Hosp.DO.IT Hospitalgemeinschaft

Robin Data ComplianceOS

AWO Niedersachsen gGmbH AWO Psychiatriezentrum

Von der Digitalstrategie über IOP bis zum ISMS

DMEA 24. und 25. April 2023

Neue Voraussetzungen

1. B3S für Nicht-Kritis-Häuser
2. Seit 1. Januar 2022 gesetzlich verpflichtend
3. Einbindung der Stakeholder
4. Externe Unterstützung
5. ISB Lehrgang

Rechtliche Grundlagen

- Mit dem im Patientendaten-Schutzgesetz (PDSG) neu hinzugefügten und überarbeiteten § 75 c SGB V werden alle Krankenhäuser verpflichtet, ab **1. Januar 2022** organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen zu treffen und diese alle zwei Jahre an den Stand der Technik anzupassen. Dies gilt ausdrücklich auch für die Krankenhäuser, die nicht bereits als „Kritische Infrastruktur" eingestuft wurden (NKG-Mitteilung 500/2020).
- Auch Arztpraxen sind künftig – nach § 75b SGB V - zur Sicherung ihrer IT-Systeme verpflichtet.
- § 75 b und § 75 c SGB V beziehen sich auf **§ 8a BSIG**, welcher durch B3S bzw. die ISO-Normen 27001, 27002 und 27799 umgesetzt wird.
- Für den B3S-Geltungsbereich erfolgt die Risikoeinschätzung entsprechend der Anforderungen folgender Normen:
  - Informationssicherheit - allgemein: DIN ISO/IEC 27001 „Informationssicherheits-Managementsysteme - Anforderungen" und ISO 27002 (allg. Umsetzungsempfehlungen)
  - Informationssicherheit von Medizingeräten in IT-Netzwerken: DIN EN 80001-1 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten", ISO 27799 enthält Umsetzungsempfehlungen für das Gesundheitswesen

Leitlinie

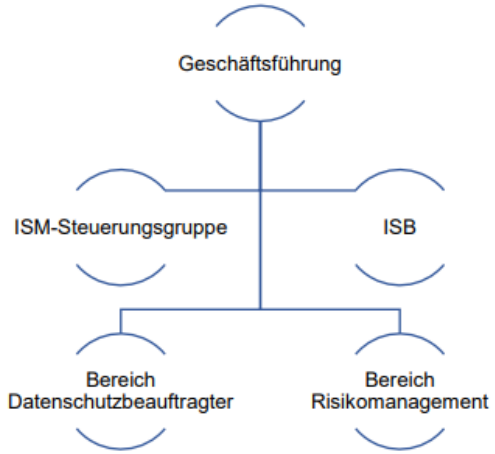
1. Rahmen setzen zur Umsetzung der Anforderungen B3S
2. Definition der Kritischen Dienstleistung (KDL)
3. Definition der Verantwortungsbereiche
4. Bestimmung des ISB
5. Arbeitsgruppendefinition
6. Positionierung der Informationssicherheit im Haus

AWO Niedersachsen gGmbH | Leitlinie für die Informationssicherheit

8. Etablierung einer ISM-Steuerungsgruppe

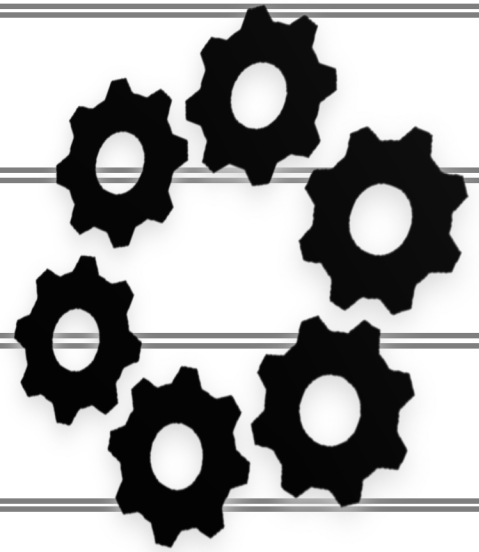
Die ISM-Steuerungsgruppe bezeichnet das interne Gremium, das die Informationssicherheitsmaßnahmen bespricht und für die Umsetzung im klinischen- und Verwaltungsumfeld im Sinne der Informationssicherheitsprozesse vorbereitet.
Es wird aus der IKT-Abteilung, der Datenschutzbeauftragten, der Qualitätsmanagementbeauftragten, der Risikomanagementbeauftragten und dem ISB besetzt. Unterstützend sind die jeweiligen Fachbereiche und klinischen Bereiche tätig.
Strategische Informationssicherheitsmaßnahmen werden mit der Geschäftsführung, der Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten gemeinsam verabschiedet.

9. Organisationsstruktur für Informationssicherheit



Arbeitsgruppe und Bereichsverantwortliche

1. Auflistung der Bereichsverantwortlichen
2. Einbindung der Bereiche
3. Aufgabendefinition
4. Zusammenstellung der Arbeitsgruppe
5. Steuerkreis Informationssicherheit und Dokumentation
6. Schulung



Geltungsbereich und Assets

1. Drei Bausteine des Geltungsbereiches:

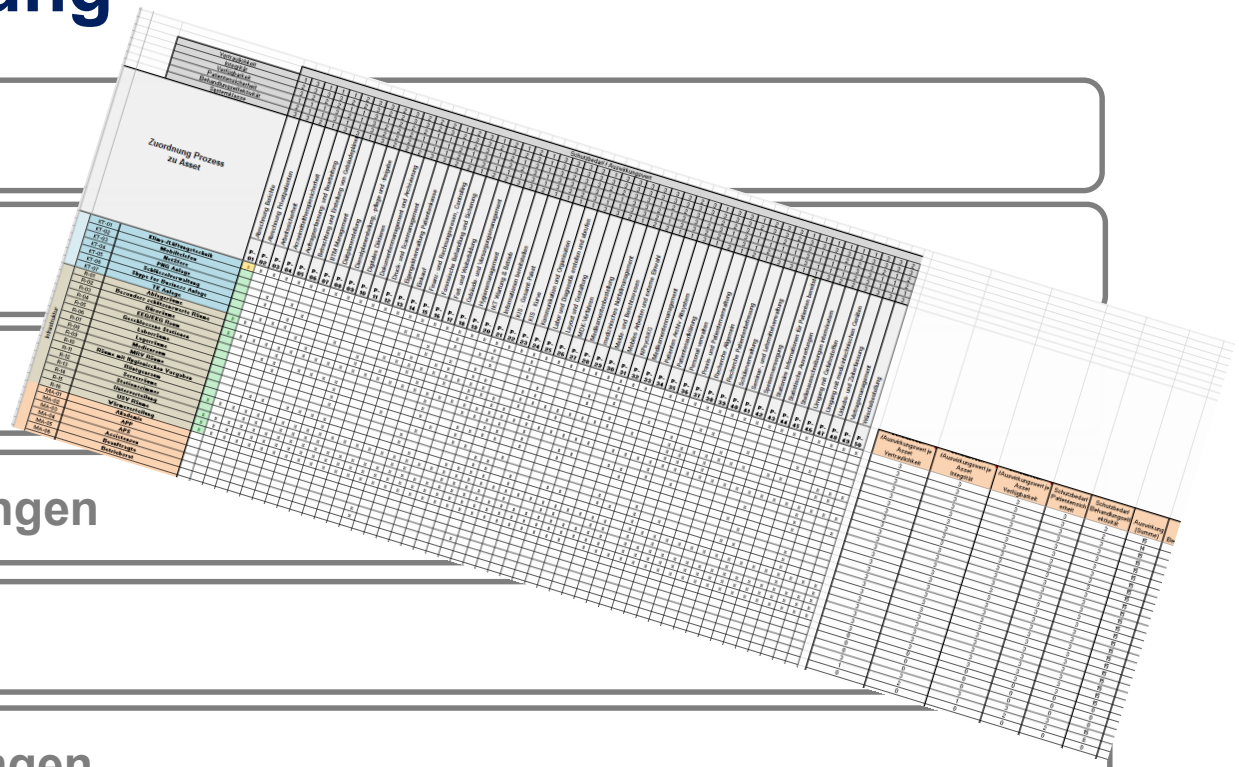
- Prozesse
- Assets
- Asset-Bewertung

Risikobereichskategorie	Risikofeld	Kurztitel	Risikoart	Meldende Perso	Eintrittswahrscheinlichkeit	Bedeutung	Entdeckungswahrscheinlichkeit
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 1 Nichtverfügbarkeit wichtiger, medizinisch relevanter Daten im DiagnoseProzess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 2 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Therapie-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 3 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Pflege-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 4 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Entlassungsprozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 5 Nichtverfügbarkeit von für den Behandlungsprozess wichtiger Prozess- und Freigabeinformationen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 6 Nichtverfügbarkeit von behandlungsprozessrelevanten IT-Systemen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Nichtverfügbarkeit	GEF 7 Nichtverfügbarkeit von behandlungsrelevanten Logistikketten	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Inkonsistenzen	GEF Inkonsistenzen Allgemein	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Inkonsistenzen	GEF 8 Inkonsistenzen in für den Behandlungsprozess relevanten Datenbeständen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Inkonsistenzen	GEF 9 Inkonsistenzen bei der Übertragung von für den Behandlungsprozess relevanten Datenbeständen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Manipulation Data	GEF Manipulation Daten Allgemein	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Manipulation Data	GEF 10 Manipulation von medizinisch relevanten Daten im Diagnose-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Manipulation Data	GEF 11 Manipulation von medizinisch relevanten Daten im Therapie-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Manipulation Data	GEF 12 Manipulation von medizinisch relevanten Daten im Pflege-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Manipulation Data	GEF 13 Manipulation von medizinisch relevanten Daten im Entlassungs-Prozess	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Unterbrechung	GEF Unterbrechung Allgemein	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Unterbrechung	GEF 14 Unterbrechung von behandlungsrelevanten Kommunikationsabläufen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Vertraulichkeitsverlust	GEF Vertraulichkeitsverlust Allgemein	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Vertraulichkeitsverlust	GEF 15 Vertraulichkeitsverlust bei besonders sensiblen Patienten- und Behandlungsinformationen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Verlust der Datenauthentizität	GEF Vertraulichkeitsverlust Allgemein	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Verlust der Datenauthentizität	GEF 15 Vertraulichkeitsverlust bei besonders sensiblen Patienten- und Behandlungsinformationen	Patientenbezogenes Risiko			5	
6.3.002 AMONDIS eShop Apotheke	Fremdsteuerung | Manipulation Systeme	GEF Fremdsteuerung / Manipulation Systeme Allgemein	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Fremdsteuerung | Manipulation Systeme	GEF 17 Fremdsteuerung/Manipulation von medizinische relevanten IT-Systemen	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Fremdsteuerung | Manipulation Systeme	GEF 18 Fremdsteuerung/Manipulation von Medizingeräten	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Fremdsteuerung | Manipulation Systeme	GEF 19 Fremdsteuerung/Manipulation von relevanten Infrastrukturkomponenten	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF Nichtverfügbarkeit Allgemein	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 1 Nichtverfügbarkeit wichtiger, medizinisch relevanter Daten im DiagnoseProzess	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 2 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Therapie-Prozess	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 3 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Pflege-Prozess	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 4 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Entlassungsprozess	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 5 Nichtverfügbarkeit von für den Behandlungsprozess wichtiger Prozess- und Freigabeinformationen	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 6 Nichtverfügbarkeit von behandlungsprozessrelevanten IT-Systemen	Patientenbezogenes Risiko			5	
6.4.001 Big Blue Button	Nichtverfügbarkeit	GEF 7 Nichtverfügbarkeit von behandlungsrelevanten Logistikketten	Patientenbezogenes Risiko			5	
	Inkonsistenzen	GEF Inkonsistenzen Allgemein				2	
						2	
						2	
						2	
						2	
						2	
						2	
						2	
						2	

2. Dimension der Bewertung:

- Auswirkung/Bedeutung (Integrität, Vertraulichkeit, Verfügbarkeit, Patientensicherheit, Behandlungseffektivität), Systemklasse

Umsetzung



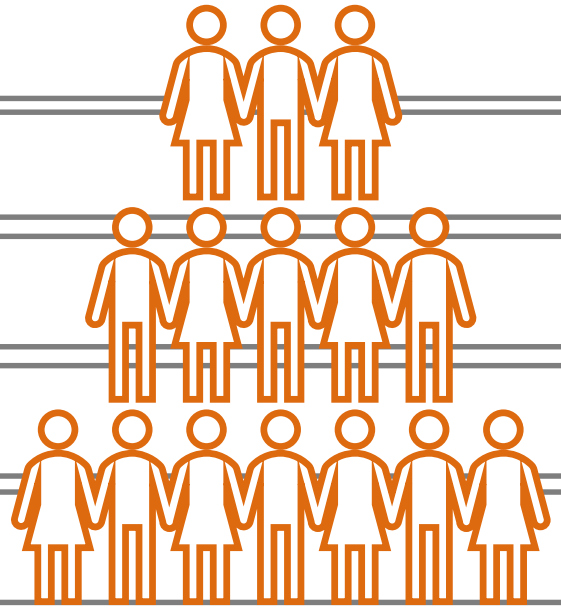
1. Vorbereitung
2. Positionierung im Haus
3. Einbindung ISB
4. Strukturierung der umzusetzenden Anforderungen
5. Zeitaufwand
6. Gefährdungen, Schwachstellen und Bedrohungen
7. Arbeitsumfang: Von 160 definierten Assets über Bewertungsdimensionen und Gefährdungen zu über 4.000 Bewertungen

ISMS

1. Hersteller
2. Datenstrukturen
3. Eintritts- und Entdeckungswahrscheinlichkeiten
4. Gefährdungsbewertung der Assets
5. Anforderungsbewertung und -erfüllung

Herausforderungen

1. Zeitaufwand
2. Menschliche Ressource
3. Verantwortungen
4. Verständnis im Haus
5. Einbindung ISB
6. Prozesswandlungen
7. Schulungen



AG ISMS Hosp.Do.IT

1. Kick off 12.01.2021
2. Teilnehmer vorwiegend im Nicht-Kritis-Bereich
3. Anbietergewinnung
4. Weiterentwicklung… => durch Ahrtal beflügelt
5. Von Unterlagenerstellung über Umsetzungsunterstützung zum Mustermandanten

!Arbeitsgruppe "ISMS": Fokus § 75c SGB V

AG ISMS Hosp.Do.IT

1. Kick off 12.01.2021
2. Teilnehmer vorwiegend im Nicht-Kritis-Bereich
3. Anbietergewinnung
4. Weiterentwicklung… => durch Ahrtal beflügelt
5. Von Unterlagenerstellung über Umsetzungsunterstützung zum Mustermandanten

!Arbeitsgruppe "ISMS": Fokus § 75c SGB V

COMPLIANCE-FELDER

Gesetze
Datenschutz, Steuerrecht, LKSG, Hinweisgeberschutzgesetz, KRITIS

Normen
27000er, B3S, 9001, TISAX, BSI-Grundschutz

Assets
Schutzbedarfe und elementare Gefährdungen analysiere

Risiko-Management
Alle Risikofelder wiederholbar auf einer Plattform managen

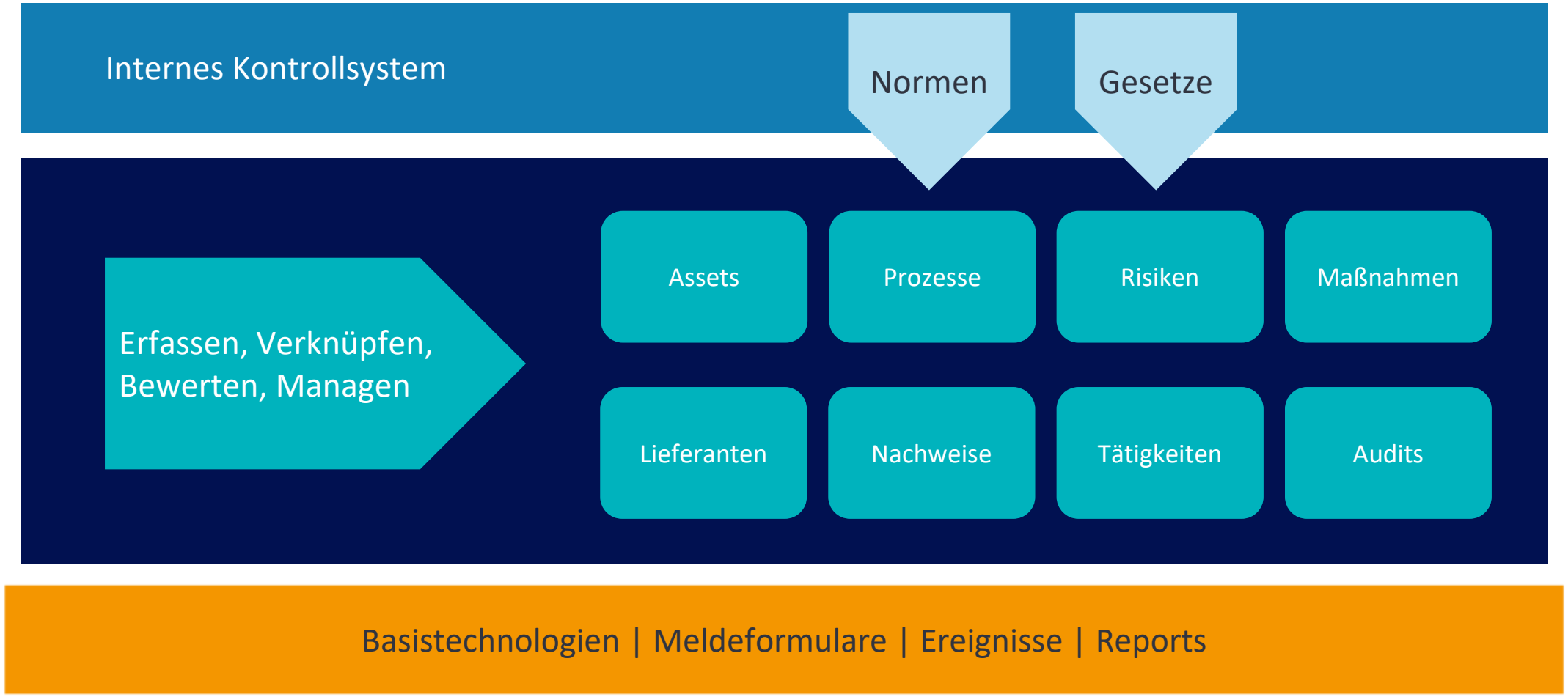
Lieferanten-Management
Lieferanten und Services erfassen und Risiken bewerten

Verträge & Nachweise
Sammeln der passenden Informationen am richtigen Ort

Tätigkeitenmanager
Komplexe Vorgänge gemeinsam im Kontext managen

Formulare & Workflows
Eigene Formulare erstellen und Aufgaben delegieren

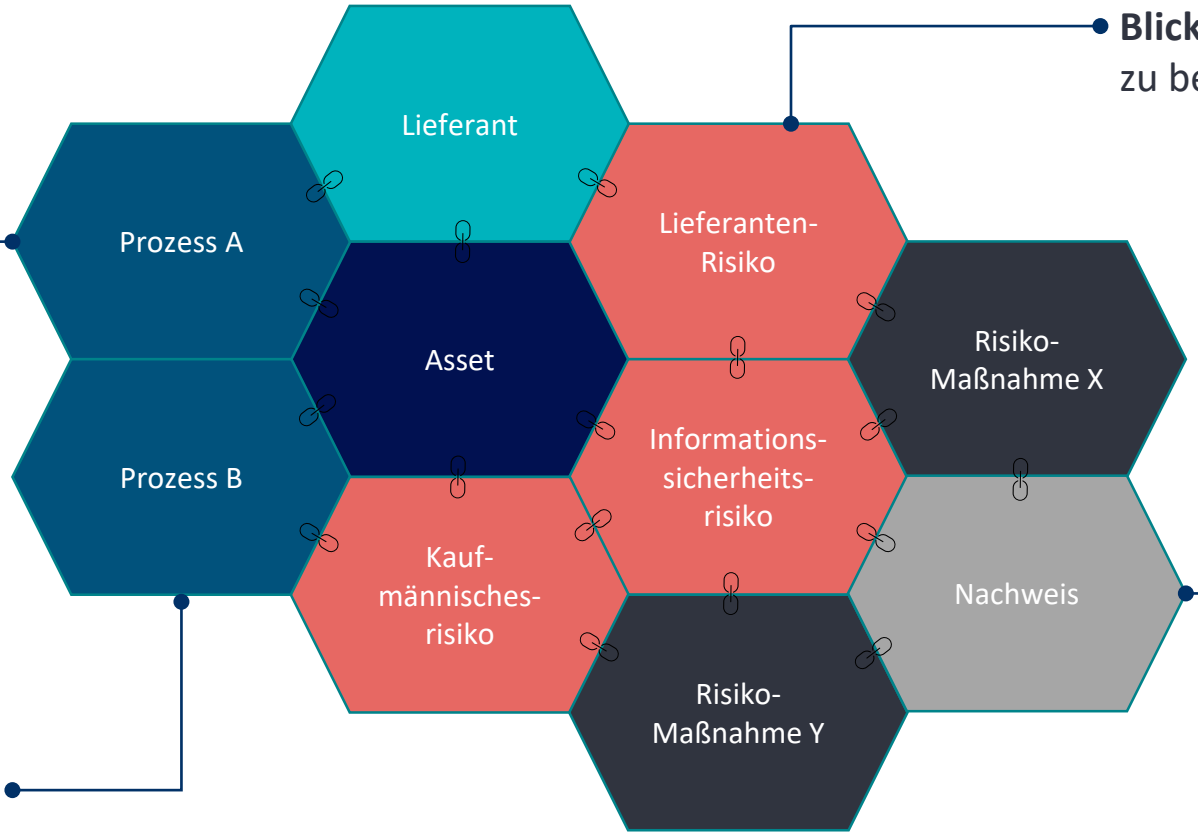
ComplianceOS® Systemarchitektur



Durchgängige Modellierung. Gemeinsame Perspektive.

Prozesse durchgängig **modellieren** und **verknüpfen**

Daten gleichzeitig aus **unterschiedlichen Blickwinkeln** der Risikoverantwortlichen zu betrachten



Doppelaufwand vermeiden

Im Ergebnis für die Daten **gemeinsame Perspektiven** der Verantwortlichen

BASISINFORMATION

- Mitarbeit:
  - Vorarbeiten in der ISMS Gruppe
  - Mitglieder der ISMS-Gruppe, insbesondere Herr Seelhorst, Dr. Meier in Zusammenarbeit mit Prof. Döring
- Basis
  - Das Hosp.Do.IT-Mustermandant berücksichtigt den Standard B3S und Anleihen aus dem BSI-Grundschutz (Elementare Gefährdungen)
- Aktuell umgesetzt:
  - Prozesse → Definierte kritische Dienstleistungen (Kernprozesse)
  - Schutzbedarfsanalyse → Assetklassen und Schutzbedarfsbewertungsschema
  - Risikomanagement → Risikoklasse und Risikoschutzbedarfsanalyse
  - Reifegradbewertung der Controls → SPICE Model (ISO/IEC 15504)

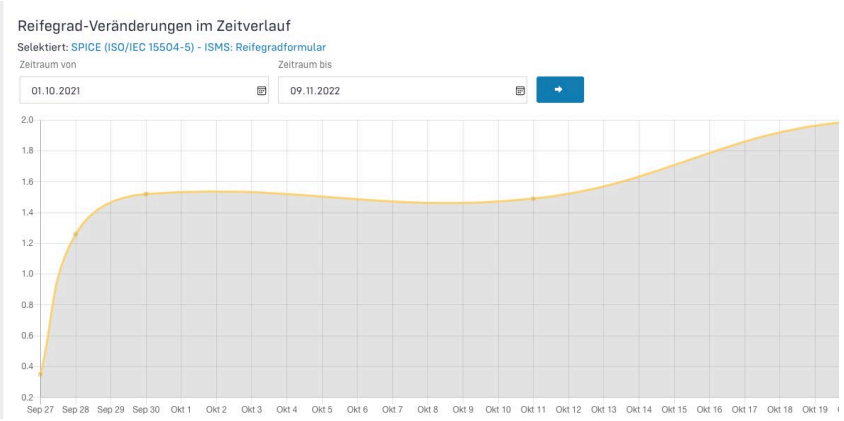
ARBEITSERGEBNISSE MUSTERMANDANT (AUSZUG)

			Patientensicherheit	
3	9	18	27	3
2	4	8	12	2
1	1	2	3	1
Schutzbedarf	1	2	3	
	Behandlungseffektivität			

- **Assetmanagement (Nach B3S):**
  - Definition von Asset-Klassen- und Asset-Unterklassen
  - B3S-konformes *Bewertungsschemas* zur *Schutzbedarfsermittlung* (B3S-Systemklassen) unter Berücksichtigung de *Behandlungseffektivität* und *Patientensicherheit*
  - Fragenkatalog zur Umsetzung *wiederholbarer Bewertungen*
  - Einbinden elementarer Gefährdungen zur *Umsetzung von BSI-KRITIS-Vorgaben*
- **Risikomanagement (Nach B3S):**
  - Definition von Risikofelder und Risikoklassen
  - B3S-kompatibles Risikobewertungsschema zur Risikoermittlung von Patientensicherheitsrisiken, Informationssicherheitsrisiken und Datenschutzrisiken

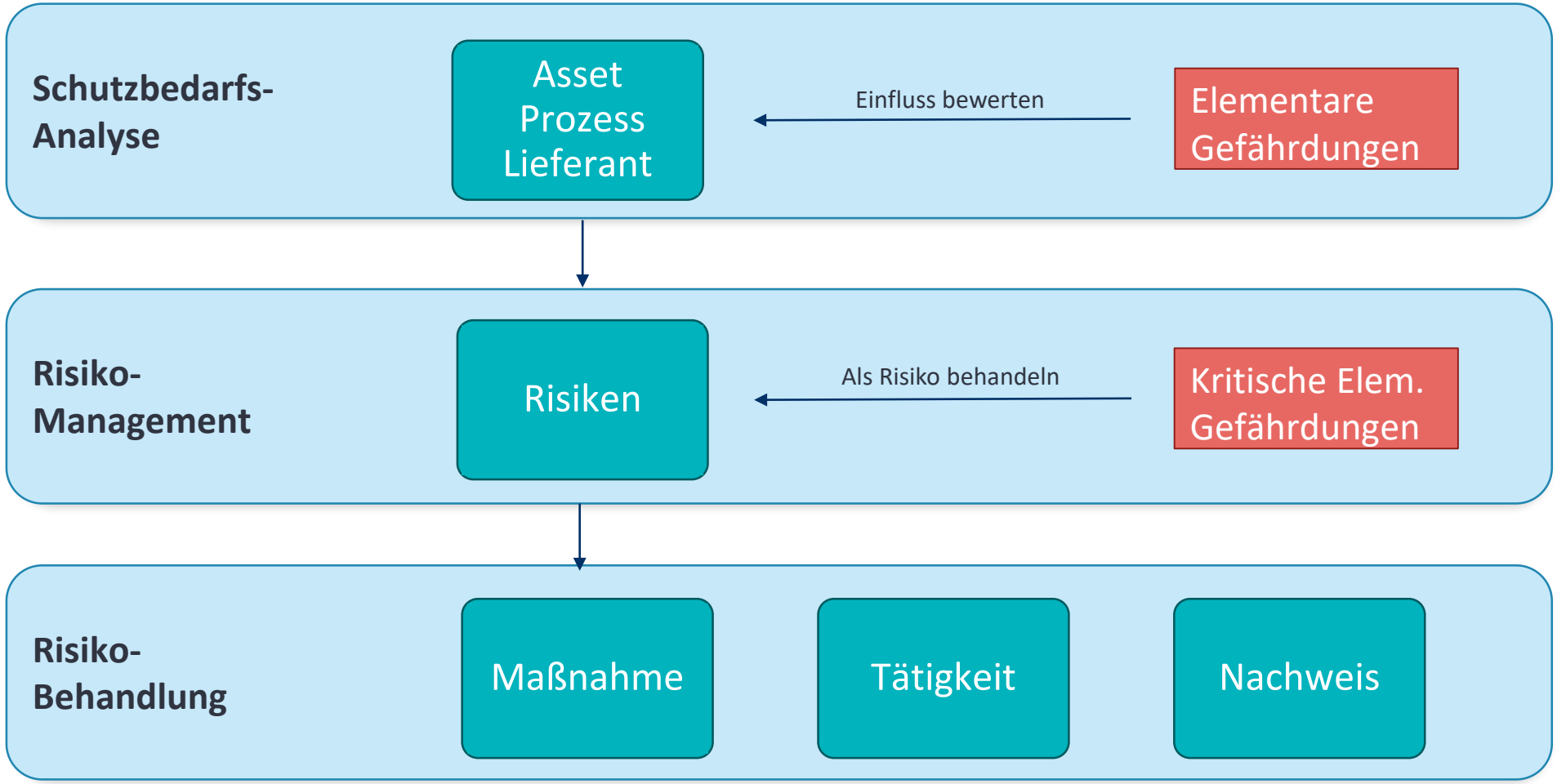
Arbeitsergebnisse Mustermandant (Auszug)

- **Audits, Internes Kontrollsystem und Rechtskataster**
  - Integration des B3S Standards (Originaltexte) zur Umsetzung der Kontrollsystems
  - Auditmanagement für die Kontrollen
  - Maßnahmenverfolgung
  - Reifegradmodelle z. B. nach ISO / IEC 15504



- **Maßnahmen- und Nachweismanagement**
  - Maßnahmen und Nachweise (Verträge) können kontextbezogen verwaltet werden
- **Viele weitere Standards mit Vorlagen integriert**
  - Datenschutz, 27000er, BSI-Grundschutz, Qualitätsmanagement, ...

Vom Schutzbedarf zum Risiko zur Maßnahme



RISIKOBEWERTUNGEN MÜSSEN WIEDERHOLBAR SEIN

Risikobewertung

- Risikobewertung - 17.06.2022 12:51:24 (Andre Döring, dr.andre.doering+sta-kkh@gmail.com)
- Risikobewertung - 17.06.2022 13:48:00 (Andre Döring, dr.andre.doering+sta-kkh@gmail.com)
- Risikobewertung - 29.06.2022 23:51:23 (Andre Döring, dr.andre.doering+sta-kkh@gmail.com)

Bewertungsformular: ISMS Standardrisiko

ISMS: Eintritts- und Entdeckungswahrscheinlichkeit

- Wie häufig ist das Risiko in der Vergangenheit aufgetreten?
- Wie häufig könnte das Risiko in der Zukunft aufgetreten?
- Wie gut ist das Risiko zu entdecken?

ISMS: Schadenshöhe

- Wie schätzen Sie finanziellen Schaden bei Eintritt des Risikos ein?
- Wie schätzen Sie den Einfluss des eintretenden Risikos auf kritische Dienstleistungen ein?
- Welchen Einfluss hat das eingetretene Risiko auf die Reputation des Hauses?
- Wie schwer wiegen Gesetzverstöße bei eintretendem Risiko?
- Wie viele Personen sind bei eintreten des Risikos betroffen?

Ergänzende Begründungen und Erläuterungen

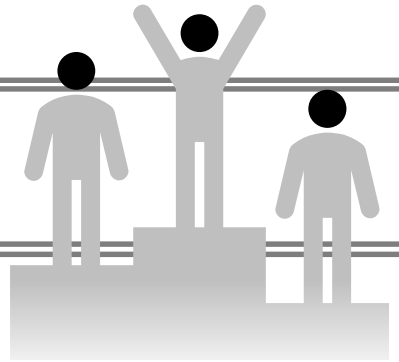
Risikobewertung - 29.06.2022 18:15:29 (Andre Döring, ado@robin-data.io)

ISMS: Eintritts- und Entdeckungswahrscheinlichkeit	Score
Selten	2,00
ISMS: Schadenshöhe	**Score**
Hoch	2,00
Gesamt-Bewertung	**Gesamt-Score**
Mittleres Risiko - Risiko verlagern oder reduzieren	4

Ergänzende Begründungen und Erläuterungen

Fazit

1. Neuer B3S seit Anfang 2023
2. Zeitlicher Aufwand
3. Unterschätzung der Positionierung im Haus



Gemeinsam sind wir eine starke Gemeinschaft !

DANKE FÜR IHRE AUFMERKSAMKEIT

Dr. Pierre-Michael Meier

Hospitalgemeinschaft Hosp.Do.IT
Generalbevollmächtigter

Rochusweg 8
D-41516 Grevenbroich

Tel: +49 (0) 2182-57 03 60
Fax: +49 (0) 2182-57 03 42
Mobil: +49 (0) 170-23 03 11 1
E-Mail: Pierre-Michael.Meier@Hosp-Do-IT.de
Web: www.Hosp-Do-IT.de

Prof. Dr. André Döring

Robin Data GmbH
Geschäftsführer

Fritz-Haber-Str. 9
D-06217 Merseburg

Tel: +49 (0) 3641-479236-0
Fax: +49 (0) 3641-479895-9
E-Mail: ado@robin-data.io
Web: https://www.robin-data.io/

Björn Seelhorst

AWO Psychiatriezentrum
Geschäftsbereichsleiter IKT

Vor dem Kaiserdom 10
D-38154 Königslutter

Tel: +49 (0) 5353-90 18 00
Fax: +49 (0) 5353-90 10 95
E-Mail: Bjoern.Seelhorst@awo-apz.de
Web: www.awo-psychiatriezentrum.de