TLP-White für Audit-Teams, Prüfende Stellen und KRITIS-Betreiber

Kommentierung OH §8a Nachweisführung V1.1 des BSI aus Sicht der Branche „medizinische Versorgung“ mit Fokussierung auf den B3S „med. Versorgung“ V1.1 vom 22.10.2019.

Autoren:

BAK AK Prüfnachweis: Dr. S. Bücken (UKER), Dr. H. Beck (UMG),
Dr. R. Schieweck (Agaplesion), M. Biche (Agaplesion Mitteldeutschland),
B. Töpert (Alb Fils Kliniken), V. Götzfried (BSI)

Im Informationsaustausch/Einbezug folgender Prüfender Stellen:

Sana Management Service GmbH
AuraSec GmbH
HiSolutions AG
DEKRA Certification GmbH
Sollence GmbH
CETUS Health IT Leadership Gesellschaft für Digitalisierung und Service mbH
Deutsche Managementsystem Zertifizierungsgesellschaft mbH
DQS GmbH
KPMG AG
Datenschutz cert GmbH
TÜV TRUST IT GmbH
Institut Prof. Dr. Becker
TÜV Süd
Adiccon GmbH
AUDEG - Deutsche Auditoren eG
Rödl&Partner GmbH

Freigabe durch den BAK „med. Versorgung“ am 12.11.2020

Einleitung

Betreiber Kritischer Infrastrukturen müssen gemäß § 8a (1) BSIG ihre **Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind**, gegenüber dem BSI auf geeignete Weise nachweisen. Ein Nachweis gemäß §8a (3) muss sich demzufolge auf diese Vorgaben fokussieren.

Das vorliegende Dokument soll KRITIS-Betreibern der Branche „medizinische Versorgung“ und Prüfenden Stellen ein **gemeinsames Prüfverständnis** erlauben, wie – vor dem Hintergrund des **B3S „med. Versorgung“ in der Version 1.1 als Prüfgrundlage** - ein Nachweis gemäß „OH §8a Nachweisführung V1.1“ (im Weiteren „OH §8a V1.1“) sinnvoll durchgeführt werden kann. Das gemeinsame Verständnis der Anforderungen soll u.a. durch Vorschläge für Nachweisdokumenten-Design (insbesondere Geltungsbereich und Netzstrukturplan), die Prüfnachweisplanung durch Anwendung des „BAK Prüfnachweisplaner-Tool V3.0“ sowie branchenspezifische Fallbeispiele gestärkt werden.

Eine Nachweisführung im Sinne einer „B3S-Checklisten-Prüfung“ ist im Branchenkontext weder zielführend, um den Anforderungen des §8a (3) BSIG gerecht zu werden, noch gewollt. **Prüfschwerpunkt müssen die angemessenen organisatorischen und technischen Maßnahmen zur Absicherung der informationstechnischen Systeme, Komponenten und Prozesse im individuellen Betreiberkontext sein!**

Abgrenzung:

Ein Nachweis gemäß §8a (3) BSIG ist **keine Überprüfung des generellen Business-Continuity-Managements** eines KRITIS-Betreibers im Sinn des betriebswirtschaftlichen Sprachgebrauchs und auch **keine Überprüfung des Datenschutzmanagementsystems** gemäß DSGVO, auch wenn der Nachweis gemäß §8a (3) natürlich in Teilbereichen das betriebliche Kontinuitätsmanagement und das technische Datenschutzkonzept eines Krankenhauses berührt.

Es ist zudem nicht Ziel dieses Dokuments einen standardisierten Prüfplan für den Nachweis nach §8a (3) gemäß der Prüfgrundlage B3S „med. Versorgung“ vorzuschreiben. **Es sollen vielmehr Grundsätze der Nachweisführung im Branchenkontext „med. Versorgung“ auf Basis des gültigen B3S V1.1 als Prüfgrundlage vorgeschlagen und Empfehlungen für diese Nachweisführung gegeben werden.**

Festlegung des Geltungsbereiches und Netzstrukturplan

Für eine Bewertung von ISMS und Maßnahmenplanung eines KRITIS-Betreibers ist die Abgrenzung des Geltungsbereiches (Scope) und eine Übersichtsdarstellung des KRITIS-Kontextes im Netzbereich (Netzstrukturplan) sowie ein kDL-systembezogenes Risikomanagement bei der Nachweisführung von entscheidender Bedeutung. Ohne eine entsprechende Abgrenzung des Geltungsbereiches der Kritischen Dienstleistung (kDL) ist eine zielgerichtete Stichprobenfestlegung für das Audit-Team nicht möglich. „Anhang C“ der „OH §8a V1.1“ definiert die grundsätzlichen Anforderungen an die Geltungsbereichsdarstellung durch das BSI.

Krankenhäuser werden in einem reglementierten Kontext betrieben und verfügen i.d.R. über differenzierte Darstellungen ihres Betreiberkontextes in Form von strukturierten Qualitätsberichten

und entsprechende Organigramme, die öffentlich zugänglich sind. Ein Audit-Team kann sich also beispielsweise schnell einen Überblick verschaffen, in dem es vom Betreiber die Markierung des Geltungsbereiches kDL auf dem Organigramm einfordert. Diese modifizierte Organigramm-Darstellung bietet sich demzufolge auch als ein Bestandteil der Anlage zum „Nachweisformular P“ des BSIG, bei der Nachweisführung an.

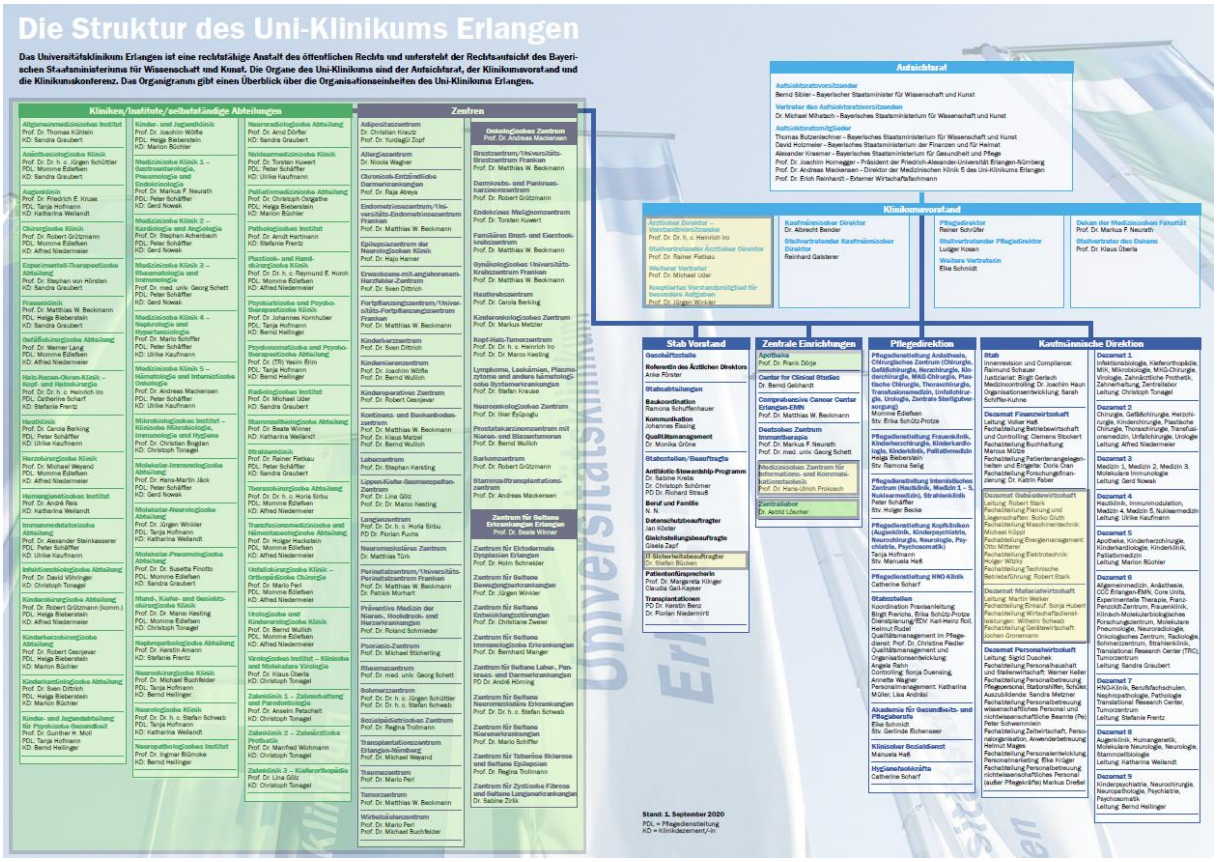

Abb. 1: Organigramm eines KRITIS-Krankenhauses mit Markierung der kDL-relevanten Funktionseinheiten

Über die Anforderungen des B3S hinaus, ist in der Anlage ein Beispiel für eine differenzierte Prozess-zu-Funktionsabteilungsanalyse beigefügt. Es handelt sich hierbei um einen Ausblick auf eine mögliche Anforderung, die bezüglich des ***aktuell gültigen B3S jedoch keine (!) Muss/Soll-Vorgabe*** *darstellt. Dieses Beispiel soll das Audit-Team jedoch darauf aufmerksam machen, dass die im B3S aufgezeigten Hauptprozesswege eines KRITIS-Krankenhauses sehr komplexe Abhängigkeiten in Bezug auf die Prozess-zu-Funktionsabteilungs-Zuordnung aufweisen können, die bei der Prüfung der Festlegung des Geltungsbereichs im Gespräch mit dem Betreiber berücksichtigt werden sollten.*

Risikomanagementprozess

Der Geltungsbereich ist für die Branche „medizinische Versorgung“ gemäß KRITIS-Verordnung auf die Stationäre Versorgung und alle Funktionsbereiche eines Krankenhauses festgelegt, die zu dieser Kritischen Dienstleistung im Rahmen des Betriebes von informationstechnisch relevanten Informationssystemen beitragen. Der B3S gibt bezüglich dieser für die kDL-Erbringung wichtigen Systeme und Funktionseinheiten (u.a. DIN 13080) einen umfassenden Überblick. Auch gibt der B3S eine Definition der wichtigsten kDL-relevanten Informationssystem-Klassen im Krankenhaus vor.

Hierbei bleibt er abstrakt an dem Hauptprozessen des stationären Betriebes und den Überbegriffen der Systeme orientiert (siehe hierzu B3S, S. Kap. 5.2,1 bis Kap. 5.2.1.5).

Auf Basis dieser B3S-kDL-Hauptsystemklassen erstellt der Betreiber im Rahmen des vorgegebenen B3S-Risikomanagementansatzes eine Liste der für die kDL-Hauptprozesse wichtigen Informationsmanagementsysteme und bewertet diese in Bezug auf ihre Kritikalität für die Erbringung der Kritischen Dienstleistung nach drei Kritikalitäts-Klassen (siehe hierzu B3S, Kap. 4.3 sowie Kap. 5.2.2 bis Kap. 5.2.3.11 und Kap. 6.5 ff.).

Es handelt sich bei diesem Vorgehen um ein Kernelement des Risikomanagements eines ISMS im Krankenhaus nach B3S.

Vor dieser Grundrisikobewertung der kDL-relevanten Informationssysteme tritt eine formalisierte, detaillierte Gefährdungslage- und Risikobewertung einzelner kDL-relevanter IT-Systeme nach dem Vorgehensmodell "Bedrohung und Schwachstelle ergeben eine Gefährdung" der im B3S genannten Schutzziele gemäß B3S Kap. 6 bis Kap. 6.3 ff. bei der Bewertungsrelevanz zurück. Wichtig ist in Bezug auf die B3S Schutzziele die gelebte Risikokultur und die tatsächliche Absicherung der Funktionsfähigkeit des KRITIS-Betreibers bezüglich der Erbringung der Kritischen Dienstleistung. Das Audit-Team muss hier jedoch dringend prüfen, ob die Risikoklassifizierung des KRITIS-Betreibers nachvollziehbar und sinnvoll erfolgt ist.

==========
Beispiele für Kritikalitätsentscheidungsbegründungen:

Beispiel 1.1: Klasse der Sonographiegeräte wird mit Risikoklasse 3 – nicht kritisch – bewertet.
Betreiberbegründung: Das Krankenhaus verfügt über n-Sonographiegeräte, die bei einem Ausfall/Kompromittierung das geforderte Leistungsspektrum im Kontext der kDL durch Geräteredundanz abdecken.
Kommentar: Nachvollziehbar, wenn eine entsprechende Inventarliste diese Redundanzsysteme ausweist.

Beispiel 1.2.: Das Labor-System wird mit Risikoklasse 3 – weniger kritisch – bewertet.
Betreiberbegründung: Zur Not kann man die Prozesse auch per Papierworkflow abwickeln.
Kommentar: Es geht um die grundsätzliche Verfügbarkeit des Systems und nicht um eine mögliche Ersatz-/Notfalllösung, zudem müssen Labor-Automaten ihre Daten im Regelbetrieb einspeisen können. Die kDL kann bei einem Systemausfall nur in Teilen und nicht im vollständigen Umfang aufrechterhalten werden.

Beispiel 1.3: Das KIS-system wird vom Betreiber mit Risikoklasse 3 – wenig kritisch – bewertet.
Betreiberbegründung: Wir arbeiten mit einem externen Dienstleister zusammen, dass KIS-System gehört also nicht zu unserem Systemportfolio, da fremdbetrieben.
Kommentar: Auch ausgelagerte aber für die kDL-Erbringung wichtige Informationssysteme, haben aus der Perspektive der kritischen Dienstleistung eine hohe Kritikalität für die Funktionsfähigkeit des Betreibers. Es muss somit eine sorgfältige Risikobetrachtung erfolgen und die Verfügbarkeit des Systems vertraglich und technisch sichergestellt werden.

(Legende: Grün – akzeptabel/ Rot – nicht akzeptabel)
==========

Aufgrund der sich überlagernden Risikomanagementsysteme im Krankenhauskontext (betriebswirtschaftlich, medizinisch und informationssicherheitstechnisch) kommt es teilweise zu

einer Missinterpretation bei der Anforderung „ein Risikomanagement vorweisen “. Nachweisschwerpunkt sind gemäß §8a (1) BSIG die zur Absicherung der Funktionsfähigkeit des KRITIS-Betreibers ergriffenen Maßnahmen bezogen auf die informationstechnischen Systeme, Komponenten oder Prozesse. Dies muss daher auch von den Audit-Teams fokussiert und überprüft werden. Es reicht somit nicht aus, „**ein Risikomanagementsystem**“ am Krankenhaus vorweisen zu können. Wie z.B. auch in dem Leitdokument „RiKrIT“ (Risikomanagement in der Krankenhaus-IT, BSI/BBK) vorgeschlagen, ist es andererseits sinnvoll das Risikomanagement im Krankenhaus methodisch aufeinander abzustimmen. Es ist jedoch nicht Ziel des Nachweises nach §8a (3) das gesamte Risikomanagement eines Krankenhaus-Betreibers zu prüfen, sondern nur den Teil des Risikomanagements der sich auf die kDL-relevanten informationstechnischen Systeme, Komponenten und Prozesse bezieht.

Die korrekte Abgrenzung von Geltungsbereich und Risikomanagementfokussierung ist somit die Grundlage für eine korrekte Nachweisführung gemäß B3S im Rahmen der vorgeschlagenen Stichprobenauswahl bzw. dem Prüftagekontingent (ACHTUNG: keine Personentage!), welches mittels des Prüfnachweisplaner-Tools vorgeschlagen wird.

Netzstrukturplan

Neben der Abgrenzung des Geltungsbereiches für den Nachweis gemäß §8a (3) fordert die „OH §8a 1.1.“ in „Anlage C“ einen Netzstrukturplan des Krankenhausbetreibers. Im Gegensatz zu anderen KRITIS-Sektoren handelt es sich bei den sogenannten „Anlagen“ der Kritischen Infrastruktur „med. Versorgung“, um Krankenhäuser, die eine Vielfalt von medizinischen Behandlungsprozessen abzubilden haben und daher im Netzwerkaspekt hoch komplex und i.d.R. auch hoch divers sind. Es bietet sich daher an, diese Komplexität abstrakt auf grundsätzliche Netzwerkstrukturen zu reduzieren. Der B3S gibt hier kein Format vor. Ein Beispiel für eine derartige Darstellung mit einer Reduktion der Komplexität, die in der Darstellung dennoch gut erkennen lässt, wie sich die Netzstruktur des Betreibers aufbaut, geben die folgenden Skizzen, die als Diskussionsbasis mit den KRITIS-Betreibern dienen können. Eine Übermittlung von detaillierten, technischen Netzplan-Unterlagen oder zu groben Netzstruktur-Darstellungen ist weder für den Nachweisprozess noch für die Nachweisführung gegenüber dem BSI sinnvoll.

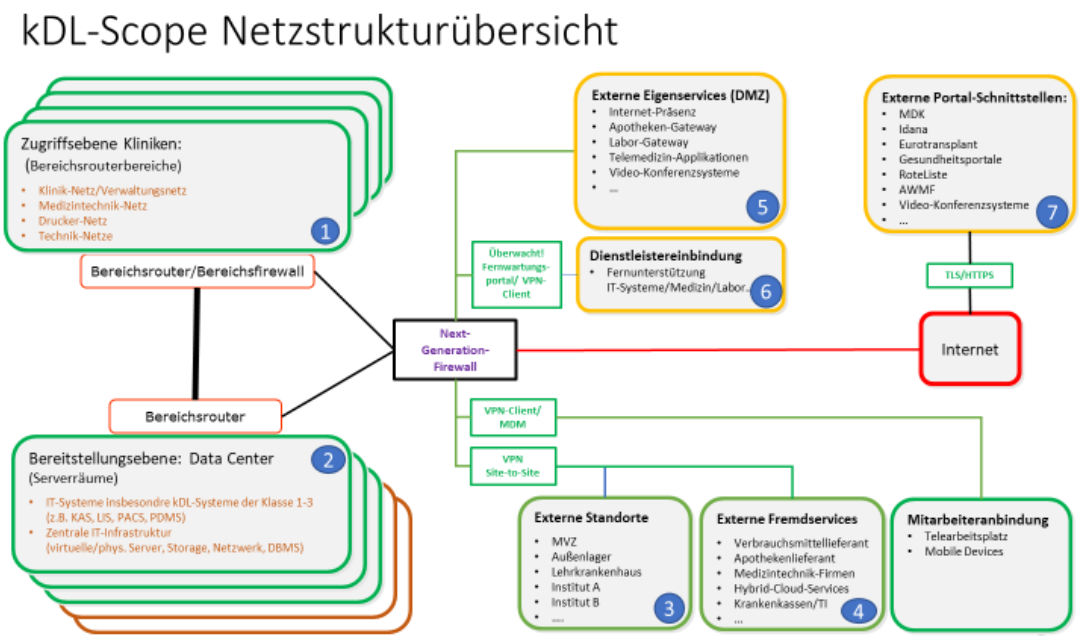

Abb. 2.: Beispiel für eine Netzstrukturübersicht, die Bereitstellungsebene, Zugriffsebene, Externe Standorte, Extern eingebundene Fremdservices, Mitarbeitereinbindung, Dienstleistereinbindung mit den Hauptkommunikationswegen im Netz erkennen lässt und mittels Referenzierung auf Beiblätter (Nummern) entsprechend erweiterbar ist.

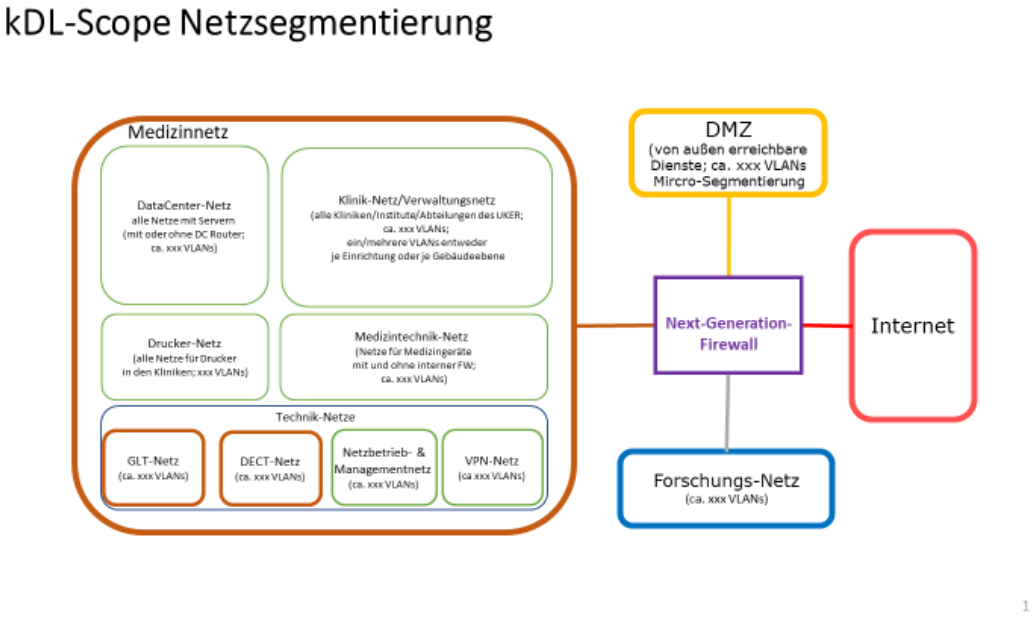

Abb. 3: Beispiel für eine Netzsegmentierungsübersicht, welche einen schnellen Überblick über die Segmentierungsstrategie des KRITIS-Betreibers erlaubt.

Prüfnachweisplaner-Tool

Der BAK „med. Versorgung“ veröffentlicht ein auf einer Excel-Datei basierendes Prüfnachweisplaner-Tool, welches insbesondere die Angebotsabstimmung und die konkrete Prüfplanung im Kontext eines §8a-Nachweises auf Basis des B3S „med. Versorgung“ zwischen Prüfenden Stellen und KRITIS-Betreibern vereinfachen soll. Es ist als **Prozessunterstützung mit Empfehlungscharakter** und nicht als striktes Vorgabeinstrument gedacht. In Grenzen kann das Prüfnachweisplaner-Tool für andere Prüfgrundlagen im Kontext „med. Versorgung“ sicher als Orientierung genutzt werden. Das Prüfnachweisplaner-Tool ist jedoch, genauso wie das vorliegende Dokument, auf den Nachweisprozess nach B3S V.1.1 fokussiert. Andere Prüfgrundlagen, wie es im Prüfnachweisplaner-Tool der ersten Version der Fall war, sind aufgrund des nun verfügbaren B3S im aktuellen Prüfnachweisplaner-Tool nicht mehr enthalten.

Im Wesentlichen bildet das Prüfnachweisplaner-Tool folgenden Prozessschritte im Nachweisgeschehen ab:

1.) Anfrage der Betreiber bei potentiellen Prüfenden Stellen und Eingrenzung des Prüftageumfangs für den Nachweis gemäß §8a (3). Dieser **Prüftageumfang ist eine reine Empfehlung**, die eine Orientierung für einen sinnvollen Prüfumfang bei einem Nachweis nach B3S geben soll. Es obliegt dem Betreiber und der Prüfenden Stelle zu ermitteln, ob die Empfehlung für die spezifische Nachweissituation passend ist. Ziel ist es, sich mit der Prüfenden Stelle über ein Prüftagekontingent als Basis eines Angebotes zu einigen, ohne sicherheitsrelevante Daten an die Prüfende Stelle abzugeben.

   Alternativ können mit den vom Betreiber adressierten Prüfenden Stellen in einem Vorauswahlverfahren Geheimhaltungsvereinbarungen getroffen werden, die dann einen offeneren Umgang mit sensiblen Informationen (z.B. Vorprüfungsnachweisen u.ä.) erlauben.

   Der BAK gibt bezüglich der Angebotsphase die dringende Empfehlung keine sensiblen Unterlagen oder Dokumente an adressierte, potentielle Nachweis-Partner ohne vertragliche Absicherung herauszugeben!

2.) Festlegung der groben Prüftage-Verteilung auf die empfohlenen Prüfschwerpunkte ISMS, Basis-IT-Absicherung und kDL-Systemabsicherung durch die Prüfende Stelle/Audit-Teams, auf Basis der vom Betreiber zur Verfügung gestellten Informationen, also der Liste der kDL-relevanten und risikobewerteten Informationssysteme, der Nachweisdokumente der vorhergehenden Nachweiszyklen und ggf. verfügbarer Zertifikatsnachweise.

3.) Festlegung der Detailprüfungsschwerpunkte durch die Prüfende Stelle/die Audit-Teams gemäß der B3S-Schwerpunktrasterung bzw. den Nachweisschwerpunkten ISMS, IT-Basis-Absicherung, kDL-Informationssystemabsicherung.

4.) Dokumentation des Prüfablaufes gemäß „OH §8a V1.1“, „Anhang B“.

Angebotserstellung mit dem Prüfplaner-Tool

Ziel: Die Vergleichbarkeit des Prüfumfangs zum Zweck der Qualitätssicherung und Ressourcenplanung für Prüfende Stelle und Betreiber sicherstellen**.** Abstimmung des Angebots ohne vorab vertrauliche Informationen austauschen zu müssen.

Abgrenzung: Das Prüfnachweisplaner-Tool schlägt ein Prüftagekontingent vor und nicht (!) die Personentage. Es geht bei der Prüfplanungsunterstützung durch das Excel-Tool um die Prüfungsintensität und nicht um die Prüftageverteilung oder die personelle Organisation der Prüfung.

Für das Nachweisgeschehen selbst, wird in der „OH §8a V1.1“ ansonsten ein Vier-Augen-Prüfkontext als SOLL-Vorgabe vorgeschlagen. Diese Vorgabe ist in jedem Fall dann bei der Prüfungsplanung zu berücksichtigen, wenn der Einbezug entsprechender Branchenkenntnis im Nachweisverlauf ergänzend zu den Kompetenzen „Audit-Führung“ und „IT-Sicherheitstechnologie“ dringend geboten ist.

Ablauf-Empfehlung:

- KRITIS-Betreiber fordert auf Basis des B3S & Prüfplaner-Tool ein Angebot an. Das Prüfplaner-Tool gibt hierzu eine Empfehlung für ein Prüftagekontingent nach Betreiberkomplexität (Fachabteilungen/vollstationäre Fälle). Der in der Prüftagematrix vorgeschlagene Kontingentwert inkl. des ggf. notwendigen Hebefaktors muss vom Betreiber ausgewählt werden. Überprüfbar ist die vom Betreiber getroffene Einordnung gemäß seines Komplexitätsgrades nach Fallzahlen und Fachabteilung i.A. unter https://www.deutsches-krankenhaus-verzeichnis.de/.
- Die Prüfenden Stellen können bei ihrer Angebotsfindung Vorzertifizierungen und ggf. andere Tatbestände berücksichtigen. Dies kann zu einer Reduzierung, einer Prüftagesteigerung und/oder Prüfungsschwerpunktverschiebung führen. Hierzu muss der Betreiber die z.B. Zertifizierungsunterlagen an die Prüfenden Stellen vor Angebotserstellung übergeben.

Bezüglich der zu berücksichtigenden Zertifizierungen ist zu beachten, dass es sich hierbei um aktuelle **Informationssicherheitszertifizierungen**, z.B. nach ISO 27001 oder BSI-Grundschutz u.a., handeln muss. Zudem ist der adressierte Geltungsbereich/Scope und die Fokussierung der Zertifizierung auf die Vorgaben des BSIG zu prüfen, bevor diese Vorzertifizierung akzeptiert wird. Vergleiche hierzu auch BSI-FAQ „Nutzung eines bestehenden ISO 27001-Zertifikates als Bestandteil eines Nachweises gemäß §8a (3) BSIG".

https://www.bsi.bund.de/DE/Themen/KRITIS/FAQ/FAQ_ISO27001/faq_ISO27001_node.html
(Stand vom 04.11.2020)

Die **Abb. 1** und **Abb. 2** zeigen die Eingabemasken der Betreiberangaben, die für eine Angebotserstellung und eine zielgerichtete Prüfplanung durch die Prüfende Stelle notwendig sind.

KRITIS-Branche "medizinische Versorgung"

BAK Handlungsempfehlung 2020 zur B3S V1.1 10/2019 Nachweisführung

TLP-White | Vers. 3.0/2020 | © BAK "medizinische Versorgung" 12.11.2020

Autoren: Markus Biche (Agaplesion Mitteldeutschland), Jürgen Schwestka (Rödl&Partner), Dr. Stefan Bücken (UKER), Alexander Häußler (TÜV Süd)

Prüfumfang und Prüfplanungs-Sheet: Prüfplan B3S "medizinische Versorgung"

Name und Anschrift des KRITIS-Betreibers:	Musterklinik, Neustadt	Prüfjahr:	2021
Name und Anschrift der "Prüfenden Stelle":	Musterprüfer, Helmstadt		

Tabelle zur Ermittlung des Prüftagekontingentes nach Betreiberkomplexität:		Voll-Stationäre Fälle				
Anzahl Fachabteilung		30000-40000	40001-50000	50001-60000	60001-70000	>70000
Fachabteilungen nach §301-Datenübermittlung	<=20	10	10	11	11	12
	<=30	11	11	12	12	13
	<=40	12	12	13	13	14
	<=50	13	13	14	14	15
	<=60	14	14	15	15	16
	>60	15	15	16	16	17
Forschung und Lehre-Faktor	Hebefaktor Normalkrankenhau	1,0	1,0	1,1	1,2	1,3
Universitätsklinikumsfaktor	Hebefaktor Universitätsklinika	1,2	1,2	1,3	1,4	1,6

Empfehlung Prüftage (PRT)	passenden Wert für das Prüftagekontingent für Ihr Klinikum aus obiger Tabelle	13	Hebefaktor Forschung und Lehre:	1,0	hell graue Felder zur Texteingabe! Orange Auswahlfelder! Löschen im Eingabeteil: "rechte Maustaste" & "Inhalte löschen" im Eingabefeld
Reduktion oder Zuschlag in Prüftagen durch Vorzertifizierung, Redundanzprüfungspotential bzw. Zusatzaufwand (Abzug mit "-" eintragen!)		-2	Rechenzetrum ISO27001 zertifiziert		
Verhandeltes Prüftage-Kontingent	1PRT = 8h	11	Begründung Zu- oder Abschlag (oberhalb)		

*) PRT=Prüftage als Gesamtumfange der Prüfung, unabhängig von der Zusammensetzung des Prüfteams

Vom Betreiber an die Prüfende Stelle nach Abschluß einer Geheimhaltungsvereinbarung zu übermittelten Anlagen	
Übersicht Informationsverbund	Übergabe nach Vertragsschluß
IT-Sicherheitskonzept	Übergabe nach Vertragsschluß
ISMS Dokumentenplan	Übergabe nach Vertragsschluß
Ergänzende Unterlagen:	Vorangegangene Prüfpläne, Zertifzierunsbelege u.ä.
ISO27001- Zerfizierung	Zertifizierungsnachweis

Prüfplanaufteilungsempfehlung nach Prüftagen			
Prüfkategorie		Aufwand in	Kommentar:
Prüfungs-Overhead (Vorprüfung Geltungsbereich, Prüfplan, Reporting - Schritte 1, 2, 5, 6 aus Orientierungshilfe)	ca. 20% des Gesamtprüfvolumens	3	

Abb. 1: Betreiberangabe zur Abstimmung mit der Prüfenden Stelle mit Hilfe des Prüfnachweisplaner-Tools.

Prüfplanaufteilungsempfehlung nach Prüftagen			
Prüfkategorie		Aufwand in	Kommentar:
Prüfungs-Overhead (Vorprüfung Geltungsbereich, Prüfplan, Reporting - Schritte 1, 2, 5, 6 aus Orientierungshilfe)	ca. 20% des Gesamtprüfvolumens	3	
ISMS-Prüfung und Basis-Absicherung/Vorortprüfung + Dokuprüfung	ca. 40% des Gesamtprüfvolumens	4	
kDL-Detailprüfung/Vorortprüfung	ca. 40% des Gesamtprüfvolumens	4	
Summe der festen PTR-Tage	100%	11,00	

Bewertungsmatrix kDL-relevante IT-Systeme

B3S-Kritikalitätsklassen:

Klasse 1: Ausfall der Systeme kann nur kurzfristig kompensiert werden

Klasse 2: Ausfall der Systeme kann mittelfristig kompensiert werden

Klasse 3: Ausfall der Systeme kann längerfristig kompensiert werden

Achtung: Systeme nach Kritikalitätsklassen 1-3 in den vorgesehenen Feldbereichen eintragen!

kDL-relevante Systeme im Informationsverbund - Kritikalitätsklasse 1
Krankenhausinformationssystem (KIS)
Laborinformationssystem (LIMS)
Radiologieinformationssystem (RIS)
Picture Archiving and Communication System (PACS)
Medizintechnik
Kommunikationstechnik
(Siehe B3S Kap. 5.2.2 und 6.5)

Abb. 2: Liste der kritikalitätsbewerten kDL-relevanten informationstechnischen Systeme – Betreiberangabe (Systeme verallgemeinert bzw. vereinfacht).

Nachweisplanung mit dem Prüfplaner-Tool

Ziel: Eine sinnvolle Verteilung des verhandelten Prüftage-Kontingentes auf die Nachweisorganisation und die Prüffelder ISMS-Prüfung, IT-Basis-Absicherung und kDL-System-Detailprüfung, sowie Festlegung der Nachweisstichprobe anhand von B3S-Vorgaben und Liste der kritikalitätsbewerteten kDL-Informationssysteme des Betreibers.

Abgrenzung: Es geht um die Verteilung der vom Prüfnachweisplaner-Tool vorgeschlagenen bzw. zwischen Prüfender Stelle und KRITIS-Betreiber ausgehandelten Prüftage-Kontingentes und nicht um die Personentage, die gemäß der Nachweisstrategie der Prüfenden Stelle für das Audit-Team nötig sind, um eine entsprechenden §8a (3) Nachweis zu führen. Das Prüftage-Kontingent fokussiert die zeitliche Prüftiefe, nicht den personellen Aufwand. Personentage und Tagesätze sind ökonomische Kriterien, die hier nicht adressiert werden.

Ablauf-Empfehlung:

- Die Prüfende Stelle/das Audit-Team legt mit Hilfe des Prüfplaner-Tools, Tab-Sheet „Prüfnachweisplanung“ (**Abb. 3**), die entsprechenden Prüfschwerpunkte fest und gewichtet diese in Bezug auf Overhead, ISMS- Basis-IT-Prüfung und kDL-System-Detailprüfung im Rahmen des verhandelten Zeitkontingentes.

Bezüglich der Festlegung der Prüfschwerpunktfestlegung sollte die Prüfende Stelle/das Audit-Team zumindest die vorhergehende Nachweisdokumente nach §8a (3) vom Betreiber einfordern. Dies dient zum einen dazu, um überprüfen zu können, ob erkannte Mängel aus der Vorprüfung entsprechend der Maßnahmenumsetzungsplanung abgestellt wurden. Zum anderen soll die Sichtung der vorhergehenden Unterlagen dazu dienen, die aktuellen Prüfschwerpunkte so zu wählen, dass es über den mehrjährigen Prüfungsverlauf nicht zu einer einseitigen Prüfung kommt (z.B. immer nur das KIS-System). Zudem sind erhebliche Veränderungen im Kontext der informationstechnischen Systeme, Komponenten oder Prozesse beim Betreiber zwischen den Nachweisterminen zu erfragen und bei der Prüfschwerpunktfestlegung zu berücksichtigen.

Prüfungsplanung:

Prüfungs-Overhead, ca. 20% des Gesamtprüfvolumens

Planungsempfehlung:		3,00	
	Prüffeld	Geplante Tage	Kommentar:
Schritt 1: Vorbereitung der Prüfung sowie Prüfung der Eignung des Geltungsbereichs		1,00	
Schritt 2: Erstellung des Prüfplans		1,00	
Schritt 5: Nachbereitung der Vor-Ort-Prüfung		0,50	
Schritt 6: Erstellung des Prüfberichtes		0,50	
		3,00	100%

ISMS-Prüfung und Basis-IT-Absicherung, ca. 40% des Gesamtprüfvolumens

Planungsempfehlung:		4,00	
Prüffelder ISMS-Prüfung	Prüffeld	Geplante Tage	Kommentar:
Prüffeld 1	Dokumentenprüfung	1,00	
Prüffeld 2	Prüfung der allgemeinen Umsetzung	1,00	
Prüffelder Basis-Absicherung	Prüffeld	Geplante Tage	Kommentar:
Prüffeld 1	Bauliche/physische Sicherheit	0,50	
Prüffeld 2	Asset Management	0,50	
Prüffeld 3	Sichere Interaktion im Internet	0,50	
Prüffeld 4	Absicherung von Netzübergängen	0,50	
		4,00	100%

kDL-System-Detailprüfung, ca. 40% des Gesamtprüfvolumens

Planungsempfehlung:		4,00	
Prüffelder kDL-Systeme	Prüffeld (Auswahlfeld ggf. nach oben scrollen)	Geplante Tage	Kommentar:
kDL-System (Kritikalitätsklasse 1)	Krankenhausinformationssystem (KIS)	1,00	
kDL-System (Kritikalitätsklasse 1)	Laborinformationssystem (LIMS)	0,50	
kDL-System (Kritikalitätsklasse 1)	Picture Archiving and Communication System (PACS)	0,50	
kDL-System (Kritikalitätsklasse 1)	Medizintechnik	1,00	
kDL-System (Kritikalitätsklasse 2)	OP-Planungssystem	0,25	
kDL-System (Kritikalitätsklasse 2)	Systeme der Transportlogistik	0,50	
kDL-System (Kritikalitätsklasse 2)			
kDL-System (Kritikalitätsklasse 2)			
kDL-System (Kritikalitätsklasse 3)	Video-Überwachungsanlage	0,25	
kDL-System (Kritikalitätsklasse 3)			
		4,00	100%

Zusammenfassung der Prüfungsplanung

Abb. 3: Zeitbezogene Prüfschwerpunktsetzung mit Hilfe des Prüfplaner-Tools

Detailplanung mit dem Prüfplaner-Tool

Ziel: Eine am B3S orientierte Festlegung von Prüfschwerpunkten anhand der bei der Nachweisplanung definierten Prüffelder, differenziert nach ISMS-Prüfung, IT-Basis-Absicherung und kDL-System-Detailprüfung, sowie Festlegung der Nachweisstichprobe anhand von B3S-Vorgaben und Liste der kritikalitätsbewerteten kDL-Informationssysteme des Betreibers.

Abgrenzung: Es geht bei der Festlegung der Prüfschwerpunkt nicht um die Definition eines Prüffragensatzes oder des Prüfverfahrens in Bezug auf die Nachweisführung.

Ablauf-Empfehlung:

- Die Prüfende Stelle/das Audit-Team wählt mit Hilfe des Prüfplaner-Tools, Tab-Sheet „Detailplanung“ (**Abb. 4**), die entsprechenden B3S-Prüfschwerpunkte in den verschiedenen vorausgewählten Prüffeldern aus. Zu differenzieren ist die ISMS-Überprüfung, deren Prüfungsschwerpunkt mit Zeitangaben nach Dokumenten und Realitätsprüfung erfolgt. Weiterhin – durch ankreuzen – die Basis-IT-Prüfung, also die Überprüfung der übergreifenden IT-Sicherheitsmaßnahmen, die flächendeckende Wirkung für den Betreiber entfalten und Grundvoraussetzung für einen abgesicherten Betreib der kDL-relevanten IT-System sind. Des Weiteren – durch ankreuzen – die B3S-Prüfschwerpunkttehemen für die kDL-System-Detailprüfung.

Die Detailplanung fokussiert lediglich grob die Prüfschwerpunkte. In Bezug auf die Detailfragestellungen sind die Prüfenden Stellen/Audit-Teams auf ihre eigene Fachkenntnis in den Kompetenz-Domänen „Auditkompetenz, „IT-Sicherheitskompetenz“ und „Branchenkompetenz“ angewiesen. Die Detailplanung setzt den Prüfungsrahmen, gibt aber keine Prüfungsfragen, die Vorortüberprüfungsanforderungen oder ein Nachweise-Dokumente-Portfolio vor.

B3S ISMS Prüfung kDL-Systeme

Nur hellgraue Felder sind aktiv befüllbar!

		Dokumentenprüfung	Prüfung der allgemeinen Umsetzung	Baulicher/physische Sicherheit	Asset Management	Sichere Implantation im Internet	Absicherung von Nutzergeräten	Krankenhausinformationssystem (KIS)	Laborinformationssystem (LIMS)	Picture Archiving and Communication System (PACS)	Notfallmedizin	On-Premisesysteme	Systeme der Transportlogistik	0	0	Weiter Überwachungsanlage	0
		ISMS		Basis-Infrastruktur				kDL-Systeme									
	Planungsempfehlung (Übertrag Sheet "Prüfnachweisplaner"):	1,00	1,00														
	Geplante Tage	1,00	1,00	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage	Geplante Tage
	in Prozent:	100%	100%	0,50	0,50	0,50	0,50	1,00	0,50	0,50	1,00	0,25	0,50	0,00	0,00	0,25	0,00
Systemunabhängige Prüffelder	4.2.5 Risikobehandlung		0,2														
	4.2.6 Risikokommunikation und -überwachung																
	7 Anforderungen und Maßnahmeempfehlungen zur Umsetzung																
	7.1 Informationssicherheitsmanagementsystem (ISMS)		0,2														
	7.2 Organisation der Informationssicherheit	0,2															
	7.2.1 Geschäftsführung / Leitung		0,2														
	7.2.2 Beauftragter für Informationssicherheit (ISB, CISO)		0,2														
	7.2.3 Prozess- /Anwendungsverantwortlicher																
	7.3 Meldepflichten nach § 8b Absatz 4 BSI-Gesetz																
	7.4 Betriebliches Kontinuitätsmanagement		0,2				x										
	7.5 Asset Management				x												
	7.6 Robustefresiliente Architektur																
	7.7 Physische Sicherheit			x													
	7.8 Personelle und organisatorische Sicherheit																
	7.9 Vorfallerkennung und Behandlung					x	x										
	7.10 Überprüfungen im laufenden Betrieb					x	x										
	7.11 Externe Informationsversorgung und Unterstützung																
	7.12 Lieferanten, Dienstleister und Dritte						x										
	7.13 Technische Informationssicherheit																
	7.13.1 Netz- und Systemmanagement (Netztrennung und Segmentierung)							x									
	7.13.2 Absicherung Fernzugriffe							x			x						
	7.13.3 Härtung und sichere Basiskonfiguration der Systeme und Anwendungen								x	x							
	7.13.4 Schutz vor Schadsoftware							x									
	7.13.5 Intrusion Detection / Prevention																
	7.13.6 Identitäts- und Rechtemanagement							x	x								

Abb. 4: Detailplanungs-Sheet des Prüfnachweisplaner-Tools

Nachweisführung gemäß Anlage B „OH §8a 1.1“ mit Hilfe des Prüfplaner-Tool

Ziel: Der letzte vom Prüfplaner-Tool unterstütze Nachweisprozess ist die strukturierte Erzeugung des Nachweisprotokolls gemäß den Vorgaben der „OH §8a 1.1“ durch die Prüfende Stelle/das Audit-Team, welches als Nachweisdokument abschließend durch den Betreiber an das BSI zum Prüfungsnachweis übermittelt werden muss.

Abgrenzung: „Anhang B“ der „OH §8a 1.1“ fordert einen Überblick über den Prüfablauf, dieser ist abzugrenzen von der im „Anhang D“ der „OH §8a 1.1“ geforderten Mängelliste.

Ablauf-Empfehlung:

- Das Tabellenblatt „Anlage_Prüfablauf“ (**Abb. 5**) wird vom Audit-Team in Bezug auf die ausgewählten Prüffelder und Prüfschwerpunkten zeitnah zum Prüfgeschehen ausgefüllt und abschließend ausgedruckt bzw. als PDF den Nachweisdokumenten beigefügt.

Die „Anlage Prüfablauf“ ersetzt keine detaillierte Prüfprotokollführung im Nachweisgeschehen, sondern hat die Aufgabe eine strukturierte Übersicht über das Prüfgeschehen zu erzeugen. Ein ausführliches Auditprotokoll ist weiterhin zu erstellen und dem KRITIS-Betreiber auszuhändigen, so dass dieses bei Nachfragen durch das BSI vorliegt und ggf. bei Detailnachfragen dem BSI je nach Fragestellung in Teilen oder als Ganzes übermittelt werden kann.

Prüfthema	Prüfgrundlage	Art der Prüfung				Prüfmethode								Prüfobjekt	Beteiligte Prüfer	Prozess- bzw. Fachverantwortliche
		Dokumenten-prüfung	Prüfung der Umsetzung	Basis-Absicherung	kDL-System-prüfung	Mündliche Befragung	Inaugenschein-nahme	Dokumenten-analyse	technische Vor-Ort-Prüfung	Penetrationstests	Datenanalyse	schriftliche Befragung	Einsichtnahme bestehender Nachweise			
Branchenspezifischer Geltungsbereich	B3S Krankenhaus, Kapitel 5.1	X	-												Müller	Hansen, Bauer, Fischer
Ergänzende Regelungen zum Geltungsbereich	B3S Krankenhaus, Kapitel 5.2	-	-													
Übersicht der Kernprozesse und Funktionszuordnung innerhalb des Geltungsbereichs	B3S Krankenhaus, Kapitel 5.2.1	-	-													
Festlegung der spezifischen Ziele und Anforderungen des B3S an die	B3S Krankenhaus, Kapitel 5.3	-	-													
Leitlinie zur Informationssicherheit	B3S Krankenhaus, Kapitel 5.4	X	-												Müller	
Management-Anforderungen für die Implementierung eines Informations-	B3S Krankenhaus, Kapitel 4.2	X	-												Müller	
Ermittlung der Risikoobjekte und Risiko-Eigentümer	B3S Krankenhaus, Kapitel 4.2.1	-	-													
Festlegung von Kritikalität	B3S Krankenhaus, Kapitel 4.2.2	-	-													
Risikoidentifikation	B3S Krankenhaus, Kapitel 4.2.3	-	-													
Risikobewertung	B3S Krankenhaus, Kapitel 4.2.4	X	-												Müller/Meier	
Risikobehandlung	B3S Krankenhaus, Kapitel 4.2.5	-	X			x	x	x							Müller/Meier	Hansen, Bauer, Fischer
Risikokommunikation und -überwachung	B3S Krankenhaus, Kapitel 4.2.6	-	-													
Informationssicherheitsmanagementsystem (ISMS)	B3S Krankenhaus, Kapitel 7.1	-	X			x	x	x							Müller/Meier	Hansen, Bauer, Fischer
Organisation der Informationssicherheit	B3S Krankenhaus, Kapitel 7.2	X	-												Müller	Hansen, Bauer, Fischer
Geschäftsführung / Leitung	B3S Krankenhaus, Kapitel 7.2.1	-	X			x		x							Müller/Meier	Hansen, Bauer, Fischer
Beauftragter für Informationssicherheit (ISB, CISO)	B3S Krankenhaus, Kapitel 7.2.2	-	X			x									Müller/Meier	Hansen, Bauer, Fischer
Prozess- /Anwendungsverantwortlicher	B3S Krankenhaus, Kapitel 7.2.3	-	-	-				x							Meier	Peters
Meldepflichten nach § 8b Absatz 4 BSI-Gesetz	B3S Krankenhaus, Kapitel 7.3	-	-	-												
Betriebliches Kontinuitätsmanagement	B3S Krankenhaus, Kapitel 7.4	-	X	X		x	x	x						Absicherung von Netzübergängen	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Asset Management	B3S Krankenhaus, Kapitel 7.5	-	-	X		x			x		x			Asset Management	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Robuste/resiliente Architektur	B3S Krankenhaus, Kapitel 7.6	-	-	-												
Physische Sicherheit	B3S Krankenhaus, Kapitel 7.7	-	-	X		x	x		x					Bauliche/physische Sicherheit	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Personelle und organisatorische Sicherheit	B3S Krankenhaus, Kapitel 7.8	-	-	-												
Vorfallerkennung und Behandlung	B3S Krankenhaus, Kapitel 7.9	-	-	X		x	x	x	x		x			Sichere Interaktion im Internet; Absicherung von Netzübergängen	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Überprüfungen im laufenden Betrieb	B3S Krankenhaus, Kapitel 7.10	-	-	X		x	x	x	x		x			Sichere Interaktion im Internet; Absicherung von Netzübergängen	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Externe Informationsversorgung und Unterstützung	B3S Krankenhaus, Kapitel 7.11	-	-	-												
Lieferanten, Dienstleister und Dritte	B3S Krankenhaus, Kapitel 7.12	-	-	X		x		x						Absicherung von Netzübergängen	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Netz- und Systemmanagement (Netztrennung und Segmentierung)	B3S Krankenhaus, Kapitel 7.13.1			-	X	x	x	x	x					Krankenhausinformationssystem (KIS)	Müller/Meier	Peters, Hansen, Fischer,Ebelein
Absicherung Fernzugriffe	B3S Krankenhaus, Kapitel 7.13.2			-	X	x	x	x	x		x			Krankenhausinformationssystem (KIS); Medizintechnik	Müller/Meier	Dietrich, Hansen, Ebelein
Härtung und sichere Basiskonfiguration der Systeme und Anwendungen	B3S Krankenhaus, Kapitel 7.13.3			-	X					x				Laborinformationssystem (LIMS); Picture Archiving and Communication System (PACS)	Müller/Meier	Dietrich, Hansen, Ebelein
Schutz vor Schadsoftware	B3S Krankenhaus, Kapitel 7.13.4			-	X					x			x	Krankenhausinformationssystem (KIS)	Müller/Meier	Dietrich, Hansen, Ebelein
Intrusion Detection / Prevention	B3S Krankenhaus, Kapitel 7.13.5			-												
Identitäts- und Rechtemanagement	B3S Krankenhaus, Kapitel 7.13.6			-	X	x	x	x			x			Krankenhausinformationssystem (KIS); Laborinformationssystem (LIMS)	Müller/Meier	Dietrich, Hansen, Ebelein
Sichere Authentisierung	B3S Krankenhaus, Kapitel 7.13.7			-	X									Picture Archiving and Communication System (PACS); OP-Planungssystem		

Abb. 5: „Anlage_Prüfablauf-Blatt“ des Prüfplaner-Tools

Grundsätze der Nachweiserbringung

Das Ziel des Nachweises nach §8a (3) ist die Überprüfung angemessener organisatorischer und technischer Maßnahmen zur **Absicherung der Funktionsfähigkeit** des KRITIS-Betreibers in der medizinischen Versorgung (kDL). Hierbei sind insbesondere die informationstechnischen Systeme, Komponenten und/oder Prozesse der kDL im Fokus. Es geht somit um einen IT-risikoorientierten Nachweisansatz der die IT-unterstützten der Prozesse des KRITIS-Betreibers mit der Fokussierung der Erbringung der Kritischen Dienstleistung „stationäre medizinische Versorgung“ fokussiert.

Branchenspezifisch können Krankenhäuser aufgrund der medizinischen Fokussierung aber auch wegen der konkurrierenden MPG-Gesetzgebung, Sozialgesetz- und Krankenhausgesetzgebung nicht zwingend alle IT-sicherheitstechnischen Schwachstellen vollumfänglich mittels anerkannter Verfahren der IT-Sicherheitstechnik beheben oder vermeiden. Es ergeben sich im Kontext der Branche „med. Versorgung“ daher z.T. Risikobehandlungspläne mit Ansätzen zur Risikominderung oder Risikoakzeptanz, welche vor allem die Erbringung der Kritischen Dienstleitung „stationäre medizinische Versorgung“ im Fokus haben und nicht ausschließlich den „Stand der IT-Sicherheitstechnik“. Hierdurch verbleiben teilweise Restrisiken im informationstechnischen Kontext, die vom Betreiber bewusst und begründet akzeptiert werden können und müssen. Es ist somit für das Audit-Team wichtig, insbesondere die Angemessenheit der getroffenen technisch-organisatorischen Maßnahmen des KRITIS-Betreibers in Bezug auf die Sicherstellung der zu erbringenden kritischen Dienstleistung „stat. Versorgung“ zu bewerten. Vor diesem Hintergrund geht es in der Nachweisführung also z.B. nicht ausschließlich darum, technische IT-Sicherheitsstandards, wie z.B. Länge und Entropie eines Passwortes usw., zu bewerten. Auch geht es im Kontext §8a (3) Nachweisführung nicht um die monetären Unternehmensrisiken (Risikomanagement nach KonTrAG oder BCM im betriebswirtschaftlichen Sinne). Es geht vielmehr primär um die Aufrechterhaltung der Funktionsfähigkeit des KRITIS-Betreibers im Sinne der kDL durch angemessene organisatorisch-technische Maßnahmen.

Interpretation der B3S-Prüfgrundlage und Audit-Grundsätze

Der B3S ist ein sich weiter entwickelndes Dokument, welches daher nicht als streng gefasster Prüfkatalog/Checkliste oder als „Stand der Technik“ zur Systemabsicherung in der Branche medizinische Versorgung im absoluten Sinne zu verstehen ist. Er ist in der jetzigen Form viel mehr als Anleitung zum Aufbau eines branchenspezifischen ISMS-Standards zu verstehen. Die Nachweisführung anhand des B3S-Maßnahmenkataloges muss daher immer im Sinne der Aufrechterhaltung der Funktionsfähigkeit der zu erbringenden, kritischen Dienstleistung "stationäre, medizinische Versorgung“ erfolgen. Eine Checklisten-artige Prüfung ist hier weder sinnvoll noch gewollt, so dass insbesondere der Branchenkenntnis im Audit-Team erhebliche Bedeutung zugemessen werden muss.

Grundsätzlich sollte eine Nachweisführung folgendem Grundsatz folgen:

Von außen nach innen (technische Perspektive) und von oben nach unten (organisatorische Perspektive) prüfen!

Die bedeutet zum einen, dass es sinnvoll ist, Maßnahmen zur Absicherung der informationssicherheitstechnischen Systeme, Komponenten und/oder Prozesse in der Rangfolge Außenschutz (Perimeter-Absicherung), Basis-IT-Schutz (Flächenabsicherung), kDL-Systemschutz (Detailabsicherung im kDL-Kontext) unter Berücksichtigung der jeweiligen Risikoklassifizierung zu prüfen. Grundidee muss es hierbei sein, die getroffenen organisatorisch-technischen Maßnahmen in ihrer Schutzwirkung für das Gesamtsystem des KRITIS-Betreibers zu bewerten.

Zum anderen bedeutet der Nachweisgrundsatz, dass primär von der Führungsebene zur Umsetzungsebene zu prüfen ist. Oftmals wird der §8a des BSIG „Sicherheit in der Informationstechnik Kritischer Infrastrukturen“ von der Leitungsebene der KRITIS-Betreiber noch immer als reines IT-Thema und nicht als organisationsübergreifende, ganzheitliche Problemstellung im Betreiberkontext verstanden. Fehlt der operativen Umsetzungsebene jedoch die Rückendeckung durch die Leitungsebene und wurde keine gemäß dem B3S eingeforderte Informationssicherheitsorganisation mit entsprechendem Maßnahmen-Controlling und Reporting an die Leitungsebene etabliert, ist nur im Ausnahmefall davon auszugehen, dass der KRITIS-Betreiber über ein strukturiertes Informationssicherheitskonzept im Sinn des BSIG verfügt.

Mängelliste mit Umsetzungsplan

Die sogenannte Mängelliste soll Mängel bzgl. der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, offenlegen. Die Unterteilung der Feststellungen in schwerwiegende Mängel, geringfügige Mängel und Empfehlungen sollte sich daher ebenfalls an den tatsächlichen Risiken für die Erfüllung der Kritischen Dienstleistung orientieren und nicht an Zertifikatsverfahren oder Formalia, wie z.B. fehlende ISMS-Dokumente. Wichtig ist vor allem die real gelebte Absicherung des KRITIS-Betreibers und nicht der theoretisch-formale Überbau.

Die gemäß „OH 8a 1.1“ geforderte Mängelliste sollte diesem Grundprinzip folgend nur dort zwingend durch einen Umsetzungsplan ergänzt werden, wo schwerwiegende Informationssicherheitsmängel

vorliegen, deren zeitnahe Behebung geboten ist. Primär geht es beim Umsetzungsplan vor allem darum, die Kommunikation mit dem BSI zu erleichtern und Rückfragen durch das BSI zu minimieren. Bei schwerwiegenden Mängeln sind daher geplante Maßnahmen aufzuführen und realistisch zu terminieren. Eine Umsetzungsplanung bei einfachen Mängeln ist nur dann geboten, wenn dies auch sinnvoll möglich ist. Krankenhäuser weisen komplexe Investitions- und Organisationsstrukturen auf. Sie müssen sich zumindest im öffentlichen Bereich an Fördermittelrichtlinien, Ausschreibungsregeln, wettbewerbsrechtliche Regelungen u.ä. im nationalen und europäischen Kontext halten, sodass bei der Beseitigung eines Mangels systembedingt ggf. ein erheblicher, zeitlicher Vorlauf zu berücksichtigen ist.

Grundsätzlich sollten Audit-Teams somit zwischen **Mängel** im Sinne des §8a (1) und **Abweichungen** im Sinne des B3S-Maßnahmenkataloges unterscheiden. Eine Abweichung vom B3S-Maßnahmenkatalog ohne eine erkennbare Gefährdung der Funktionsfähigkeit des KRITIS-Betreibers soll daher dem KRITIS-Betreiber für den internen, kontinuierlichen Verbesserungsprozess offengelegt werden (Empfehlungscharakter), aber nur dann in die Mängelliste gemäß „OH §8a 1.1“ „Anlage D“ übernommen werden, wenn er zu einer Gefährdung des Krankenhausbetriebes führt. Neben der Mängelliste gemäß „Anlage D“ ist somit im Rahmen der Auditdokumentation eine Feststellungsliste in Bezug auf geprüften B3S-Controls zu erstellen und dem KRITIS-Betreiber auszuhändigen. Diese Feststellungsliste kann bei Detailnachfragen dem BSI, je nach Fragestellung, in Teilen oder als Ganzes als zusätzlicher Nachweis übermittelt werden.

==========

Beispiele für Mängelklassifikationen:

Zu einem Dokument (z.B. Regelung zum Patchmanagement) fehlt die Dokumentenlenkung.
Formaler Mangel: Dies sollte nicht als Mangel gewertet werden, da kein direktes Risiko für die Kritische Dienstleistung vorliegt.

Es erfolgt kein koordiniertes Patchmanagement. Die Systeme weisen erheblich veraltete Versionsstände auf, für die es keine nachvollziehbare Begründung gibt.
Tatsächliches Risiko: Da hier die Erbringung der Kritischen Dienstleistung gefährdet ist, muss dies als schwerwiegender Mangel gewertet werden.
(Anmerkung: Dies bezieht sich nicht auf Systemen, bei denen eine Patchmanagement z.B. durch regulatorische Anforderungen ausgeschlossen ist.)

Es gibt keinen formalisierten Freigabeprozess in Bezug auf das Patchmanagement, die betriebenen Systeme werden jedoch administrativ ordnungsgemäß und umsichtig aktualisiert und betrieben. Ein Freigabeprozess ist nur bei größeren Updates vorgesehen.
B3S-Abweichung: ANF-MN 131 wird nicht vollumfänglich erfüllt, es ist jedoch keine unmittelbare Betriebsgefährdung zu erkennen, so dass der Sachverhalt nicht als Mangel zu werten ist.

(Legende: Grün – Feststellungsliste/Rot – Mängelliste gemäß Anlage D)
==========

Ablaufempfehlung: Die Feststellungsdokumentation und die Mängelliste nach „Anlage D“ wird vom Audit-Team erstellt. Der Umsetzungsplan ist vom Betreiber zu erstellen. Eine Abstimmung des Umsetzungsplans zwischen Betreiber und Prüfer ist nicht notwendig. Bei der Planung der Prüfungstermine ist genügend Zeit für die Erstellung des Umsetzungsplans im Nachgang der Prüfung vorzusehen.

ISMS und BCMS Reifegradbestimmung gemäß „Formular P“

Das Ziel des B3S ist es, eine Vorgabe für ein sinnvolles ISMS zu machen. Die Nachweisführung gemäß §8a (3) überprüft somit grundsätzlich die Reife des ISMS gemäß B3S und seinen Umsetzungsstand. Hierzu gehören auch Ausfallkonzepte und entsprechende Maßnahmenpläne für IT-Systeme mit kDL-Bezug. Diese umfassen insbesondere technisch-organisatorische Absicherungsmaßnahmen, Alarmierungspläne sowie Wiederherstellungs- und Wiederanlaufpläne für die kDL-relevanten Informationssysteme aus dem IT-Betriebsaspekt.

Hiervon abzugrenzen ist das betriebliche Kontinuitätsmanagements im Kontext der Kritischen Dienstleistung. Hierunter ist bei der Nachweisführung mit der Prüfgrundlage B3S insbesondere die Reife der organisatorisch-technischen Ersatzverfahren zur Aufrechterhaltung der Verfügbarkeit der kDL beim IT-Ausfall zu verstehen (siehe B3S Kap. 7.4).

Bei beiden Fokussierungen (ISMS/BCM) sind die Einübung der Verfahren und die Überprüfung der Verfahren und Verfahrensübergang von gestörtem zum normalen Betrieb mit zu bewerten.

ISMS: Aspekte, wie die Redundanz technischer Systeme, Wiederherstellungs- und Wiederanlaufplanung usw..

BCM: Aspekte, die das Ersatzverfahren inkl. der hierfür ggf. vorhandenen und nötigen Infrastruktur zur Aufrechterhaltung der kDL im Störfall sowie beim Übergang vom Ersatzverfahren zum Normalbetrieb betreffen.

Abgrenzung: Im Rahmen der Nachweisführung steht nicht das Kontinuitätsmanagement des Wirtschaftsbetriebs im Blickpunkt, sondern die Fokussierung des Nachweises auf die für die kDL wichtigen informationstechnischen Systeme, Komponenten und/oder Prozesse.

Ablaufempfehlung: Die Reife von ISMS und BCM sind im „Nachweisformular P“ vom Audit-Team in Form einer groben Bewertung anzugeben. Hierzu ist der erläuternde Absatz im **„Nachweisformular P, Version 1.0, Stand 10.07.2020**“, zu berücksichtigen.

Ablauf-Empfehlung eines Nachweis-Audits nach Beauftragung durch den KRITIS-Betreiber und Festlegung von Prüftagekontingent und Prüffeldern:

Audit Teil 1:

- Ergebnisse der letzten §8a-Prüfung berücksichtigen mit Mängelliste und Prüfbericht als Grundlage (Klinik erklärt sich bereit die Dokumente an den Prüfer zu übergeben, Prüfer erklärt sich bereit die Prüfpunkte zu berücksichtigen)
- Vorabprüfung und Festlegung der Prüfschwerpunkte auf Basis des IT-Risiko-Managements
- Übergabe Dokumente
    - Übersicht Geltungsbereich/Informationsverbund
    - Klassifizierung der IT-Systeme nach Kritikalitätsklassen (im Prüfplaner-Tool)
    - IT-Sicherheitsrichtlinie / IT-Sicherheitskonzept
    - ISMS-Dokumentenplan
- Beschreibung des internen Kontrollsystems
    - Monitoring Umsetzungstand der Maßnahmen
    - Umgang mit Schwachstellen und Risiken
- Prüfung der Dokumente
    - Angemessenheit des Geltungsbereichs/Informationsverbunds (Anhang C der OH §8a 1.1)
    - Vollständigkeit der Dokumente (Existenz und Inhalt)

Audit Teil 2:

- Audit-Durchführung gemäß der im Prüfplaner-Tool festgelegten Prüffelder und Prüfschwerpunkte unter Berücksichtigung der gemäß OH §8a 1.1, Kap. 5.3 vorgeschlagenen Prüfmethodik mit einer Fokussierung auf die tatsächlichen Sachverhalte und nicht nur auf Basis von vorgelegten Dokumenten/Nachweisen:

    - Mündliche Befragung (Interview)
    - Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten, Gegenständen
    - Dokumentenanalyse (auch elektronische Daten)
    - technische Vor-Ort-Prüfung bzw. gezielte Beobachtung
    - Penetrationstests
    - Datenanalyse (z.B. Logfiles, Firewall-Konfiguration, Auswertung von Datenbanken etc.)
    - schriftliche Befragung (z.B. Fragebögen)
    - Einbeziehung bestehender Nachweise (z.B. Prüfung des Prüfberichtes einer in anderem Kontext vorgenommenen Prüfung).

Audit Teil 3:

Erstellung des Mängelberichtes (siehe Absatz: „Mängelliste mit Umsetzungsplan“, dieses Dokumentes).

- Abstimmung des Mängelberichts (Prüfende Stelle und Betreiber)
- Erstellung Nachweisdokumentation (Nachweisformular P sowie geforderte Anhänge gemäß der Anlage der OH §8a V1.1.
- Erstellung des Umsetzungsplans zu zeitnah und unmittelbar behebbaren Mängeln (siehe Absatz: „Mängelliste mit Umsetzungsplan“, dieses Dokumentes).

Anlage: Beispiel für eine Prozess-zu-Funktionsanalyse/Grundlage der Risikobewertungsmatrix für relevante informationstechnische kDL-Systeme.

Es handelt sich hierbei um einen Ausblick auf eine mögliche Anforderung, die bezüglich des aktuell gültigen B3S keine (!) Muss/Soll-Vorgabe darstellt. Dieses Beispiel soll das Audit-Team jedoch darauf aufmerksam machen, dass die im B3S aufgezeigten Hauptprozesswege eines KRITIS-Krankenhauses sehr komplexe Abhängigkeiten in Bezug auf die Prozess-zu-Funktionsabteilungs-Zuordnung aufweisen können, die bei der Prüfung der Festlegung des Geltungsbereichs im Gespräch mit dem Betreiber berücksichtigt werden sollten.

Funktionsabteilung/ Prozessschritte	P-1.1 Notfallaufnahme-/-Patienten-aufnahme	P-2.1 Anamnese und Stellung von Verdachtsdiagnosen	P-2.2 Diagnoseerstellung	P-2.3 Durchführung von Laboruntersuchungen	P-2.4 Erstellung eines Therapieplans & Verordnungen von Arznei-, Heil- und Hilfsmitteln	P-3.1 Anwendung von Operationsverfahren (inkl. Sterilgutversorgung)	P-3.2 Anwendung medikamentöser, physikalischer, manueller Heilmethoden	P-3.3 Anwendung gerätebasierter Heilmethoden, Einsatz von lebenserhaltenden Technologien, Intensivstation	P-3.4 Bereitstellung von Arznei- und Hilfsmitteln	P-4.1 Visite	P-4.2 Durchführung von pflegerischen Maßnahmen	P-4.3 Sicherstellung der Versorgung /-Hygiene-/-Verpflegung	P-5.1 Erstellung des Arztbriefes mit Medikationsliste, ggf. anschließende Therapieplanung	P-5.2 Entlassung des Patienten und Erläuterungen /Sicherstellung der Medikamentenversorgung ggf. Sicherstellung der poststationären Versorgung, Kurzzeitpflege, etc.
Augenklinik	x	x	x		x	x	x	x	x	x	x	x	x	x
Institut für Rechtsmedizin				x										
Neuroradiologische Abteilung														
…														

Legende:

	Aufnahme
	Diagnose
	Therapie
	Pflege
	Entlassung

Übersicht über die Prozessschritte, Aufgaben und Vorgänge in der Medizinischen Versorgung

Prozessschritt	Prozess	Aufgabe	Relevanz für die kDL
Aufnahme	P-1.1	Notfallaufnahme / Patientenaufnahme	☑
	P-1.3.1	Triage vornehmen	
	P-1.3.2	Patienten anmelden	
	P-1.3.3	Erstanamnese durchführen	
	P-1.3.4	Notfall-Diagnostik durchführen	
	P-1.3.5	Notfall-Dokumentation durchführen	
	P-1.3.6	Notfall-Brief erstellen	
Diagnose	P-2.1	Anamnese und Stellung von Verdachtsdiagnosen	☑
	P-2.2.1	Anamnese medizinisch durchführen	
	P-2.1.2	Anamnese pflegerisch durchführen	
	P-2.1.3	Patient aufklären	
	P-2.1.4	Anforderung/en erstellen *(für Untersuchungen)*	
	P-2.2	Diagnosestellung	☑
	P-2.2.1	Termin planen / Geräte belegen	
	P-2.2.2	Patiententransport zur Diagnostik	
	P-2.2.3	Untersuchung durchführen	
	P-2.2.4	Patiententransport zur Station	
	P-2.2.5	Dokumentation erstellen	
	P-2.2.6	Befund erstellen	
	P-2.2.7	Archivierung durchführen	
	P-2.3	Durchführung von Laboruntersuchungen	☑
	P-2.3.1	Veranlassung	
	P-2.3.2	Transport	
	P-2.3.3	Probeneingang	
	P-2.3.4	Analytik	
	P-2.3.5	Postanalytik	
	P-2.4	Erstellung eines Therapieplans & Verordnungen von Arznei-, Heil-, und Hilfsmitteln	☑
	P-2.4.1	Erstellung des Therapieplans und Verordnung von Arznei-, Heil- und Hilfsmitteln	
Therapie	P-3.1	Anwendung von Operationsverfahren (inkl. Sterilgutversorgung)	☑
	P-3.1.1	Patient zum Eingriff aufklären	
	P-3.2.1	Patient zum Anästhesierisiko aufklären	
	P-3.1.3	OP-Planung erstellen	
	P-3.1.4	Patient vorbereiten	
	P-3.1.5	Patiententransport zum OP	
	P-3.1.6	Anästhesie einleiten	
	P-3.1.7	OP / Eingriff durchführen (Arzt)	
	P-3.1.8	OP / Eingriff durchführen (Pflegepersonal)	
	P-3.1.9	OP / Eingriff durchführen (Anästhesist)	
	P-3.1.10	Anästhesie ausleiten (Aufwachraum)	

	P-3.1.11	Patiententransport zur Station	
	P-3.1.12	OP-Dokumentation erstellen	
	P-3.1.13	OP-Bericht erstellen	
	P-3.2	Anwendungen medikamentöser, physikalischer, manueller Heilmethoden	☑
	P-3.2.1	Verordnung erstellen	
	P-3.2.2	Medikamentöse Heilmethoden ausführen	
	P-3.2.3	Physikalische und manuelle Anwendung durchführen	
	P-3.3.4	Dokumentation erstellen	
	P-3.3	Anwendung gerätebasierter Heilmethoden, Einsatz von lebenserhaltenden Technologien, Intensivstation	☑
	P-3.3.1	Intensiv Monitoring durchführen	
	P-3.3.2	Mobile Radiologie durchführen (Intensiv und OP)	
	P-3.3.3	Beatmung durchführen	
	P-3.3.4	Arzneimitteltherapie durchführen (Intensivstation)	
	P-3.3.5	Strahlentherapie durchführen	
	P-3.3.6	Dialyse durchführen	
	P-3.4	Bereitstellung von Arznei- und Hilfsmitteln	☑
	P-3.4.1	Arznei- und Hilfsmittel bereitstellen	
Krankenpflege	P-4.1	Visite	☑
	P-4.1.1	Visite durchführen	
	P-4.2	Durchführung von pflegerischen Maßnahmen	☑
	P-4.2.1	Pflegeplanung erstellen	
	P-4.2.2	Körperpflege und Prophylaxen durchführen	
	P-4.2.3	Medikamente stellen und darreichen	
	P-4.3.4	Einnahmekontrolle der Medikamente durchführen	
	P-4.3.5	Vitalparameter ermitteln und dokumentieren	
	P-4.3.6	Mobilisierung und Lagerung durchführen	
	P-4.3.7	Wundmanagement durchführen (und z.B. Dekubitus-Dokumentationen)	
	P-4.3.8	Patientenüberwachung (Monitoring)	
	P-4.3.9	Point-Of-Care-Testing	
	P-4.3	Sicherstellung der Versorgung/Hygiene/Verpflegung	☑
	P-4.3.1	Speisenbestellung durchführen	
	P-4.3.2	Speisenherstellung durchführen	
	P-4.3.3	Speisenverteilung durchführen	
	P-4.3.4	Hygiene planen und einhalten	
	P-4.3.5	Hygiene durchführen	
	P-4.3.6	Hygiene dokumentieren	
Entlassung	P-5.1	Erstellung des Arztbriefes mit Medikationsliste, ggf. anschließende Therapieplanung	☑
	P-5.1.1	Arztbrief diktieren / schreiben	
	P-5.1.2	Arztbrief kontrollieren und freigeben	
	P-5.1.3	Arztbrief versenden	
	P-5.2	Entlassung des Patienten und Erläuterungen / Sicherstellung der Medikamentenversorgung ggf. Sicherstellung der poststationären Versorgung, Kurzzeitpflege, etc.	☑