aufrechterhaltung der kritischen Dienstleistungen (kDL) im Störungs- sowie im Notfall sichergestellt und geeignete Maßnahmen zur schnellstmöglichen Wiederherstellung vorgesehen werden.
Hierzu SOLL ein betriebliches Kontinuitätsmanagementsystem etabliert werden.

ANF-0035 Mit der Umsetzung eines betrieblichen Kontinuitätsmanagements SOLLEN die strategischen Ziele der Organisation verfolgt werden. Die sich hieraus ergebenden spezifischen Ziele SOLL in einer Leitlinie zum betrieblichen Kontinuitätsmanagement vorgegeben werden.

ANF-0037 Wird ein Betriebliches Kontinuitätsmanagement-System zur Absicherung der kDL betrieben, MUSS dieses von der Geschäftsführung freigegeben werden

kdL: kritische Dienstleistung

Quelle: B3S V1.2

Business Continuity Management

Führung und Verpflichtung

Unternehmen sind verpflichtet

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen.

- eine rasche Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall sicherzustellen

vgl. VERORDNUNG (EU) 2016/679

Art. 32 DSGVO Sicherheit der Verarbeitung

Wie mache ich mich abhängig?

Betrachtungswinkel:

DSGVO - BCM - KRITIS

Prüfung auf die Schutzziele:

Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität

Patientensicherheit

Leistungsfähigkeit des Klinikums

Lieferketten, ausgelagerte Dienstleistungen

Logische und Phys. Netze

Aktive Komponenten

Anwendungen (Software)

Systeme

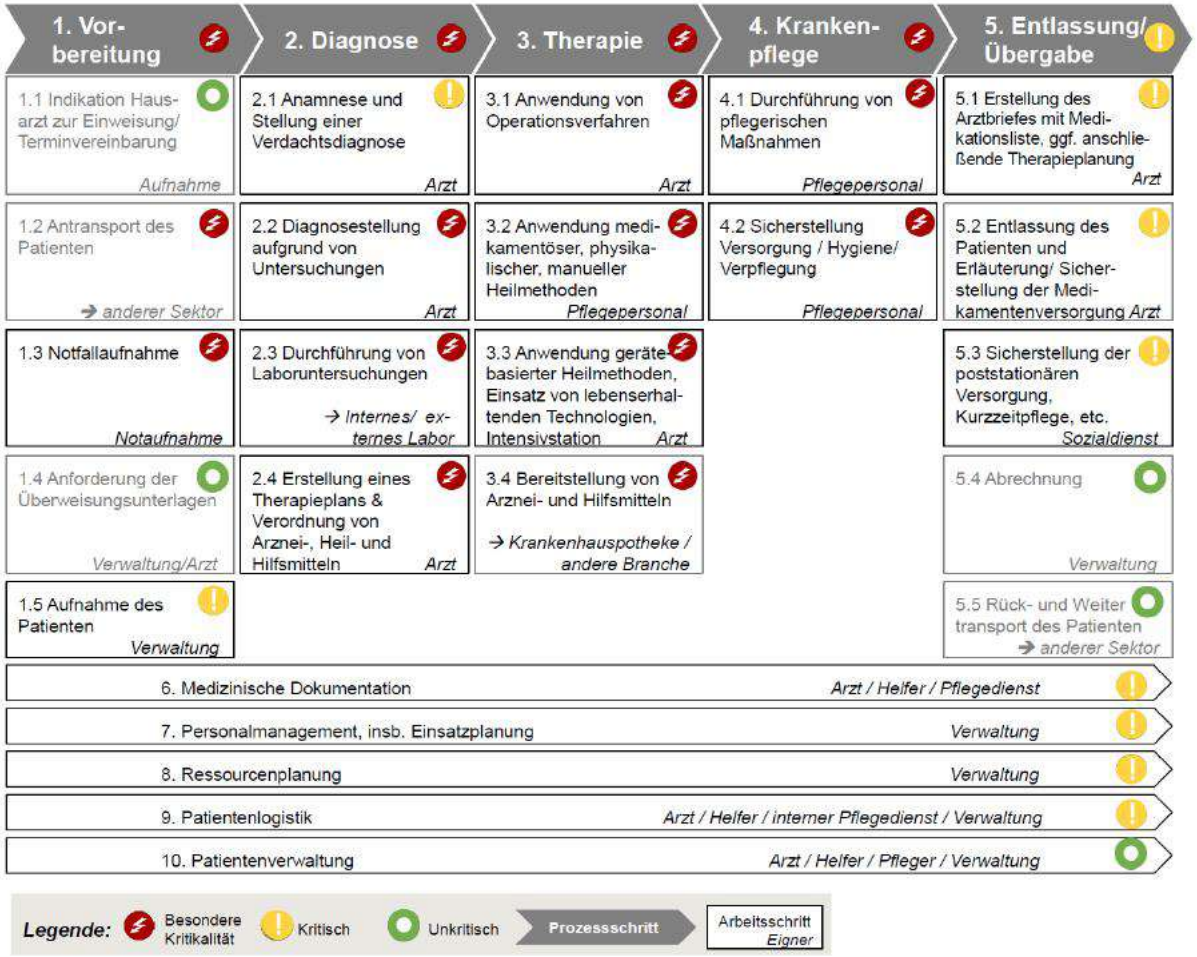
Räume

Gebäude

z.B.
Radiologie-PACS
Spracherkennung
Telefonie
Fax
Trinkwasser
Vollentsalzung

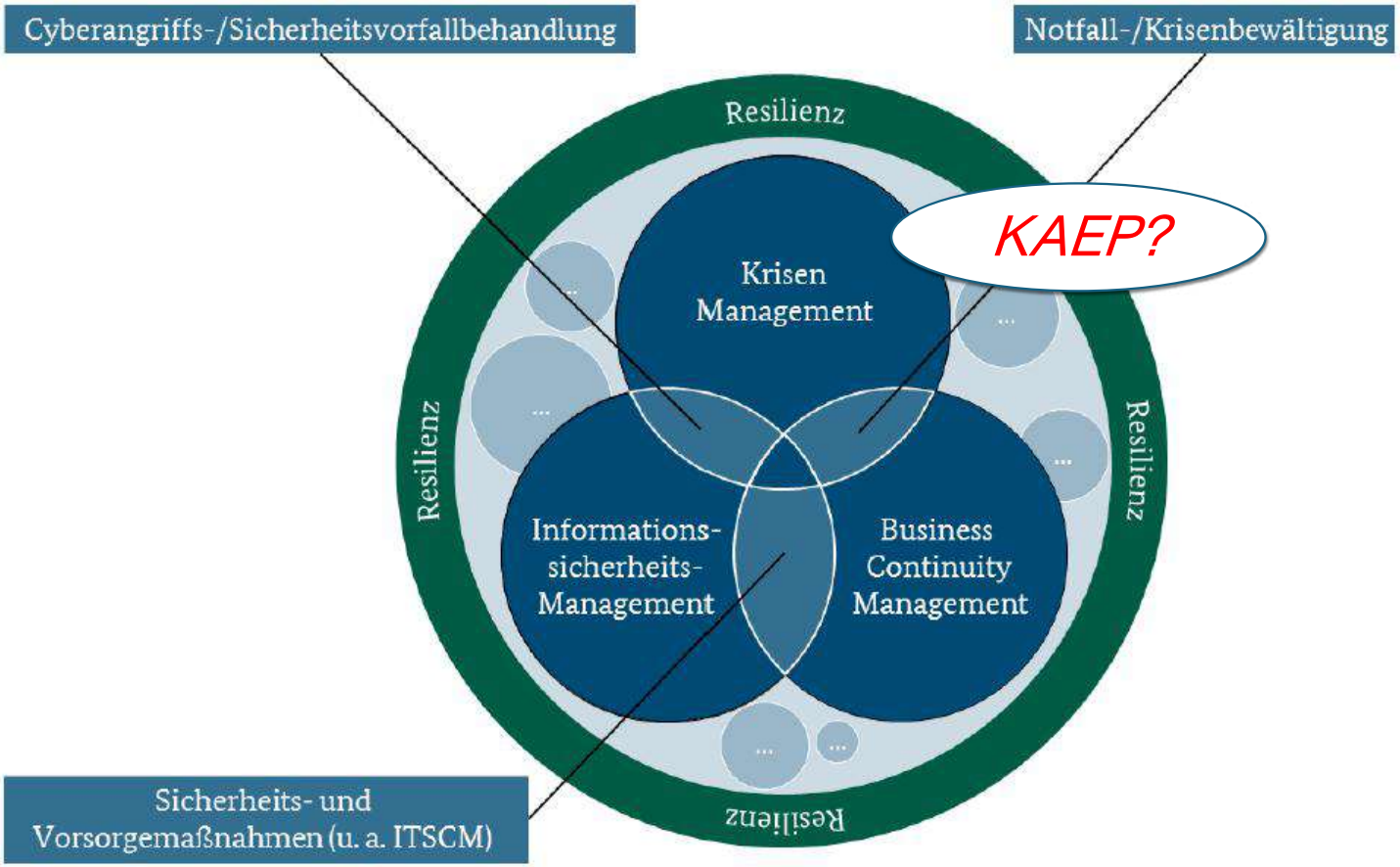
Dokumentation
z.B. in
- Verarbeitungsverzeichnis
- Inventarisierungssoftware
- „Werteverzeichnis“
- Prozesslandkarte

Wie mache ich mich abhängig?



(KRITIS- Sektorstudie Gesundheit 2016)

BCM - Begriffsklärung



Quelle: BSI Standard 200-4

Notfallvorsorge:
Vermeidung/Verringerung von Risiken

Notfallbewältigung:
Konkrete Reaktionen bei Eintritt von Notfällen

BCM und TOM

Wer ist dieser TOM?

Technisch-organisatorische Maßnahmen sollen den Schutz personenbezogener Daten sicherstellen sollen

Technisch-organisatorische Maßnahmen werden als „TOM“ oder „TOMs“ abgekürzt.
In Artikel 32 der DSGVO werden bereits Beispiele technisch-organisatorische Maßnahmen aufgelistet.

TOMs dienen auch als Nachweis der Einhaltung der DSGVO, weswegen eine schriftliche Dokumentation obligatorisch ist (Art. 24 Abs. 1 DSGVO).

➢**Mehrwerte durch in der Vorbereitung auf Notfälle und Krisen!**

Definitionen Störung, Notfall und Krise

(Eigene) Definitionen kommuniziert?

Business Continuity Management

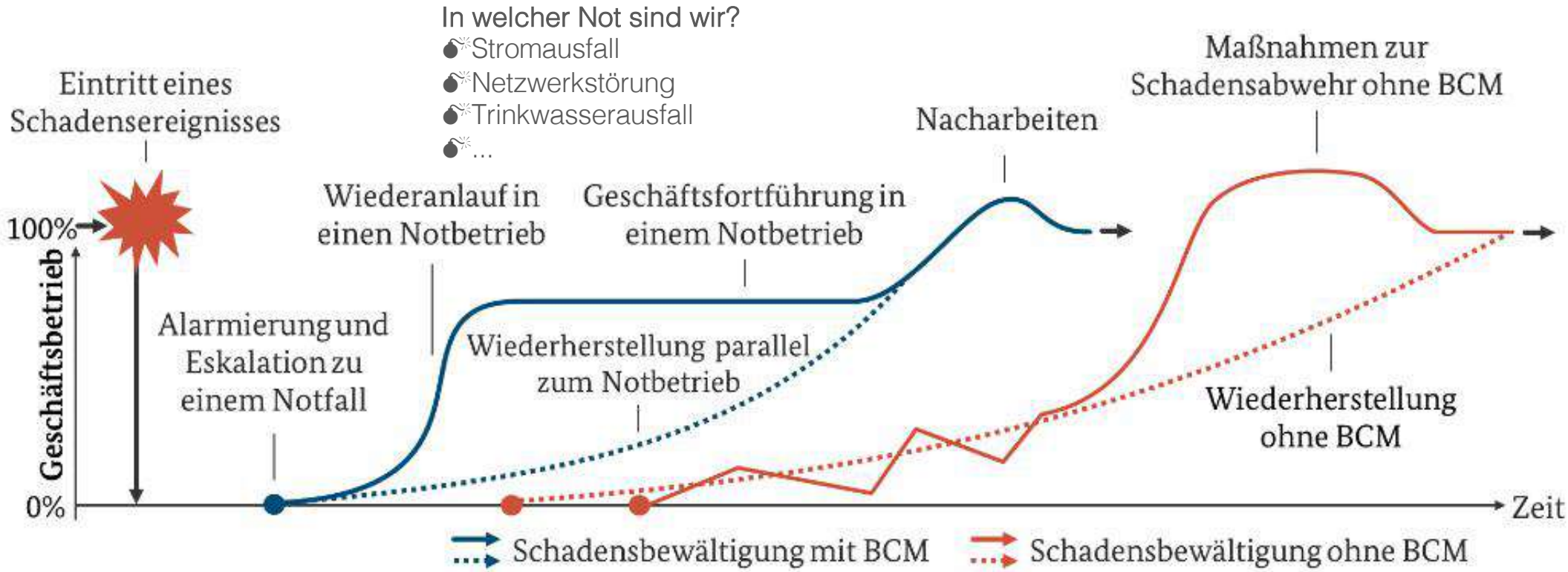
Eskal

Störung

- Betriebliche Unterbrechung
- Innerhalb des Normalbetriebs behebbar (keine Notfallpläne erforderlich)
- Keine BAO erforderlich

(Quelle: BSI Standard 200-4)

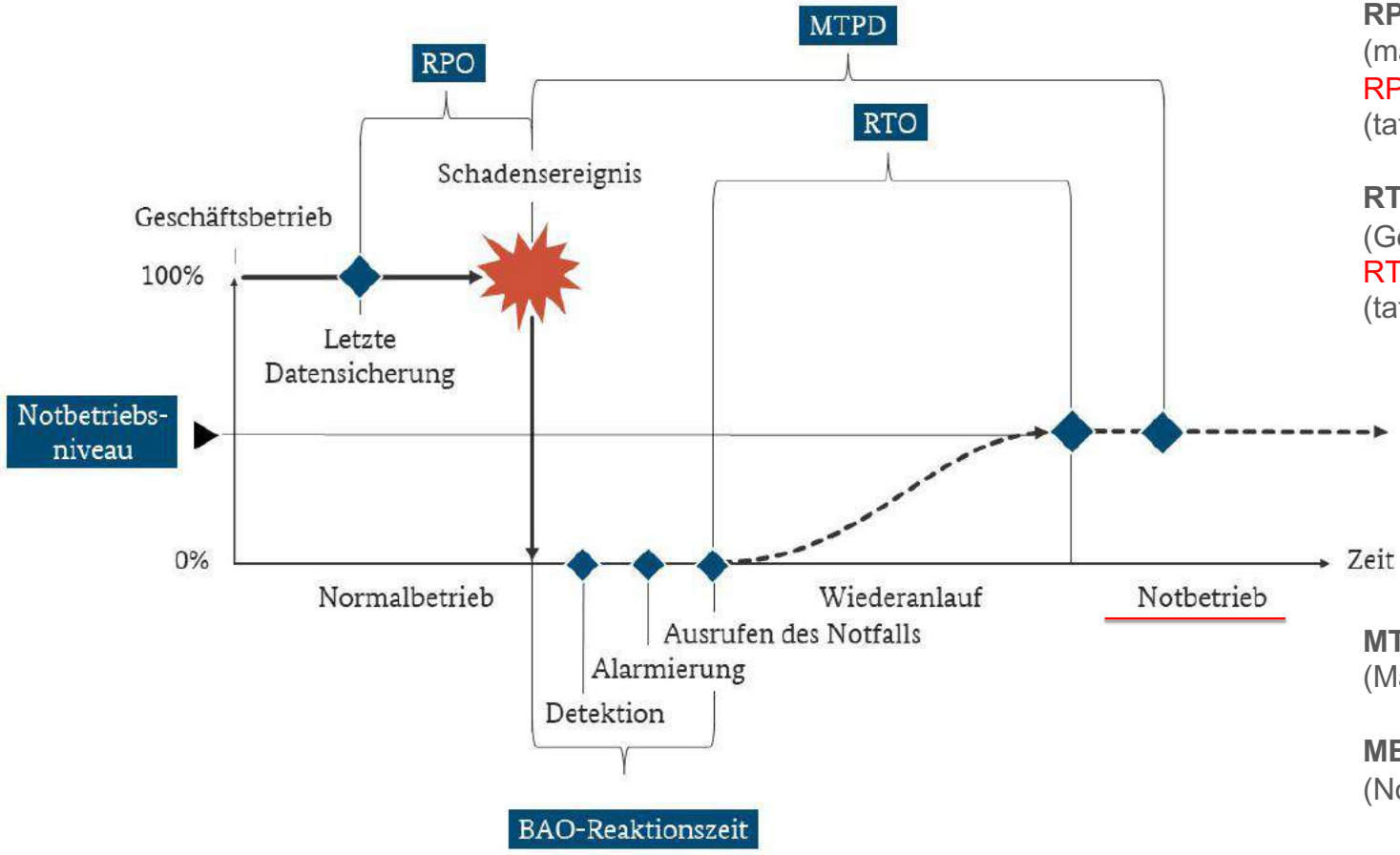
Wiederanlauf und Wiederherstellung



(Quelle: BSI Standard 200-4)

Wiederanlauf und Wiederherstellung

Wichtige Kennzahlen



RPO: Recovery Point Objective
(maximal zulässiger Datenverlust mzD)
RPA: Recovery Point Actual
(tatsächlicher Datenverlust)

RTO: Recovery Time Objective
(Geforderte Wiederanlaufzeit, WAZ)
RTA: Recovery Time Actual
(tatsächliche Wiederanlaufzeit)

MTPD: Maximum Tolerable Period of Disruption
(Maximal Tolerierbare Ausfallzeit, MTA)

MBCO: Minimum Business Continuity Objective
(Notbetriebsniveau)

Festlegung relevanter Parameter Beispiel MTA

Untragbarkeitsniveau im B3S

Klasse 1: Ausfall der Systeme kann nur kurzzeitig kompensiert werden
Klasse 2: Ausfall der Systeme kann mittelfristig kompensiert werden
Klasse 3: Ausfall der Systeme kann längerfristig kompensiert werden

Für diese Systemklassen sollen differenzierte Anforderungen entsprechend der individuellen Kritikalität definiert werden.

Die Bewertung der Kritikalität eines Systems in den Bereichen Informationstechnik, Medizintechnik, Kommunikationstechnik und Versorgungstechnik erfolgt zunächst auf Grundlage der Zeitspanne, in der nach Ausfall des Systems noch keine relevante Einschränkung der medizinischen Leistungserbringung zu erwarten ist.

- Eigene Definition **erforderlich**

Branchenspezifischer Sicherheitsstandard „Medizinische Versorgung“, v1.2

Schulung und Training

Erforderlich auf allen Ebenen und für alle Berufsgruppen

Mindestens zu den Aspekten:

- Ersatzverfahren (Notbetrieb)	: Anwender
- Notfallkonzepte	: Technik
- BIA	: Führungs- und Leitungspersonen
- Stabsarbeit :	: Klinikums Einsatzleitung (Krisenstab)
- alle Aspekte	: Institutionsleitung

Vielfältige Vermittlungsmöglichkeiten

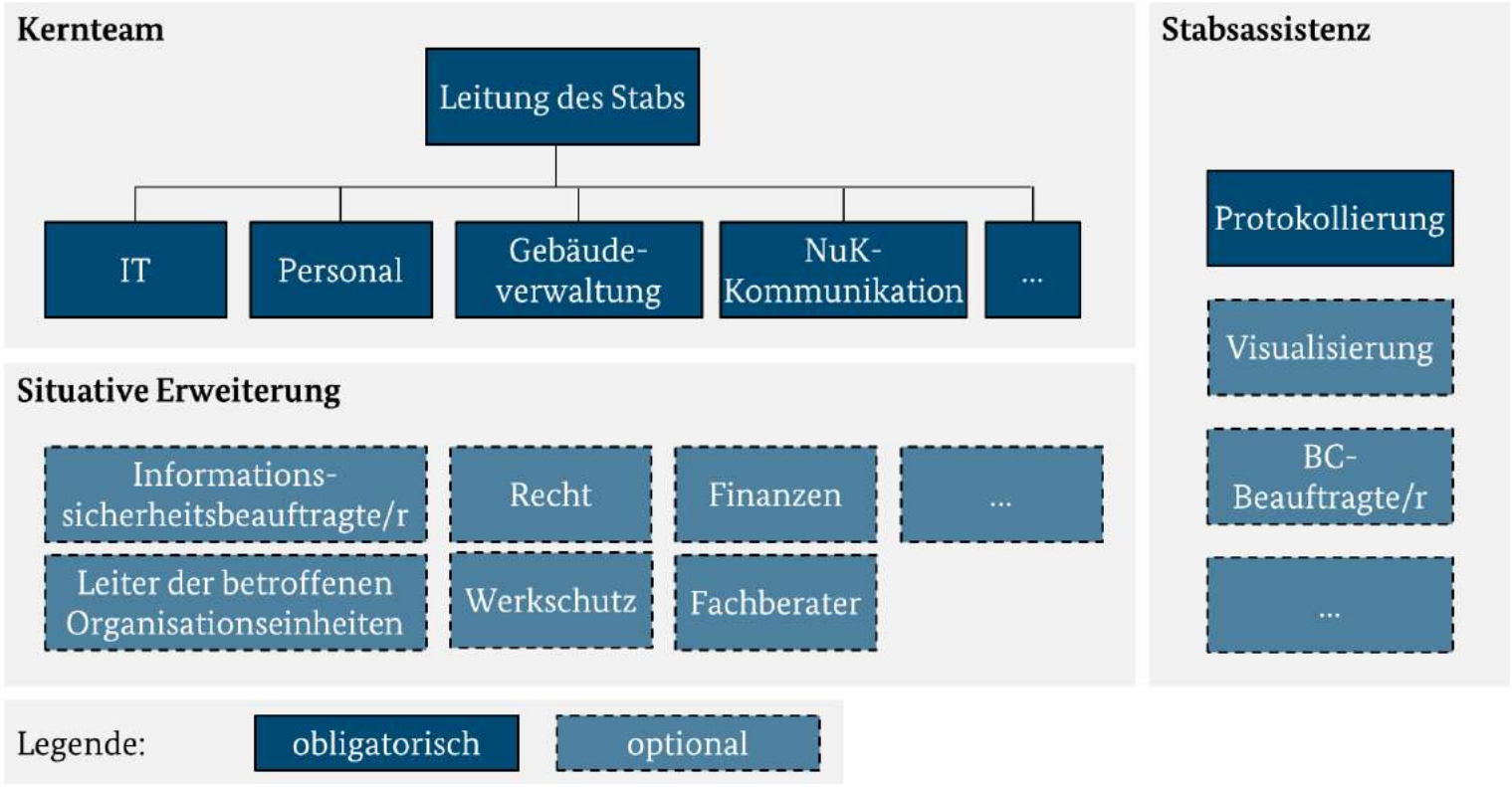
- Online/Präsenz
- Unterweisungen – Workshops – Kampagnen
- Übungen verschiedenen Umfangs

Interne – externe Vorbereitung und Durchführung

Quelle: BBK Webinar Risikoanalyse und KRITIS 29.11.2024

Schulung und Training

Bedarf in der Führungsebene:



Business Continuity Management, Abb. 23 S. 101, Hrsg. BSI, 2023, ISBN (Print): 978-3-8462- 1518-0

BCM – Kommunikation – im B3S

ANF-0041 Für diejenigen Kern- und Unterstützungsprozesse mit hohem Schadenspotenzial MÜSSEN **Geschäftsfortführungspläne** verfügbar sein, die Notfall- und Wiederanlaufpläne umfassen. (…)
ANF-0042 Die Notfallpläne MÜSSEN allen beteiligten Mitarbeitern zur Verfügung stehen. Sie SOLLEN Lieferanten, Dienstleistern und Dritten ebenfalls zur Verfügung gestellt werden, wenn dies im Rahmen der Notfallmaßnahmen erforderlich oder sinnvoll ist.
ANF-0043 Die im Notfall zu verwendenden **Kommunikationswege** (Alarmierungspläne) MÜSSEN festgelegt sein.
ANF-0044 Alarmierungspläne MÜSSEN durch die am jeweiligen Prozess beteiligten Mitarbeiter nachweislich zur Kenntnis genommen werden und diesen stets zur Verfügung stehen. Sie SOLLEN Lieferanten, Dienstleistern und Dritten ebenfalls zur Verfügung gestellt werden, wenn dies im Rahmen der Alarmierungspläne erforderlich oder sinnvoll ist.
ANF-0045 Es SOLLEN regelmäßig **Notfallübungen** durchgeführt werden. Diese MÜSSEN an der Kritikalität der Prozesse und Systeme ausgerichtet sein.

Quelle: BBK Webinar Risikoanalyse und KRITIS 29.11.2024

BCM – Kommunikation BSI 200-4

Für die NuK-Kommunikation sollten im Vorhinein verbindliche Regeln für folgende Aufgaben definiert und dokumentiert werden:

- interne Kommunikation (Was dürfen oder müssen die Mitarbeitenden wann erfahren?)
- externe Kommunikation durch Mitarbeitende (Was dürfen die Mitarbeitenden wann und wie gegenüber der Presse und in sozialen Medien äußern und was nicht?)
- externe Kommunikation durch Rolle Kommunikation (Was soll die Rolle Kommunikation wann und wie gegenüber der Presse und in sozialen Medien bekannt geben?)
- Regelungen für den Kontakt mit Polizei und anderen Behörden sowie Hilfsorganisationen
- Meldepflichten der Institution, die sich aus einem Notfall ergeben
- Regelungen zum Medienmonitoring

(NuK= Notfall und Krisen)

Business Continuity Management, S. 139, Hrsg. BSI, 2023, ISBN (Print): 978-3-8462- 1518-0

BCM – Kommunikation BSI 200-4

Folgende Anforderungen an die Kommunikation sollten eingehalten werden:

- Ausfallsicherheit der Kommunikationsmittel (z. B. Notstrom)
- Redundanz der Kommunikationsmittel (z. B. Ersatz-TK-Anlage)
- Schutz der vertraulichen Kommunikation
- Eingrenzung und Aktualität der Nutzungsberechtigungen
- Festlegung der Kommunikationskanäle
  (Social Media, Mitarbeiter-App, E-Mail, Chat, Fax, ..)
- Festlegung der Medienformate
  (Pressemitteilung, Pressekonferenz, Stellungnahme auf der Webseite, Post auf SM, …)

Business Continuity Management, S. 140, Hrsg. BSI, 2023, ISBN (Print): 978-3-8462- 1518-0

BCM – Kommunikation ISO 22301

8.4.3.1 Die Organisation muss Verfahren dokumentieren und aufrechterhalten zu folgenden Punkten:

- **Was** wird **Wann** mit **Wem** und **Wie** kommuniziert?
  - intern und extern (nicht nur verpflichtende Meldewege)
- Wie ist die **Verfügbarkeit der Kommunikationsmittel** auch im Störungsfall sichergestellt?
- Welche Regelungen greifen in der Beantwortung von Fragen der **Medien**?
- Wie erfolgen die **Aufzeichnung** zu Störung und Störungsbehandlung?
- Wie werden **Mitteilungen** interessierter Parteien entgegengenommen?
- Wie erfolgt die Koordination und Kommunikation zwischen mehreren Organisationen?

Quelle: BBK Webinar Risikoanalyse und KRITIS 29.11.2024

Die goldene Regel des BCM

Am Ende wird alles gut.

Wenn noch nicht alles gut ist,
sind wir noch nicht am Ende

Die Prüfer Perspektive

Fokus: Besteht in meinem KH eine "NIS2-Compliance"

1. Herausforderung
➔ Gibt es einen dokumentierten Prozess ?

2. Herausforderung
➔ Wird der Prozess gelebt (was bedeutet leben) ?

3. Herausforderung
➔ Ist der Prozess nachhaltig (was bedeutet nachhaltig) ?

4. Herausforderung
➔ Ist der Prozess gut (was bedeutet gut) ?

5. Herausforderung
➔ Kann sich die Organisation Krankenhaus auf den Prozess verlassen ?

6. Herausforderung
➔ Hat der Prozess Sollbruchstellen ?

7. Herausforderung
➔ Welche potentiellen Fehler müssen abgeklärt werden ?

Herausforderung und Aufgabe

Wie im **Gliederungspunkt** "Digitalisierungs- und IT-Strategie zum ISMS" aufgezeigt, hat die Hospitalgemeinschaft bei der **Einführung und Verwendung von Managementsystemen unmittelbar**

- **das Individuum und seine haftungsrechtliche Absicherung im Blick und**
- **das Unternehmen Krankenhaus und die Institutionalisierung des jeweiligen Managementsystems im Blick.**

HERAUSFORDERUNG bei der Messung des Grades der Institutionalisierung:

- Immer wenn es nicht nur um die Einführung, sondern auch um die Verwendung von Managementsystemen geht, geht es automatisch um den **Institutionalisierungs- oder Umsetzungsgrad** und somit darum, ob im **Schadensfall** ein **Organisationsverschulden der Geschäftsführung** vorliegt.
- **Für den Gesellschafter eines Krankenhauses liegt das Organisationsverschulden der Einfachheit halber dann vor, wenn der Versicherungsträger nicht zahlt.**
- **Aus dem unmittelbaren Risiko für das Unternehmen ist dann wieder ein unmittelbares Risiko des Individuums bzw. der Geschäftsführung geworden. Im Fall von NIS2 der Geschäftsleitungen.**

AUFGABE der AG ISMS der Hospitalgemeinschaft:
Auswahl eines **Tools, was nicht "nur" zur Einführung und der Verwendung** von Managementsystemen geeignet ist, **sondern auch zum Controlling**, **Messung der Umsetzung** und **Erreichung von Verbesserungenmaßnahmen**.

Auswahl des MITO-Modells

AUSWAHL der AG ISMS der Hospitalgemeinschaft:
Ausgewählt wurde das MITO-Modell:

5 MITO-Modellsegmente	PDCA Regelkreismodell
Management (Führungsvorgaben)	**Act (1)**
Input (Eingaben)	**Plan**
Transformation (Umsetzung)	**Do**
Output (Ausgaben)	**Check**
Management (Leitung)	**Act (2)**

Das MITO-Modell ist tatsächlich ein prozessorientierter Ansatz in den 5 Schritten
➔ „Gestaltung, Planung, Durchführung, Controlling und Verbesserung“ und
➔ verknüpft diese im Sinne des **PDCA Regelkreismodells** innerhalb
➔ der in der Tablle aufgezeigten **5 MITO-Modellsegmente**

Uns, den Mitglieder der Hospitalgemeinschaft steht für die Analyse, Diagnose, Therapie, Evaluierung und Entscheidungsunterstützung ein bewährten Werkzeug zur Verfügung, um den Umsetzungsgrad von NIS2 in unseren Organisationen zu messen und zu zertifizieren, d.h.
➔ nicht nur **NIS2 Zertifikat für das Individuum Geschäftsleitung**,
➔ sondern auch **NIS2 Zertifikat für die Organisation.**

Schaubild zum MITO-Modell

Anwendung des MITO-Modells für NIS2-Compliance-Check der Organisation

Im Rahmen einer Expertenbefragung werden in den Themenbereichen

- ISMS
- Risikomanagement
- Change-Management
- Business Continuity Management (BCM) bzw. Notfallmanagement
- Organisatorisch/Technische NIS2-Anforderungen

der Erfüllungsgrad und die Umsetzungstiefe ("Durchdringung") in und für das spezifischen Krankenhaus ermittelt.

Dabei gelten

Zurverfügungstellung			Reichweite (Wirkungstiefe)		
1	Nicht erfüllt	0%	1	Keine / unzureichende (Aus-)Wirkung	0%
2	Kaum erfüllt	25%	2	Umsetzung nur in den Kernbereichen ("kritischen Dienstleistungen")	25%
3	Teilweise erfüllt	50%	3	Umsetzung in wesentlichen Bereichen ("Unterstützungs-DLs")	50%
4	Im wesentlichen erfüllt	75%	4	Vollständige Umsetzung in der Organisation	75%
5	Voll erfüllt	100%	5	Die Umsetzung in der Organisation wird kontinuierlich geprüft	100%

Die Hosp-Do-IT-Items des NIS2-Compliance-Checks

Liste der erfragten Items

1.ISMS	
1.1	Matrix Risiko- und Schutzbedarfsfeststellungen
1.2	Datenschutzkonzept
1.3	IT-Betriebsführungs-/Notfallhandbuch
1.4	Sicherheitsziele und Kernprozesse
1.5	Organisation der Informationssicherheit/Steuerungsgremium

2.Risikomanagement	
2.1	Risikoanalyse
2.2	Gefährdungsübersicht
2.3	Risikoeinstufung
2.4	Risikobehandlung

3.Change-Management	
3.1	Request for Change
3.2	Planning & Riskmanagement
3.3	CAB approval (CAB=Change Advisory Board)
3.4	Implementation
3.5	Review
3.6	Closing

4.BCM	
4.1	Kritikalitätsanalyse
4.2	Verwundbarkeitsanalyse
4.3	Risikovergleich und -Bewertung
4.4	Maßnahmen
4.5	Check & Verbesserungspotential

5.Umsetzung/Realisierung	
5.1	Bewertung der Geschäftspartner & Beschaffungsprozess
5.2	Sensibilisierung und Schulung der Mitarbeitenden
5.3	Kryptographie und Verschlüsselung
5.4	Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit
5.5	Multi-Faktor-Authentifizierung

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Nr.	Bewertungskriterien	GG	Dimensionen		Kommentare	Quelle
			Erfüllungsgrad	Durchdringung		
1.ISMS						
1.1	Matrix Risiko- und Schutzbedarfsfeststellungen	1,00				
1.2	Datenschutzkonzept	1,00				
1.3	IT-Betriebsführungs-/Notfallhandbuch	1,00				
1.4	Sicherheitsziele und Kernprozesse	1,00				
1.5	Organisation der Informationssicherheit/Steuerungsgremium	1,00				
	C					
	∑ C/n		**0,00**	**0,00**		
2.Risikomanagement						
2.1	Risikoanalyse	1,00				
2.2	Gefährdungsübersicht	1,00				
2.3	Risikoeinstufung	1,00				
2.4	Risikobehandlung	1,00				
	C					
	ΣC/n		**0,00**	**0,00**		
3.Changemanagement						
3.1	Request for Change	1,00				
3.2	Planning & Riskmanagement	1,00				
3.3	CAB approval (CAB=Change Advisory Board)	1,00				
3.4	Implementation	1,00				
3.5	Review	1,00				
3.6	Closing	1,00				
	C					
	ΣC/n		**0,00**	**0,00**		
4.BCM						
4.1	Kritikalitätsanalyse	1,00				
4.2	Verwundbarkeitsanalyse	1,00				
4.3	Risikovergleich und -Bewertung	1,00				
4.4	Maßnahmen	1,00				
4.5	Check & Verbesserspotential	1,00				
	C					
	ΣC/n		**0,00**	**0,00**		
5.Technik						
5.1	Bewertung der Geschäftspartner & Beschaffungsprozess	1,00				
5.2	Sensibilisierung und Schulung der Mitarbeitenden	1,00				
5.3	Kryptographie und Verschlüsselung	1,00				
5.4	Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit	1,00				
5.5	Multi-Faktor-Authentifizierung	1,00				
	C					
	ΣC/n		**0,00**	**0,00**		
Skala: 1 = niedrig 5 = hoch	**Gesamt**		**0,00**	**0,00**		
			0 (0)*	**0 (0)***	* - Durchschnittlicher Wert aller Cluster	

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Nr.	Bewertungskriterien	GG	Dimensionen		Kommentare	Quelle
			Erfüllungsgrad	Durchdringung		
1.ISMS						
1.1	Matrix Risiko- und Schutzbedarfsfeststellungen	1,00	?	?		
1.2	Datenschutzkonzept	1,00				
1.3	IT-Betriebsführungs-/Notfallhandbuch	1,00				
1.4	Sicherheitsziele und Kernp					
1.5	Organisation der Informatic					
			0,00	0,00		
2.Risikomanagement						
2.1	Risikoanalyse	1,00	?	?		
2.2	Gefährdungsübersicht	1,00				
2.3	Risikoeinstufung	1,00				
2.4	Risikobehandlung	1,00				
	C					
	ΣC/n		0,00	0,00		
3.Changemanagement						
3.1	Request for Change	1,00	?	?		
3.2	Planning & Riskmanagement	1,00				
3.3	CAB approval (CAB=Change Advisory Board)	1,00				
3.4	Implementation	1,00				
3.5	Review	1,00				
3.6	Closing	1,00				
	C					
	ΣC/n		0,00	0,00		
4.BCM						
4.1	Kritikalitätsanalyse	1,00	?	?		
4.2	Verwundbarkeitsanalyse	1,00				
4.3	Risikovergleich und -Bewertung	1,00				
4.4	Maßnahmen	1,00				
		1,00				
			0,00	0,00		
		1,00	?	?		
		1,00				
		1,00				
		1,00				
		1,00				
			0,00	0,00		
			0,00	0,00		
			0 (0)*	0 (0)*	* - Durchschnittlicher Wert aller Cluster	

Erfüllungsgrad	
1	Nicht erfüllt
2	Kaum erfüllt
3	Teilweise erfüllt
4	Im wesentlichen erfüllt
5	Voll erfüllt

Umsetzungstiefe/Durchdringung	
1	Keine / unzureichende Durchdringung
2	Durchdringung nur der Kernbereiche
3	Durchdringung wesentlicher Bereiche
4	Vollständige Durchdringung der Organisation
5	Die Durchdringung der Organisation wird kontinuierlich geprüft und gemessen

- Je Item 5 konkrete Bewertungsfragen
- 2 Antworten:
  1. Erfüllungsgrad
  2. Durchdringung
- Antwortskala: 1 bis 5

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Cluster		Item		Bewertungsfragen	
1	ISMS	1.1	Organisation der Informationssicherheit/Steuerungsgremium	1.1.1	Die Ernennung und eines ISB bzw. ein CISO und die Festlegung des Aufgabengebietes ist ....
				1.1.2	Ein "Informationssicherheitsboard" etabliert...
				1.1.3	(Sicherheits-)Vorfälle werden strukturiert bearbeitet ....
				1.1.4	Die Berichtspflichten des ISB/CISO und die Berichtsform sind definiert ...
				1.1.5	Es finden regelmäßige Termine zw. ISB und Geschäftsleitung statt ...
		1.2	ISMS-Kompendium (Sicherheitsziele und Kernprozesse)	1.2.1	Eine Leitlinie zur strategischen Ausrichtung des Krankenhauses hinsichtlich eines ISMS ....
				1.2.2	Die Identifikation der Kernprozesse ist ....
				1.2.3	Die Sicherheitsziele sind beschrieben und von der Geschäftsleitung verabschiedet ...
				1.2.4	Bei Dokumenten des Kompendiums handelt es sich um gelenkte Dokument ...
				1.2.5	Das ISMS-Kompendium ist veröffentlicht und kommuniziert ....
		1.3	Matrix Risiko- und Schutzbedarfsfeststellungen	1.3.1	Die Methodik zur Risikofeststellung ist definiert und von der GF freigegeben ...
				1.3.2	Die relevanten Assetgruppen (=Risikoobjekte) sind ermittelt und dokumentiert ...
				1.3.3	Die (Risiko-)Verantwortlichen sind ermittelt und bestätigt ...
				1.3.4	Die Schutzbedarfsfeststellung der Kernprozesse ist erfolgt und dokumentiert ...
				1.3.5	Der Schutzbedarf der relevanten Assetgruppen wurde aus der Schutzbedarffsfeststellung erstellt ....
		1.4	Datenschutzkonzept	1.4.1	Der DSB ist unabhängig und weisungsfrei ...
				1.4.2	Das Datenschutzkonzept/die -richtlinie ist veröffentlicht und von der Geschäftsleitung verabschiedet
				1.4.3	Die Anfragen von Betroffenen werden nach der DSGVO strukturiert bearbeitet ...
				1.4.4	Datenschutzvorfälle werden strukturiert bearbeitet (inkl. der Meldung an die Aufsichtsbehörde) ...
				1.4.5	Der DSB ist in den informationssicherheitsprozess eingebunden ...
		1.5	IT-Betriebsführungs-/Notfallhandbuch	1.5.1	Ein IT-Betriebsführungshandbuch liegt vor ....
				1.5.2	Die relevanten Szenarien sind ermittelt und definiert ...
				1.5.3	Das Handbuch umfasst Sofortmaßnahmen, Notfallpläne und Wiederanlaufpläne ...
				1.5.4	Die Kontaktdaten der relevanten Partner liegen jederzeit vor ...
				1.5.5	Es finden regelmäßige Test und (Notfall-)Übungen bzgl. ermittelten Szenarien statt ...

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Cluster		Item		Bewertungsfragen	
2	Risikomanagement	2.1	Risikoanalyse	2.1.1	Die ISMS-Risikoanalyse ist im unternehmesweiten Risikomanagement berücksichtigt
				2.1.2	Die Risikoanalyse ist als wesentlicher Teil in das ISMS integriert ...
				2.1.3	Die Methodik zur Risikoanalyse ist beschrieben ...
				2.1.4	Die Verantwortlichkeiten bzgl. der Risikoanalyse sind beschrieben und kommuniziert ...
				2.1.5	Die Durchführung der Risikoanalyse ist überwacht ....
		2.2	Gefährdungsübersicht	2.2.1	Eine Übersicht über die allgemeinen Gefährdungen ist erstellt ...
				2.2.2	Eine Übersicht über die branchenspezifischen Gefärdungen ist erstellt ...
				2.2.3	Eine Gefährdungsanalyse (Bedrohungsprofile) ist erstellt ...
				2.2.4	Schwachstellen werden strukturiert ermittelt und dokumentiert
				2.2.5	
		2.3	Risikoeinstufung	2.3.1	Die Einschätzung hinsichtlich Eintrittswahrscheinlichkeit/Schadenshäufigkeit erfolgt durch Fachpersonal
				2.3.2	Die Einschätzung hinsichtlich Eintrittswahrscheinlichkeit/Schadenshäufigkeit folgt einem dokumentierten
				2.3.3	Die Risikoklassen/-stufen sind definiert ....
				2.3.4	Die Risikoverantwortlichen haben für ihre Risikoobjekte die relevanten Gefährdungen ermittelt
				2.3.5	Die Risikoverantwortlichen haben die Risikoklasse ermittelt
		2.4	Risikobehandlung	2.4.1	Der Risikobehandlungsplan ist beschrieben
				2.4.2	Kriterien zur Risikobehandlung, insbesondere die Akzeptanzkriterien, sind definiert ...
				2.4.3	Die Risiken werden nachvollziehbar und aussagefähig der Geschäftsführung berichtet ...
				2.4.4	Die Risikoeigentümer haben die Risikobehandlungsmaßnahmen festgelegt ....
				2.4.5	Die Geschäftsführung hat die Maßnahmen freigeben und die Überwachung organisiert...

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Cluster		Item		Bewertungsfragen	
					Marcel
3	Changemanagement	3.1	Request for Change	3.1.1	Systemänderungen werden dokumentiert, eine formelle Request-for-Change (RfC)-Erfassung ist nicht vorhanden
				3.1.2	Geplante Systemänderungen werden teilweise als RfC dokumentiert und benötigen eine formale Freigabe vor der Umsetzung.
				3.1.3	Geplante Systemänderungen in der IT werden grundsätzlich als RfC dokumentiert und durchlaufen eine definierte Genehmigungsprozedur.
				3.1.4	Alle Systemänderungen, einschließlich der Medizintechnik, werden vollständig als RfC dokumentiert und durchlaufen verpflichtend ein Freigabeverfahren.
				3.1.5	Alle technischen und organisatorischen Änderungen an kritischen Dienstleistungen (kDL) sind zwingend als RfC dokumentiert, lückenlos nachvollziehbar und unterliegen einem umfassenden und transparenten Genehmigungsprozess.
		3.2	Planning & Riskmanagement	3.2.1	Planung und Risikobetrachtung erfolgen selten und unstrukturiert.
				3.2.2	Planung und Risikobetrachtung erfolgen teilweise strukturiert und dokumentiert.
				3.2.3	Planung und Risikomanagement werden grundsätzlich bei größeren Changes systematisch durchgeführt.
				3.2.4	Planung und Risikomanagement werden umfassend bei allen IT- Betriebs- und Medizintechnik-Changes eingesetzt.
				3.2.5	Planung und Risikomanagement umfassen kontinuierliche Analysen, präventive Maßnahmen und vollständige Dokumentation für alle kritischen Dienstleistungen.
		3.3	CAB approval (CAB=Change Advisory Board)	3.3.1	Freigaben erfolgen, aber spontan ohne formelle Genehmigung.
				3.3.2	Teilweise formelle Freigaben mit Dokumentation der Genehmigungen.
				3.3.3	Formelle Genehmigungsverfahren erfolgen über ein dafür vorgesehenes Gremium. Ein Change Advisory Board (CAB) oder vergleichbares Gremium aus mindesten zwei Personen ist vorhanden.
				3.3.4	Freigaben von Systemänderungen erfolgen verläßlich und regelmäßig über das CAB und sind entsprechend dokumentiert
				3.3.5	Freigabeprozesse von Systemänderungen, die die kritische Dientsleistungen betreffen, sind vollständig transparent, nachvollziehbar und alle Genehmigungen umfassend durch das CAB dokumentiert.
		3.4	Implementation	3.4.1	Implementierung erfolgt ungeplant und nur teilweise dokumentiert.
				3.4.2	Implementierungen werden teilweise geplant und dokumentiert.
				3.4.3	Alle wesentlichen Implementierungen erfolgen geplant und dokumentiert.
				3.4.4	Alle Implementierungen erfolgen strukturiert, geplant und dokumentiert nach klar definierten Standards.
				3.4.5	Implementierungen sind vollständig standardisiert, systematisch dokumentiert und durchgängig überwacht.
		3.5	Review	3.5.1	Änderungen werden selten nach Umsetzung überprüft.
				3.5.2	Teilweise Prüfung und Dokumentation der Ergebnisse nach Implementierung.
				3.5.3	Systematische Reviews und Dokumentation erfolgen regelmäßig für relevante Änderungen.
				3.5.4	Alle Changes durchlaufen einen definierten Prozess zur Überprüfung, Abschluss und Dokumentation.
				3.5.5	Kontinuierliches Review, umfassende Dokumentation und Optimierung der Change-Prozesse für alle Änderungen.

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Cluster		Item		Bewertungsfragen	
4	BCM	4.1	Kritikalitätsanalyse	4.1.1	Organisationseinheiten, Prozesse und Systeme sind identifiziert und erfasst
				4.1.2	Kriterien und Kennzahlen zur Kritikalitätsanalyse sind vereinbart und werden eingesetzt
				4.1.3	Die Organisationseinheiten, Prozesse und Systeme werden regelmäßig einer Kritikalitätsanalyse unterzogen
				4.1.4	Die Bevorratung und Nachlieferung "kritischer Versorgungsgüter" ist verbindlich organisiert
				4.1.5	Abhängigkeiten zu an Dritten ausgelagerten Dienstleistungen/Prozesse werden beachtet
		4.2	Verwundbarkeitsanalyse	4.2.1	Richtlinien zur Verwundbarkeitsanalyse sind eingesetzt
				4.2.2	Es erfolgen regelmäßig Schwachstellenscans für die kritischen Informationstechnischen Systeme
				4.2.3	Es erfolgen regelmäßig Penetrationstests für die kritischen Informationstechnischen Systeme
				4.2.4	Die Hersteller/Dienstleister wurden/wreden verpflichtet, bekannt Schwachstellen zu melden ("Bringschuld")
				4.2.5	Es werden externe Informationsquellen hinsichtlich aktueller Schwachstellen genutzt (BSI, Heise, BfArM, usw.)
		4.3	Risikobewertung	4.3.1	
				4.3.2	
				4.3.3	
				4.3.4	
				4.3.5	
		4.4	Maßnahmen	4.4.1	Ein Krisenmanagement ist etabliert (mindestens KAEP= Krankenhausalarm- und einsatzplanung)
				4.4.2	Ein BCMS ist etabliert und mit dem KAEP organisatorisch abgestimmt
				4.4.3	Die Mitglieder des Krisenstab werden regelmäßg geschult
				4.4.4	Eine gesicherte Notfallkommukikation ist etabliert (Struktur und Kommunikationsmittel, "Wer mit wem" und "Mit
				4.4.5	Für verschiedene Szenarien sind Notbetriebsniveaus festgelegt
		4.5	Check & Verbesserungspotential	4.5.1	Audits oder Revisionen werden regelmäßig durchgeführt
				4.5.2	Übungen unterschiedlicher Komplexität (z. B. Planbesprechung, Planspiel, siehe auch Hilfsmittel BSI 200-4) und Zusammensetzung der Übenden werden geplant und durchgeführt
				4.5.3	Die BCM-Dokumente sind gelenkt und Unterlieben einer regelmäßigen Überprüfung
				4.5.4	Technische Lösungen und Betriebsmittel werden regelmäßig getestet (z. B. konkreter Ladestatus der Notfallhandys, Erreichbarkeit eines spezifischen Notfalldrucker, usw.)
				4.5.5	

Das Hosp-Do-IT NIS2-Compliance-Check

Sicht auf die auszufüllen Bewertungskriterien

Cluster		Item		Bewertungsfragen	
5	Technologie	5.1	Bewertung der Geschäftspartner & Beschaffungsprozess	5.1.1	Die Anforderungen an die Sicherheit der Lieferketten sind beschrieben
				5.1.2	Die relevanten Artikel und die zugehörigen Lieferketten sind identifiziert ...
				5.1.3	Mit den relevanten GP wurden entsprechende Vereinbarungen getroffen ...
				5.1.4	Die Sicherheitsmaßnahmen beim Erwerb, bei der Entwicklung und bei der Wartung in Bezug auf die Informationstechnik sind beschreiben und werden im Beschaffungsprozess (z. B. als LV Bestandteil) berücksichtigt
				5.1.5	Die Einbindung des ISB und/oder DSB in den Beschaffungsprozess ist regelhaft umgesetzt
		5.2	Sensibilisierung und Schulung der Mitarbeitenden	5.2.1	Vorgaben zur Auswahl geeigneter Mitarbeiter (Stichwort Führungszeugnis)
				5.2.2	Richtlinien zur Erteilung von Zugriffsberechtigungen
				5.2.3	Konzept zur Kontrolle und Überwachung von Zugriffsberechtigungen
				5.2.4	Die grundlegenden Verfahren zur Cyberhygiene sind identifiziert und beschrieben
				5.2.5	Regelmäßige Schulungen bzgl. Informationssicherheit sind etabeliert
		5.3	Kryptographie und Verschlüsselung	5.3.1	Ein Kryptographiekonzept ist erstellt und freigegeben ...
				5.3.2	Ein PKI-Architektur/eine Zertifikatsverwaltung ist etabliert
				5.3.3	Die notwendigen Fernwartungszugänge sind erfasst und auf der Basis des Kryptokonzeptes gesichert
				5.3.4	Eine Transportverschlüsselung ist realisiert
				5.3.5	Die Datenhaltung/Datenspeicherung ist verschlüsselt ...
		5.4	Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit	5.4.1	Ein "Personalmanagementkonzept" ist erstellt und freigegeben ...
				5.4.2	Der "Personal-Onboarding-Prozess" genügt dem Personalmanagementkonzept und ist überwacht ....
				5.4.3	Ein Konzept zum Zugriffsmanagement ("Rechte- und Rollenkonzept") ist erstellt und freigegeben
				5.4.4	Der Prozess zur Erteilung der Zugriffsberechtigungen ist etabliert und überwacht ....
				5.4.5	Die Einhaltung der erteilten Zugriffs, insbesondere auf personenbezogenen Daten wird kontrolliert und überwacht (Plausibilitätskontrollen) ...
		5.5	Multi-Faktor-Authentifizierung	5.5.1	Ein Konzept zur MFA ist erstellt und freigegeben ...
				5.5.2	Das MFA-Konzept ist bzgl. dem externen Mailzugängen etabliert ...
				5.5.3	Das MFA-Konzept ist bzgl. den IT-Administratoren bzw. den zentralen IT-Komponenten etabliert ...
				5.5.4	Die medizinischen Geräte sind im MFA-Konzept berücksichtigt, das MFA-Konzept ist bzgl. den Medizingeräten etabliert
				5.5.5	Das MFA-Konzept ist überwacht ....

Das Hosp-Do-IT NIS2-Compliance-Check

Bewertung Mitgliedshaus

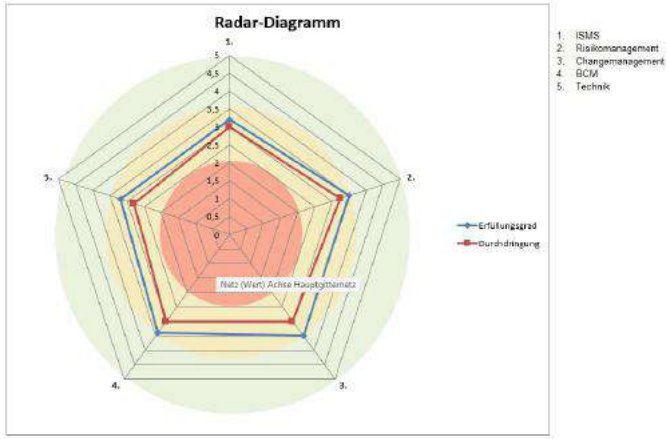
Beispiel einer Einschätzung eines Mitgliedshauses

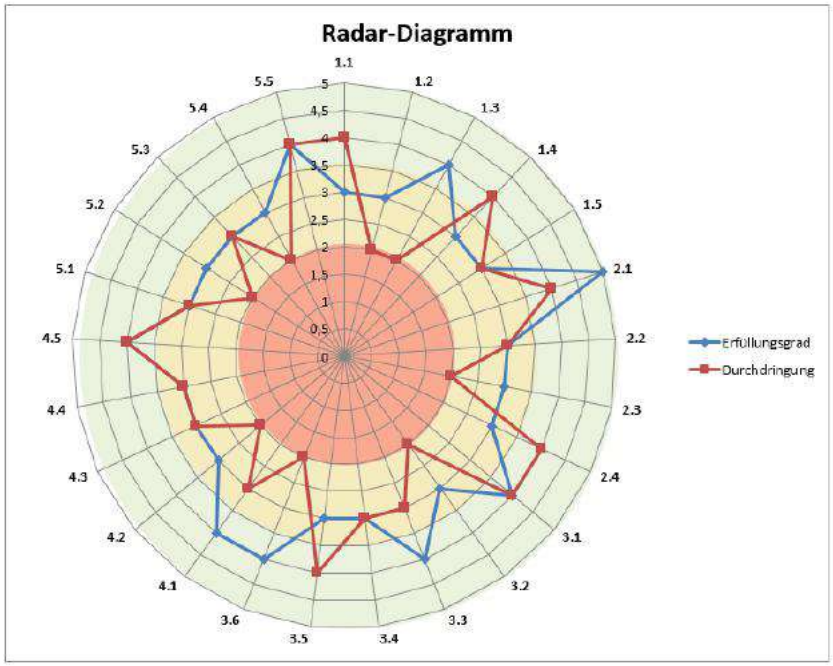
Nr.	Bewertungskriterien	GG	Dimensionen	
			Erfüllungsgrad	Durchdringung
1.ISMS				
1.1	Matrix Risiko- und Schutzbedarfsfeststellungen	1,00	4,00	2,00
1.2	Datenschutzkonzept	1,00	4,00	3,00
1.3	IT-Betriebsführungs-/Notfallhandbuch	1,00	2,00	2,00
1.4	Sicherheitsziele und Kernprozesse	1,00	4,00	3,00
1.5	Organisation der Informationssicherheit/Steuerungsgremium	1,00	4,00	3,00
	C		18,00	13,00
	∑ C/n		3,60	2,60
2.Risikomanagement				
2.1	Risikoanalyse	1,00	3,00	2,00
2.2	Gefährdungsübersicht	1,00	3,00	2,00
2.3	Risikoeinstufung	1,00	3,00	2,00
2.4	Risikobehandlung	1,00	2,00	1,00
	C		11,00	7,00
	ΣC/n		2,75	1,75
3.Changemanagement				
3.1	Request for Change	1,00	2,00	1,00
3.2	Planning & Riskmanagement	1,00	2,00	1,00
3.3	CAB approval (CAB=Change Advisory Board)	1,00	2,00	1,00
3.4	Implementation	1,00	2,00	1,00
3.5	Review	1,00	1,00	1,00
3.6	Closing	1,00	1,00	1,00
	C		10,00	6,00
	ΣC/n		1,67	1,00
4.BCM				
4.1	Kritikalitätsanalyse	1,00	3,00	2,00
4.2	Verwundbarkeitsanalyse	1,00	2,00	2,00
4.3	Risikovergleich und -Bewertung	1,00	2,00	2,00
4.4	Maßnahmen	1,00	3,00	2,00
4.5	Check & Verbesserspotential	1,00	3,00	2,00
	C		13,00	10,00
	ΣC/n		2,60	2,00
5.Technik				
5.1	Bewertung der Geschäftspartner & Beschaffungsprozess	1,00	3,00	2,00
5.2	Sensibilisierung und Schulung der Mitarbeitenden	1,00	3,00	3,00
5.3	Kryptographie und Verschlüsselung	1,00	2,00	2,00
5.4	Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit	1,00	4,00	3,00
5.5	Multi-Faktor-Authentifizierung	1,00	2,00	1,00
	C		14,00	11,00
	ΣC/n		2,80	2,20
	Skala: 1 = niedrig 5 = hoch **Gesamt**		66,00	47,00
			2,64 (2,68)*	1,88 (1,91)*

Das Hosp-Do-IT NIS2-Compliance-Check

Visualisierung der Ergebnisse der Bewertung

Die Visualisierung der Ergebnisse erfolgt im Rahmen eines Radardiagramms



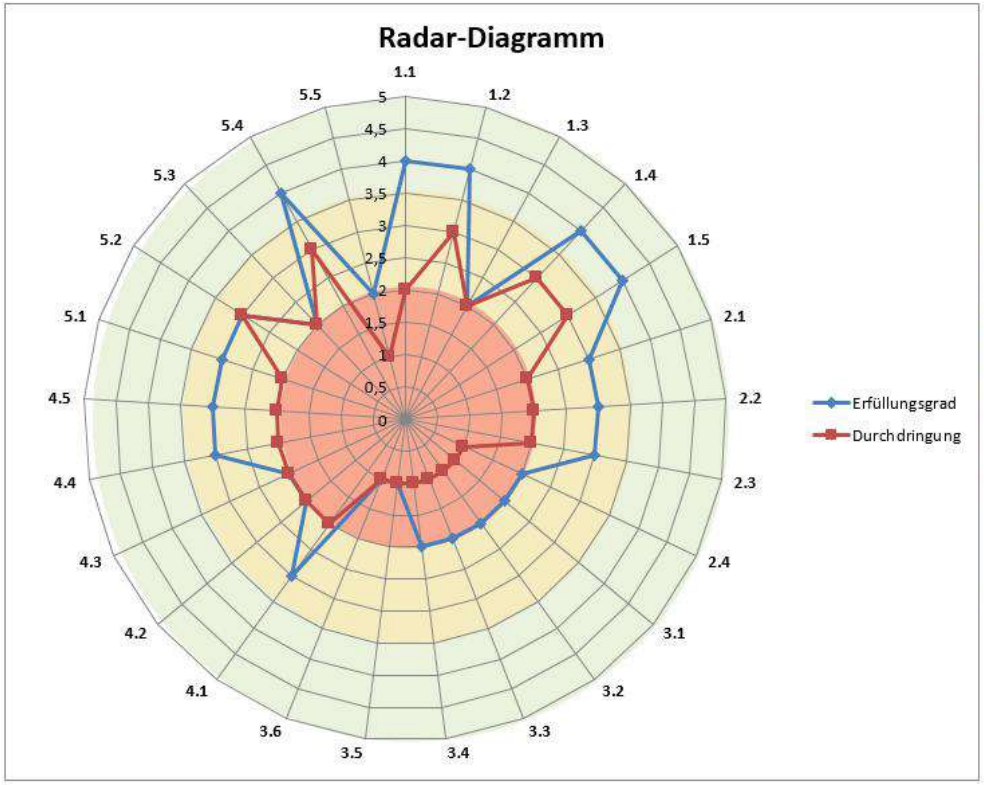


1.1 Matrix Risiko- und Schutzbedarfsfeststellungen
1.2 Datenschutzkonzept
1.3 IT-Betriebsführungs-/Notfallhandbuch
1.4 Sicherheitsziele und Kernprozesse
1.5 Organisation der Informationssicherheit/Steuerungsgremium
2.1 Risikoanalyse
2.2 Gefahrdungsübersicht
2.3 Risikoeinstufung
2.4 Risikobehandlung
3.1 Request for Change
3.2 Planning & Riskmanagement
3.3 CAB approval (CAB=Change Advisory Board)
3.4 Implementation
3.5 Review
3.6 Closing
4.1 Kritikalitätsanalyse
4.2 Verwundbarkeitsanalyse
4.3 Risikovergleich und -Bewertung
4.4 Maßnahmen
4.5 Check & Verbesserspotential
5.1 Bewertung der Geschäftspartner & Beschaffungsprozess
5.2 Sensibilisierung und Schulung der Mitarbeitenden
5.3 Kryptographie und Verschlüsselung
5.4 Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit
5.5 Multi-Faktor-Authentifizierung

Das Hosp-Do-IT NIS2-Compliance-Check

Visualisierung des Mitgliedshauses

Beispiel einer Einschätzung eines Mitgliedshauses



1.1 Matrix Risiko- und Schutzbedarfsfeststellungen
1.2 Datenschutzkonzept
1.3 IT-Betriebsführungs-/Notfallhandbuch
1.4 Sicherheitsziele und Kernprozesse
1.5 Organisation der Informationssicherheit/Steuerungsgremium
2.1 Risikoanalyse
2.2 Gefährdungsübersicht
2.3 Risikoeinstufung
2.4 Risikobehandlung
3.1 Request for Change
3.2 Planning & Riskmanagement
3.3 CAB approval (CAB=Change Advisory Board)
3.4 Implementation
3.5 Review
3.6 Closing
4.1 Kritikalitätsanalyse
4.2 Verwundbarkeitsanalyse
4.3 Risikovergleich und -Bewertung
4.4 Maßnahmen
4.5 Check & Verbesserspotential
5.1 Bewertung der Geschäftspartner & Beschaffungsprozess
5.2 Sensibilisierung und Schulung der Mitarbeitenden
5.3 Kryptographie und Verschlüsselung
5.4 Zugriffsmanagement (Rollen und Rechte) und Personelle Sicherheit
5.5 Multi-Faktor-Authentifizierung

Das Hosp-Do-IT NIS2-Compliance-Check

Projektion des Ergebnis auf einen Umsetzungsgrad

Erläuterungen zu den Stufen	
Stufe „normal“ Normierung: 1	Es wurden hinreichende Maßnahmen ergriffen, um etwaige Schadensauswirkungen auf ein begrenztes und überschaubares Ausmaß zu beschränken.
Stufe „normal mit Einschränkung“ Normierung: 2	Es wurden Maßnahmen ergriffen, um etwaige Schadensauswirkungen auf ein hinnehmbares Ausmaß zu beschränken. Bei einzelnen Maßnahmen besteht ein Verbesserungsbedarf, so dass punktuell ein höheres Ausmaß der Schadensauswirkung möglich ist.
Stufe „hoch“ Normierung: 3	Die ergriffenen Maßnahmen reichen nur dazu aus, ein etwaiges Schadensereignis auf ein beträchtliches Ausmaß zu begrenzen.
Stufe „hoch mit Einschränkung“ Normierung: 4	Die ergriffenen Maßnahmen reichen nur dazu aus, ein etwaiges Schadensereignis auf ein beträchtliches Ausmaß zu begrenzen. Es fehlen aber wesentliche Maßnahmen, so dass ein etwaiges Schadensereignisses ein bedrohliches Ausmaß annehmen kann.
Stufe „sehr hoch“ Normierung: 5	Die ergriffenen Maßnahmen sind nicht ausreichend. Ein etwaiges Schadensereignis kann ein existentiell bedrohliches, katastrophales Ausmaß annehmen.

Das NIS Compliance-Zertifikat für das Krankenhaus !

Hosp.DO.IT Hospitalgemeinschaft

Die Hospitalgemeinschaft Hosp.DO.IT *bestätigt, dass die Einrichtung*

Institution

bei der Bestimmung des NIS2-Umsetzungsgrades *die Stufe*

„normal", Normierung: 1

erreicht hat (für Details sehen sie bitte die 2. Seite).

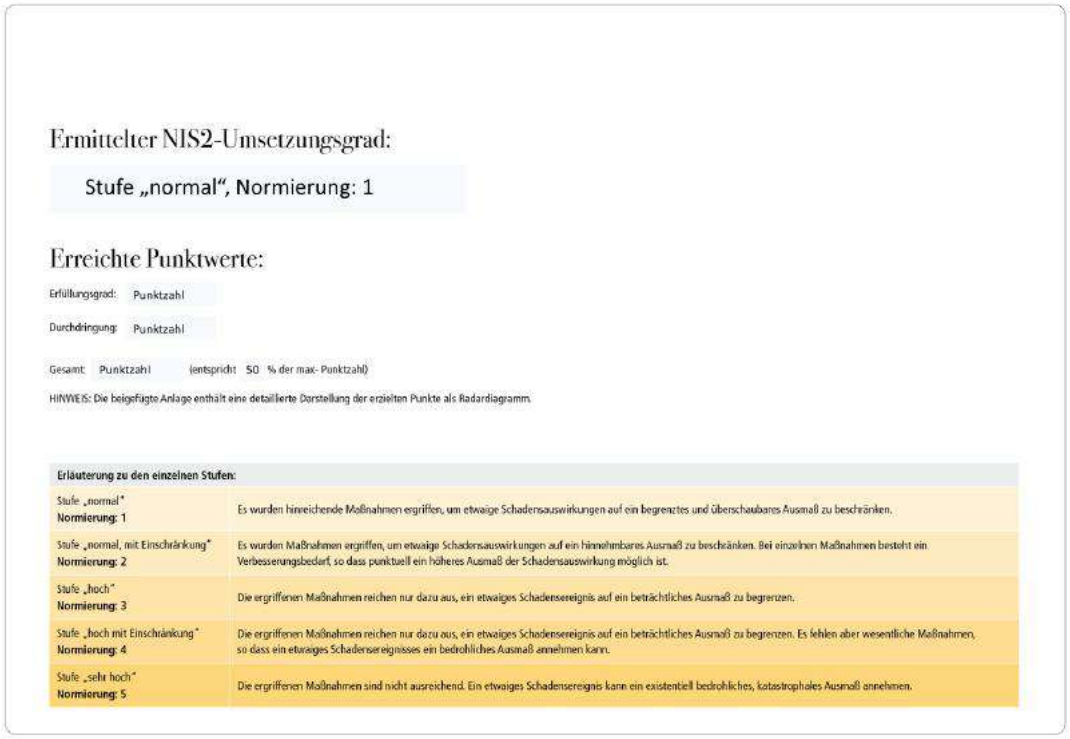
Der Einrichtung wird bestätigt eine **NIS2-Compliance Organisation** *zu sein.*

NIS2-compliance organization

Düsseldorf, 14.02.2025 Prof. Dr. Pierre-Michael Meier, CHCDO, CHCIO

Durch die Bestimmung des NIS2 Umsetzungsgrades kann nachvollzogen werden, ob die Organisation

- die Erkennung und Bewertung von Risiken, Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und
- bezogen auf die Auswirkungen von Risiken, Risikomanagementpraktiken auf die Versorgung von Patientinnen und Patienten gemäß BSIG-2025 institutionalisiert hat.



Ermittelter NIS2-Umsetzungsgrad:

Stufe „normal", Normierung: 1

Erreichte Punktwerte:

Erfüllungsgrad: Punktzahl

Durchdringung: Punktzahl

Gesamt: Punktzahl (entspricht 50 % der max. Punktzahl)

HINWEIS: Die beigefügte Anlage enthält eine detaillierte Darstellung der erzielten Punkte als Radardiagramm.

Erläuterung zu den einzelnen Stufen:	
Stufe „normal" **Normierung: 1**	Es wurden hinreichende Maßnahmen ergriffen, um etwaige Schadensauswirkungen auf ein begrenztes und überschaubares Ausmaß zu beschränken.
Stufe „normal, mit Einschränkung" **Normierung: 2**	Es wurden Maßnahmen ergriffen, um etwaige Schadensauswirkungen auf ein hinnehmbares Ausmaß zu beschränken. Bei einzelnen Maßnahmen besteht ein Verbesserungsbedarf, so dass punktuell ein höheres Ausmaß der Schadensauswirkung möglich ist.
Stufe „hoch" **Normierung: 3**	Die ergriffenen Maßnahmen reichen nur dazu aus, ein etwaiges Schadensereignis auf ein beträchtliches Ausmaß zu begrenzen.
Stufe „hoch mit Einschränkung" **Normierung: 4**	Die ergriffenen Maßnahmen reichen nur dazu aus, ein etwaiges Schadensereignis auf ein beträchtliches Ausmaß zu begrenzen. Es fehlen aber wesentliche Maßnahmen, so dass ein etwaiges Schadensereignisses ein bedrohliches Ausmaß annehmen kann.
Stufe „sehr hoch" **Normierung: 5**	Die ergriffenen Maßnahmen sind nicht ausreichend. Ein etwaiges Schadensereignis kann ein existentiell bedrohliches, katastrophales Ausmaß annehmen.

Ich beschäftige mich nicht mit dem, was getan worden ist. Mich interessiert, was getan werden muss.

Marie Curie

Take Aways Umsetzungcheck mit dem MITO-Model

1) Ready für den Versicherungsträger und den Prüfer
.. ermöglicht den gesetzlich geforderten "Prüferblick" auf die eigene NIS2-Compliance

2) Veranschaulichung der Institutionalisierung von NIS2
.. visualisiert den Erfüllungsgrad und die Umsetzungstiefe von NIS2 im Krankenhaus

3) Bereitstellung im Rahmen der Mitgliedschaft
… die Software zur Messung des Institutionalisierungsgrades ist Teil des Mitgliedsbeitrages

4) Messung mit Zertifikat für Aufwandsentschädigung
… die Durchführung der Messung des Institutionalisierungsgrades mit Zertifikat kann zur bekannten Aufwandsentschädigung hinzu gebucht werden, d.h. nach Beratungsansatz
➔ Ausfüllung der zugesandten MITO-Fragebogen,
➔ Vorstellung der Ergebnisse aus den Fragebogen,
➔ Hinterfragung und Diskussion der Eingaben, die zu dem Ergebnis geführt haben,
➔ Finalisierung der Ergebnisse bzw. des NIS2 Institutionalisierungsgrades und
➔ Festlegung der Maßnahmen zur Erreichung eines besseren Institutionalisierungsgrades.

5) Planung der künftigen Nutzung
… soll zum umfassenden Management-Kontrollinstrument weiterentwickelt werden.

Was ist für das Krankenhaus zu tun?

➔ ISMS, Lieferkettengesetz, Registrierung & BCM

Ein Informationssicherheits-Managementsystem (ISMS) ist zu institutionalisieren bzw. erweitern, siehe Lieferketten und BCM.

Im Rahmen des ISMS sind u.a. die

➔ Lieferketten zu prüfen bzw. weiter organisatorische Maßnahmen vorzunehmen.

➔ Cybersicherheitszertifikate zu prüfen und Maßnahmen zu ergreifen.

Es ist die Registrierung beim BSI vorzunehmen und sich auf kontinuierliche Kommunikation mit dem BSI und dem entsp. Landesamt einzustellen.

Es ist ein BCM (Business Continuity) aufzubauen.

Die Geschäftsführung und –leitung muss sich schulen lassen, darüber ein Zertifikat ablegen und das Zertifikat ist dem BSI vorzulegen.

Das Zertifikat bzw. die Schulungsinhalte müssen dem Gesetz genügen !

Hosp.DO.IT
Hospitalgemeinschaft

Hospitalgemeinschaft Hosp.Do.IT
Hospitalgemeinschaft für die Digitalisierung der psychiatrischen und somatischen Akut-, Fach- und Rehakliniken

Onboarding

Wir etablieren bei unseren Mitgliedern die strukturierte und operativ umsetzbare Digitalstrategie, IT-Strategie, als auch Daten-strategie der Hospitalgemeinschaft. Die Etablierung erfolgt individuell, womit die operative Steuerbarkeit erreicht wird.
Ferner wird als DSB, ISB und Projektsteuerer Verantwortung übernommen, als auch für Leistungsverzeichnisse.

Operational Excellence

Wir etablieren bei unseren Mitgliedern Methoden das laufende Geschäft so zu steuern, dass die Ziele der Strategie erreicht werden.
Die Methoden:
1) Dreiwöchige Arbeitsgruppen ISMS, TI&IOP, KPIs, Partner-Management und Personal
2) Dreiwöchige Leitungstermine
3) Rollierende Quartals-Planung

Decision Support

Unsere unterstützenden Dienste basieren auf den bereitgestellten Informationssystemen:
1) Konzepte & Vorlagen
2) Benchmarking & KPIs.
Durch die Lösungs-konzepte und Benchmarking Daten werden die strategischen Ziele nachhaltig erreicht.

Certifications & qualifications

Programme
Mitarbeiterbindung u. -gewinnung
1) Graduate Programm

digitalhealth manager®

2) Trainee Programm

digitalhealth expert®

Qualifikationen
Führungskraftenwik-klung u. -absicherung
1) KRITISDachG

KRITISDachG-compliance executive

2) NIS2 UmG

NIS2-compliance executive

Hosp.DO.IT
Infrastruktur und Service

AHIME Academy

Die Zertifizierungen CHCDO und CHCIO als Programmbestandteil.

Hospitalgemeinschaft Hosp.Do.IT
Krankenhausträger mit über 80 Institutskennzeichnen in den Landeskrankenhausplänen der Bundesländer Baden-Württemberg, Bayern, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt und Schleswig-Holstein

Die Mitgliedschaft im Kosten - Nutzen T-Konto: Seite 1 / 2

Soll = Mitgliedsbeitrag

(____) Kategorie weniger als 31.000 Patienten

(____) Kategorie zw. 31.000-41.000 Patienten

(____) Kategorie größer 41.000 Patienten

Haben = Mitgliederleistung

Anfertigung Digitale Agenda, Digitalisierungs- und Datenstrategie

Anfertigung Strategie und -Masterplanung für Informations-, Kommunikations-, Medizin- und Versorgungstechnik mit allen Investitions- und Betriebskosten eingebettet in ein ISMS

Erstellung und Institutionalisierung eine Quartals-Berichtswesen zur vorgenannten Strategie- bzw. Zielerreichung (in T., in L. in B.)

MIS - Management Informationssystem (Cloud Mandant), für KHZG-/ IT-Benchmarking, -Controlling, und Rechnungswesen

Gutachtertätigkeiten, d.h. für die bekannten Förderverfahren KHZG bzw. KFSFV, aber auch andere Mittelbeantragungen

Haftungsrechtliche Absicherung der Geschäftsführungen, d.h.
- Anfertigung ISMS mit den 5 Bestandteilen Matrix Risiko- und Schutzbedarfsfeststellung, Datenschutzkonzept, IT-Betriebs-führungs-/ -Notfallhandbuch, ISMS-Handbuch und Strukturierte Quartalsprotokolle
- Schulung mit Zertifikaten, d.h. z.B. NIS2, KRITISDachUmG.

Bereitstellung Datenschutz- und ISMS-Vorlagen oder komplettes Compliance System (Cloud Mandant)

Die Mitgliedschaft im Kosten - Nutzen T-Konto: Seite 2 / 2

Soll = Mitgliedsbeitrag

(____)	Kategorie weniger als 31.000 Patienten	12.157,58 €
(____)	Kategorie zw. 31.000-41.000 Patienten	17.560,96 €
(____)	Kategorie größer 41.000 Patienten	22.964,33 €

Haben = Mitgliederleistung

- Führungskräfte bindendes und gewinnendes Digital Leader Graduate und Trainee Programm
- Anfertigung IT-Leitbild mit Vision, Mission und Wertekanon.
- Anfertigung Cloudstrategie, d.h. Cloud Strategie u. Kostenmanagement, Governance und Compliance u. Integration und Migration, Ressourcen-Nutzung u. Anbieter Management
- Bereitstellung von „fertig“ designten Infrastruktur u. Business Lösungen der Hosp.Do.IT I. & S., d.h. MVZ BOX, IKTM-Cloud-Services, als auch eBo, beBPO und EGVP Postfach Kommunikation
- Sonderkonditionen über Rahmenverträge in den Kategorien, Basis-, Ausbildungs-, Referenz- und Entwicklungspartner.
- Übernahme von Verantwortung als externer DSB, ISB und Cloud Beauftragter zu Sonderkonditionen.
- Abwicklung von Sonderaufträgen wie z.B. Interimsmanagement, Projektsteuerung, LVs für Ausschreibungen, etc. zur Aufwandsentschädigung von € 1.178 € pro 8 Stundentag.

Unsere Mitglieder – starke Referenzen

Steuerungsgremium 2025 – 2027 der Mitgliederversammlung

ELBE KLINIKEN STADE · BUXTEHUDE

KNAPPSCHAFT KLINIKEN

Landeskrankenhaus

AWO Psychiatriezentrum

AKH GRUPPE AKH CELLE

BDH-Klinik Elzach

Burghof-Klinik

GKG Gesundheit & Lebensqualität für die Region Bamberg

STADT. KRANKENHAUS MARIA-HILF IM GESUNDHEITSPARK BRILON gGmbH

DIABETES ZENTRUM MERGENTHEIM

DR. FONTHEIM Mentale Gesundheit

DRK Trägergesellschaft Süd-West

Kinderklinik Siegen Deutsches Rotes Kreuz

GESUNDHEITSHOLDING LÜNEBURG

GEFÄSS-ZENTRUM IM KREIS AHRWEILER

Harzklinikum Dorothea Christiane Erxleben

HDZ NRW UK RUB

HÜTTENHOSPITAL Zurück ins Leben

KLINIKEN SÜDOSTBAYERN

INN KLINIKUM ALTÖTTING UND MÜHLDORF

KLINIKUM ITZEHOE

KERCKHOFF KLINIK

Wahrendorff

KLINIKUM WOLFSBURG

Medizin mit Menschlichkeit KKRN

Kloster Grafschaft Fachkrankenhaus

Krankenhäuser Buchholz und Winsen

Krankenhaus Porz am Rhein Akademischen Lehrkrankenhaus der Universität zu Köln

KRANKENHAUS MARIENSTIFT

Kreiskrankenhaus Saarburg

heilen, pflegen, helfen LICHTENAU e.V. Im Verbund der Diakonie

Medizinisches Zentrum für Gesundheit Bad Lippspringe GmbH MZG-Westfalen

OSTEMED

Rheinland Klinikum

SAUERLANDKLINIK HACHEN

SAH

SHG: Saarland Heilstätten

St. Vincenz Kliniken

Vestische Caritas-Kliniken

Westpfalz-Klinikum GmbH Moderne Medizin mit menschlichem Gesicht

ZOLLERN ALB KLINIKUM

Vielen Dank für Ihre Aufmerksamkeit!

Frank Ebling, CHCDO, CHCIO
Westpfalz-Klinikum
Beauftragter für Digitalisierung und Informationssicherheit
Hellmut-Hartert-Str. 1
D-67655 Kaiserslautern
Tel: +49 (0) 631 203-1121
Mobil: +49 (0) 160 95506025
E-Mail: febling@westpfalz-klinikum.de
Web: www.westpfalz-klinikum.de

Ruediger Gruetz
Klinikum Wolfsburg
Sauerbruchstraße 7
D-38440 Wolfsburg
Tel: +49 (0) 5361 803103
Mobil: +49 (0) tbd
E-Mail: ruediger.gruetz@klinikum.wolfsburg.de
Web: www.klinikum-wolfsburg.de

Marcel Jorkisch
AKH Celle
Zentralbereichsleiter IT
Siemensplatz 4
D-29223 Celle
Tel: +49 (0) 5141 723350
Mobil: +49 (0) tbd
E-Mail: marcel.jorkisch@akh-celle.de
Web: www.akh-celle.de

Prof. Dr. Pierre-M. Meier, CHCDO, CHCIO
Hospitalgemeinschaft Hosp.Do.IT
Generalbevollmächtigter
Am Schellberg 17
D-41516 Grevenrbroich
Tel: +49 (0) 2182 8865066
Mobil: +49 (0) 170 23 03 11 1
E-Mail: Pierre-Michael.Meier@Hosp-Do-IT.de
Web: www.Hosp-Do-IT.de

Unsere Mitgliederleistungen