DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Umsetzungshinweise nach §75c SGB V

Arbeitshilfe Gap-Analyse

Stand: 07.12.2021

Kategorie: öffentlich

Status: Freigegeben

Version: 0.98

Kürzel: GAPA

Postfach 12 05 55
10595 Berlin
Wegelystraße 3
10623 Berlin

c/o HOPE
Avenue Marnix 30
1000 Brüssel
Telefon +32 2 540 25 50

Commerzbank AG
IBAN DE63 1004 0000 0788 4141 00
BIC COBADEFFXXX
UST-IdNr. DE119355528

www.dkgev.de

Anwendungshinweis:

Dieses Dokument sowie die vorliegenden Empfehlungen und Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt die Deutsche Krankenhausgesellschaft keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

Inhaltsverzeichnis

Aus Gründen der leichteren Lesbarkeit wird in den Beschreibungen auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten und gelten gleichermaßen für beide Geschlechter.

Dokumentenhistorie

Ver-sion	Stand	Kap,/ Seite	Beschreibung der Änderung	Bearbei-tung
0.9	25.11.21	alle	Anlage des Dokumentes	AG 75c
0.98	07.12.21	alle	Kommentierung	AG 75c

1 Zusammenfassung

Eine GAP-Analyse erfasst das aktuelle Sicherheitsniveau des Klinikums.

Die Herausforderung dabei ist, die Erfassung und Bewertung der für den Kernprozess der medizinischen Versorgung (vollstationäre Patientenversorgung) wichtigsten Assets festzulegen.

Ausgangspunkt für die Erfassung dieser Assets ist die Prozessmodellierung, aus der dann die erforderlichen Assets inkl. Bewertung der Gefährdung und Risiken abgeleitet werden können.

2 Einleitung

Das vorliegende Dokument beschreibt die Vorgehensweise bei der Erarbeitung der GAP-Analyse

Das Dokument richtet sich an alle Beteiligten, die an der Erarbeitung der GAP-Analyse mitwirken.

3. Allgemeine Beschreibung der GAP-Analyse

Ausgangspunkt für die GAP-Analyse kann eine Prozessbetrachtung der medizinischen Versorgung im Krankenhaus sein. Die identifizierten Prozesse und Systeme werden dabei hinsichtlich ihrer Kritikalität bewertet. Dabei wird insbesondere auf die Sicherstellung der medizinischen Versorgung im Krankenhaus abgestellt.

Im Ergebnis sollen diejenigen Funktionsbereiche und Funktionsstellen identifiziert werden, die von wesentlicher Relevanz für die Aufgabenerfüllung im Kontext der medizinischen Versorgung im Krankenhaus sind.

Bei der Betrachtung können beispielsweise die Funktionsbereiche und Funktionsstellen der DIN 13080 zur Strukturierung herangezogen werden, um ein einheitliches Vorgehensmodell sicherzustellen.

Im Sinne einer prinzipienorientierten Vorgehensweise soll die folgende Einteilung daher als „Blaupause“ für die Erhebung kritischer Prozesse dienen, hierauf aufbauend kann eine „Prozesslandkarte“ als Unterstützung für die Definition des Geltungsbereichs genutzt werden.

Zur Beschreibung der Prozesse der Prozessgruppe „medizinische Versorgung“

- Aufnahme,
- Diagnostik,
- Therapie,
- Pflege,
- Entlassung,

wird auf die Inhalte des Abschnitts „Übersicht der Kernprozesse und Funktionszuordnung innerhalb des Geltungsbereichs“ der aktuellen Fassung des Branchenspezifischer Sicherheitsstandard (B3S) verwiesen.

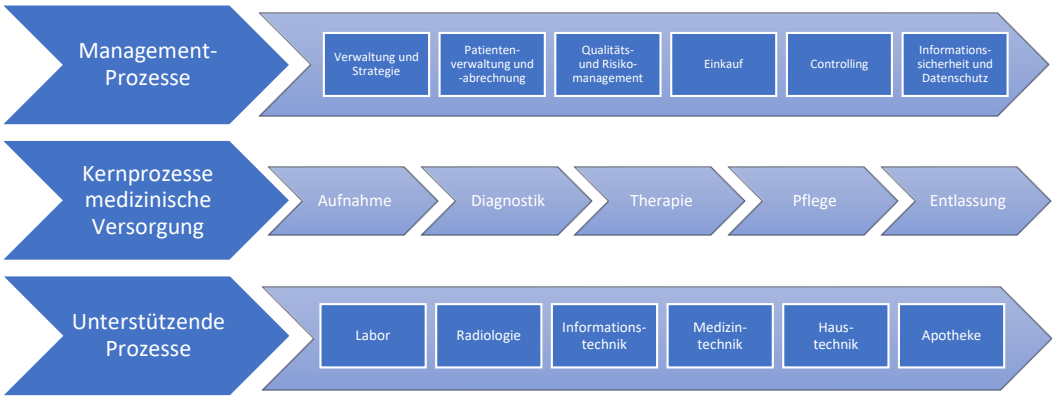

Abbildung 1: Prozessgruppen und Prozesse der medizinischen Versorgung im Krankenhaus

Aus dieser Prozessbetrachtung lassen sich die Assets für die weiteren Schritte ableiten sowie dokumentieren.

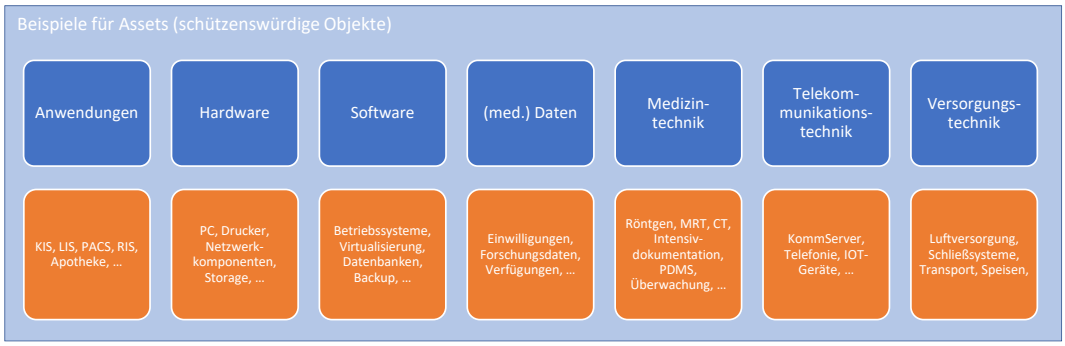

Abbildung 2: Beispiele für schützenswerte Objekte (Assets) im Krankenhaus

Ein Beispiel für die Komplexität einer GAP-Analyse eines „realen“ Krankenhauses ist der nachfolgenden Abbildung zu entnehmen. Diese umfasst die Prozesse inkl. interner und externer Informationsflüsse (rote Pfeile) sowie wesentliche Schutzeinrichtungen (Firewalls) zur Absicherung.

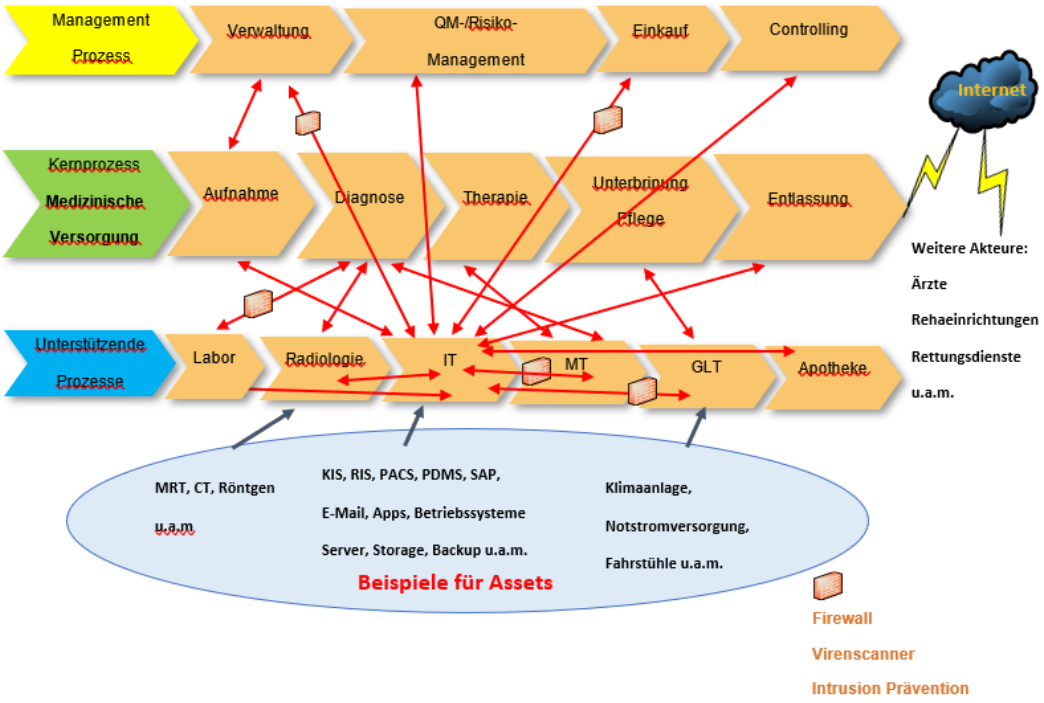

Abbildung 3: Prozessdarstellung in einem Klinikum (eigene Darstellung)

In der folgenden Skizze sind die Bausteine einer GAP- Analyse mit den wesentlichen Inhalten dargestellt, die nachfolgend beschrieben werden:

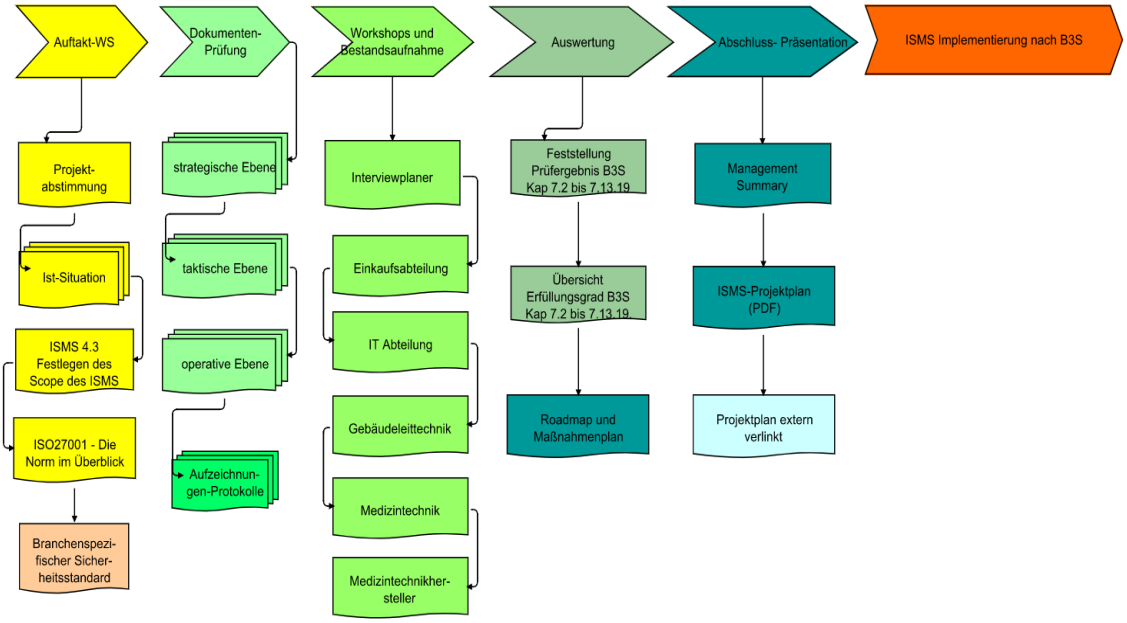

Abbildung 4: Bausteine einer GAP-Analyse (eigene Darstellung)

3.1 Beschreibung der Bausteine

3.1.1 Auftaktworkshop

In Vorbereitung auf den Auftaktworkshop sollten alle Verantwortlichen (Stakeholder) unter Berücksichtigung der Kernprozesse der medizinischen Versorgung (Abbildung 1) ermittelt werden. Diese sollten unbedingt am Workshop teilnehmen und frühzeitig eine Einladung seitens der Geschäftsführung des Krankenhauses erhalten. Zudem sollte die Leitung des Krankenhauses die Begrüßung durchführen, um die Bedeutung der Informationssicherheit für das Klinikum zu unterstreichen.

Die Workshop-Teilnehmer sollten die Ziele der Informationssicherheit im Klinikum kennen und entsprechend ihrer Bedeutung und geplanten Umsetzung sensibilisiert sein.

3.1.2 Workshops und Bestandsaufnahme

Die Bestandsaufnahme und Bewertung des aktuellen Sicherheitsniveau des ISMS kann anhand der Anforderungen der Norm ISO27001 (Prozessteil), Annex A sowie der aktuellen Fassung des Branchenspezifischen Sicherheitsstandard (B3S), eingeschränkt auf die MUSS Kriterien, erfolgen.

Dieses Vorgehen kann sinnvoll sein, wenn ein möglichst vollständiges Bild des aktuellen Sicherheitsniveaus gefordert ist.

Ziel ist es, mit den zuständigen Fachbereichen und Kliniken den Erfüllungsgrad der Anforderungen aus dem B3S Kap. 7.2 bis 7.13.19 mit den ANF-MN 001 bis 168 zu dokumentieren und zu bewerten.

Alternativ und als Einstieg kann die Bewertung auch anhand der Erfüllung der Anforderungen aus der **Arbeitshilfe „Priorisierung_Anforderungen_§75c.xlsx“** gefiltert auf die Umsetzungsstufe 1 = essentiell erfolgen. In der Unterlage wurden die Anforderungen und Risikoelemente des B3S in einen Stufenplan mit insgesamt vier Stufen überführt. Die einzelnen Stufen bauen aufeinander auf und sollen eine einfache Einstiegsmöglichkeit in die Umsetzung der Informationssicherheit aufzeigen.

Mit Umsetzung aller Stufen ist eine Einhaltung des branchenspezifischen Sicherheitsstandards B3S ebenfalls gegeben.

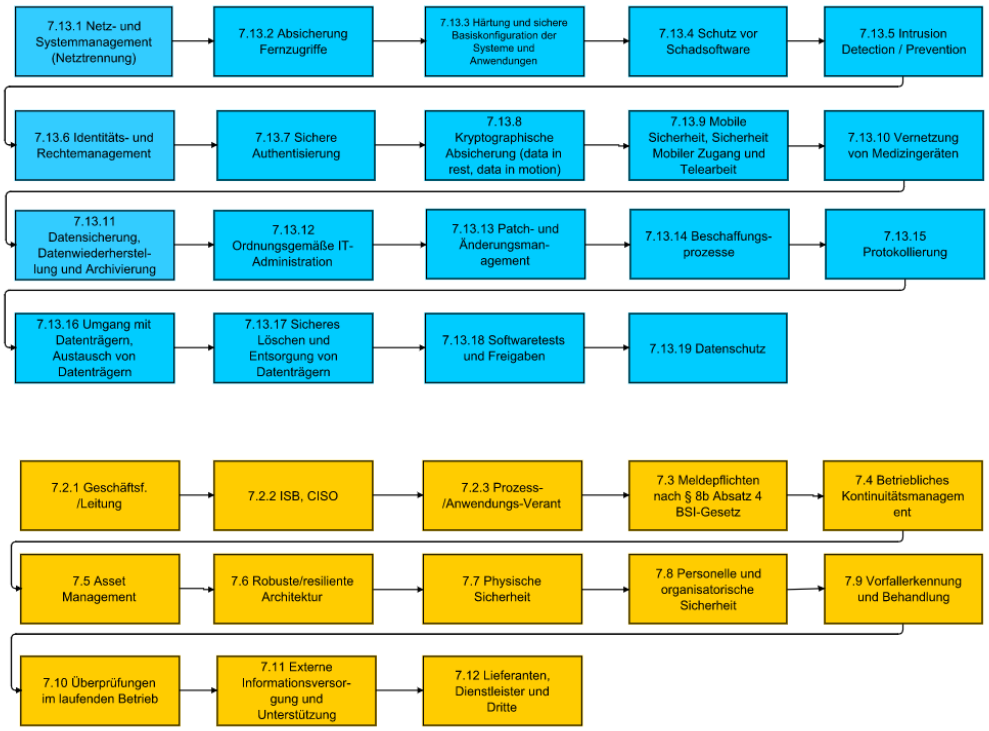

Abbildung 5: Übersicht der Anforderungskategorien des B3S (eigene Darstellung)

Eine weitere Alternative kann die LSI-Orientierungshilfe "IT-Sicherheit in Kliniken" und der Maßnahmenkatalog der Arbeitsgruppe "Smart Hospitals" der "Universität der Bundeswehr" sein.

Das Ergebnis der Bestandaufnahme dokumentiert das aktuelle Sicherheitsniveau des ISMS und kann in eine SoA (Statement of Applicability) überführt werden.

In einer SoA werden alle Kriterien aus dem Annex der ISO27001 aufgeführt und in welcher Art und Weise sie angewendet werden. Zudem kann diese Dokumentation um Maßnahmen der Umsetzung erweitert werden. Ergänzend können die Positionen aus dem Annex A der ISO27001 mit den MUSS-Maßnahmen aus dem B3S (ANF-MN) verknüpft werden, um den Zusammenhang zum B3S herzustellen.

3.1.3 Auswertung mit Roadmap

In diesem Schritt werden die Abweichungen, Korrekturmaßnahmen sowie Prioritäten bestimmt und in einen konkreten Maßnahmenplan überführt. Anhand des abgeleiteten Projektplans mit Arbeitspaketen und benötigen Ressourcen kann eine erste Kostenschätzung für die Budgetplanung sowie mögliche Realisierungszeiträume ermittelt.

3.1.4 Abschluss-Präsentation

Bei der Abschlusspräsentation werden die vorherigen Ergebnisse als Zusammenfassung (Management Summary) aufbereitet und der Geschäftsführung des Krankenhauses vorgestellt. Zudem wird ein entsprechend ausgearbeiteter Projektplan zur Einführung des ISMS vorgelegt, um eine Umsetzungsentscheidung der ermittelten Maßnahmen durch die Leitungsebene zu ermöglichen.

In der Praxis hat es sich als vorteilhaft erwiesen, bereits bei der GAP-Analyse entsprechende technische Werkzeuge (ISMS-Tools) einzusetzen. Das hat die Vorteile, dass man quasi an die Hand genommen wird und die gewonnen Informationen bei der Einführung eines ISMS weiterverwendet und fortgeschrieben werden können.

Aktuell wird der Aufwand für die Durchführung einer GAP-Analyse für ein Krankenhaus mit ca. 300 Betten auf ca. 12PT geschätzt.

Weiterhin sollte für die Umsetzung der GAP- Analyse die Bereitstellung von internen Ressourcen von mindestens 50% eines externen Beraters erfolgen. Diese Aufwände können durch den Einsatz eines ISMS- Tools u. U. weiter reduziert werden.

3.1.5 Beispiele

	Interviewplaner Klinik			Dauer der Interviews		7,8	Stunden	Interviewtermine							
				einsch. Vor- & Nachbereitung		11,6	Stunden	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit	xx.xx Uhrzeit
Pos	Prozessverantwortung Rolle	Interview-termin bestätigt	Prozess	Name	Anzahl Control	Zeit für Interviews /Control in Minuten	Anwesenheit ISB	Session-1	Session-2	Session-3	Session-4	Session-5	Session-6	Session-7	Session-8
1	Vorstand					45	x								
2	Risikomanagement					60	x								
3	Medizintechnik					60	x								
4	Qualitätsmanagement (Roxtra)					60	x								
5	IT-Abteilung					60	x								
6	Informationssicherheitsbeauftragter (ISB)					60	x								
6	Datenschutz (DSB)					60									
7	Einkauf / Apotheke					60	x								
8							x								
9							x								
						465									
						465	465	60	60	60	60	60	60	60	45

Abbildung 6: Interview-Planung (eigene Darstellung)

Erklärung zur Anwendbarkeit / Statement of Applicability (SoA)																
DIN ISO/IEC 27001:2015 Annex A	DIN EN ISO 27799:2016		Anwend-barkeit (ja/nein)	Umgesetzt (ja / nein / in Arbeit)	Grund für Auswahl / Ausschluss					Begründung für die Anwendbarkeit bzw. für die Nicht-Anwendbarkeit	Dienstanweisung Informations-technologie (DA00XX)	DA Umgang mit Medizingeräten (DA00XX)	VA Handbuch Medizininformatik	VA Handbuch Informationssicher heit (ISMS)	Weitere
					entf. Anforderungen	trägt. Anforderungen	kein Risikoanalyse	IT Practice	Nz relevant						
A.5		Informationssicherheitsrichtlinien													
A.5.1		Vorgaben der Leitung für Informationssicherheit													
A.5.1.1	5.1.1	Informationssicherheitsrichtlinien	Ja	Ja				X		Die "Leitlinie Informationssicherheit" und alle weiteren ISMS Rahmedokumente sind allen Beschäftigten über das BabDok Intranet zugänglich. Die "Leitlinie Informationssicherheit" soll sicher stellen, dass alle interessierten Parteien über die Erfordernisse des ISMS und die damit geltenden Regularien informiert sind. Die Organisation sieht dies als notwendig an um mögliche Sicherheitsvorfälle zu vermeiden.	x	x	x	Kap. 4 & 5	Informationssicherheitspolitik: *ISMS-E1-00-Leitlinie_Informationssicherheit *ISMS-E2-01-RL-InfoSec-Organisation *Dokumente in 040-Liste-IS-Dokumente - alle Dokumente?
A.5.1.2	5.1.2	Überprüfung der Informations-sicherheitsrichtlinien	Ja	Ja				X		Die "Leitlinie Informationssicherheit" basiert auf aktuellen politischen, gesetzlichen und wirtschaftlichen Faktoren sowie strategischen Planungen. Diese Faktoren befinden sich im ständigen Wandel und führen ggf. zu notwendigen Anpassungen in den Dokumenten des ISMS					*Lenkung der Dokumente in 040-Liste-IS-Dokumente

Abbildung 7: Auszug aus SoA (eigene Darstellung)

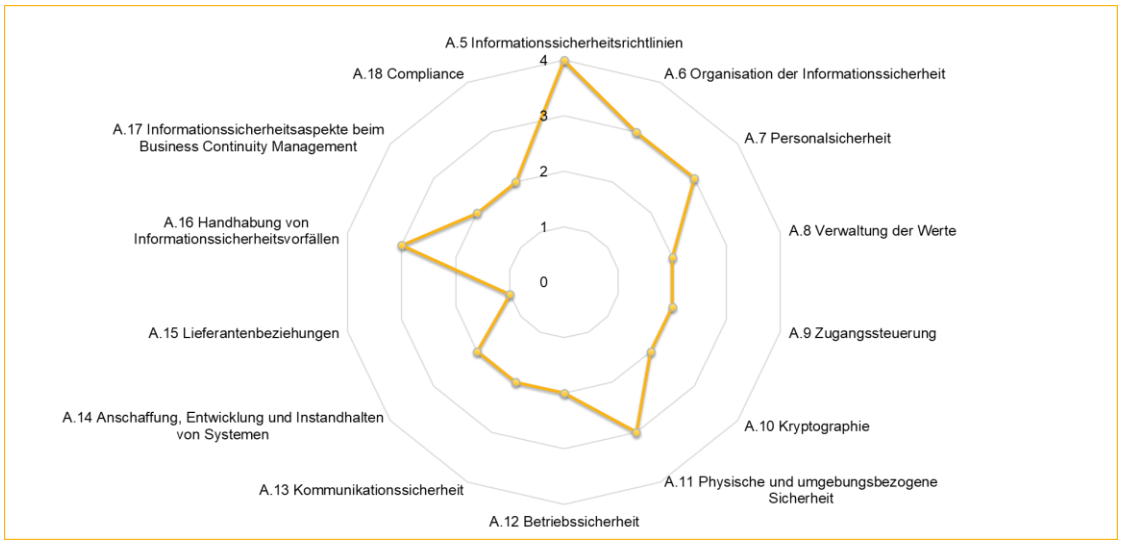

Abbildung 8: Reifegrad-Bewertung nach ISO27001 auf Basis Annex A (eigene Darstellung)

Kapitelnummer	Kapitel
-	Feststellung Prüfergebnis B3S Kap 7.2 bis 7.13.19

Inhalt

SA = Schwerwiegende Abweichung
GA = geringfügige Abweichung
VP = Verbesserungspotential
PA = Positiver Aspekt

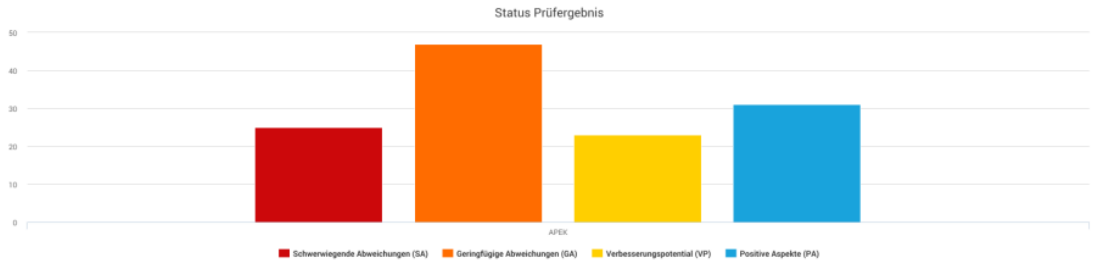

Abbildung 9: Beispiel für Prüfergebnis (eigene Darstellung)

6. Ein vergleichbarer Vertrag zu Wartung , Betrieb und Beschaffung netzgebundener Medizintechnik entsprechend der DIN 80001-1 existiert nicht (akt. Beispiel, Einführung PDMS).
7. Als Krankenhausinformationssystem (KIS) wird ORBIS eingesetzt, dies verfügt über eine eigenes Zugangskontrollsystem, Backupkonzept, Patchmanagement.
8. Ein einheitliches Rechte und Rollenkonzept und somit die Integration in dien lokalen Verzeichnisdienst (AD) besteht nicht.
9. Durch Umbaumaßnahmen wurden die Rechenzentren in beiden Standorten auf den neuesten Stand der Technik gebracht, einschließlich elektronische Zugangskontrolle

12. Für den Aufbau des ISMS muss ein Informationssicherheitsbeauftragter (ISB) von der Leitung bestellt werden. Der ISB sollte in seiner Arbeit intern und extern unterstützt werden.

Abbildung 10: Auszug aus Management Summary (eigene Darstellung)

Über alle so identifizierten Projekte muss eine Projektplanung inkl. Budgetbereitstellung unter Berücksichtigung der Abhängigkeiten und Prioritäten der Teilprojekte erstellt werden.

Anhang A – Verzeichnisse

Abkürzungen

Kürzel	Erläuterung
GAP-Analyse	Analyse der Lücke zwischen Sollvorgabe und Istzustand
SoA	Statement of Applicability (Erklärung der Anwendbarkeit)
ISMS	Information Security Management System
B3S	Branchenspezifischer Sicherheitsstandard für das Gesundheitswesen im Krankenhaus
GF	Geschäftsführung

Glossar

Begriff	Erläuterung

Abbildungsverzeichnis

Tabellenverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

B3S	Deutsche Krankenhaus Gesellschaft 22.10.2019
ISO27001	International Organization for Standardization Juni 2017

Offene Punkte / Klärungsbedarf <optional>

Kap./Abs.	Offener Punkt	Zuständig