Ausfüllhilfe „BAK-Prüfnachweisplaner-Tool §8a BSIG V1.1/12-2018“

Stand: Dezember 2018.

Motivation

Da das ITSIG und die zugehörige Verordnung nur abstrakt festlegt, wer als KRITIS-Betreiber in der Branche „medizinische Versorgung“ gilt und was als kritische Dienstleistung zu sehen ist, bleiben die Details zur Umsetzung der Anforderungen aus dem BISG im Wesentlichen offen. Aus diesem Grund hat der BAK „medizinische Versorgung“ eine Hilfestellung für die betreffenden KRITIS-Betreiber der Branche erstellt, der folgende Zielaspekte in Bezug auf eine Prüfung nach §8a BSIG adressiert:

1.) Ökonomische Planbarkeit für Betreiber und prüfende Stellen
2.) Standardisierung der §8a Prüfplanerstellung durch Grobdefinition des Prüfkontextes (Scope) und der Prüfschwerpunkte:
    a. Allgemeine Dokumenten- und Regelungsprüfung
    b. Basis-IT-Absicherung
    c. Absicherung der kDL
    d. Branchenspezifischer Risikobewertungskontext
3.) Grobstandardisierung der Prüfnachweisdokumentation und des Prüfungsverlaufs im Zeitverlauf über mehrere Prüfperioden

Das „BAK-Prüfnachweisplaner-Tool §8a BSIG“ soll zudem eine Reihe von Detailanforderungen an ein sinnvolles §8a Prüfungskonzept für die Branche „medizinische Versorgung“ abdecken. Das unterlegte Prüfungskonzept soll somit:

- in Bezug auf den Prüfnachweis angemessen sein und den Prüfungsumfang und die Prüfungsschwerpunkte so setzen, dass eine sinnvolle Stichprobe in Bezug auf die IT-Absicherung der stationären Versorgung ermöglicht wird,
- die Komplexität, den Auftrag und die Größe der einzelnen KRITIS-Betreiber berücksichtigen und eine situationsgerechte Prüfbelastung sicherstellen,
- einen vergleichbaren Prüfungsleistungsumfang definieren und möglichst zur budgetären Planungssicherheit bei Betreibern und prüfender Stelle beitragen,
- über mehrere Prüfperioden nachvollziehbar und vergleichbar sein,
- Aspekte des Ausschreibungsrechts sinnvoll berücksichtigen,
- B3S fokussiert sein und dennoch flexibel in Bezug auf die gewählte ISMS Strategie der KRITIS-Betreiber,
- nach Dokumentenprüfung, technischer Rahmenumgebung, kDL Hauptsystemen, wichtigen kDL Spezialsystemen differenzierend sein,
- sich an der Realsituation und nicht an Idealsituation in der Branche orientieren, aber den kontinuierlichen Entwicklungsprozess hin zu einer Idealsituation fördern,
- in der Ausprägung möglichst definiert, gefasst und qualitätsüberprüfbar aber nicht einengend in der Prüfschwerpunktauswahl für die prüfenden Stellen sein,
- in der Prüfverfahrensausrichtung konstruktiv und nicht destruktiv-regulativ sein. Es muss einen Konfliktlösungsmechanismus fokussieren, welcher den unterschiedlichen Rollen von KRITIS-Betreiber und prüfender Stelle/Prüfteam gerecht wird,
- die prüfende Stellen und die KRITIS-Betreiber der Branche bei der Erstellung der geforderten Prüfungsnachweise unterstützen.

Darüber hinaus soll das Prüfungskonzept motivierend auf Vorleistung der Betreiber in Bezug auf eine Zertifizierung nach ISO27001 bzw. Grundschutz o.ä. sein.

Struktur und grundsätzliches Konzept

Das „BAK-Prüfnachweisplaner-Tool §8a BSIG“ wurde als Microsoft Excel-Datei erstellt. Im Wesentlichen setzt es sich aus fünf Haupt-Tabellenblättern und mehreren Basisdaten-Tabellenblättern zusammen.

Die Haupt-Tabellenblätter „Workflow“, „Rahmenvorgaben“, „Prüfnachweisplaner“, „Risikoanalyse“ und „Prüfungsfeststellung“, bilden den aktiven Bearbeitungs- bzw. Workflowkontext des Tools. Alle anderen Tabellenblätter, bieten lediglich die Möglichkeit, die dem Prüfnachweisplanertool unterlegten Prüfungsreferenzkataloge und Stammdaten einzusehen. Eine Übersicht über diese Referenzprüfungskataloge ist in Tabellenseite „Prüfreferenzkataloge“ gegeben.

Grundsätzlich ermöglicht das Prüfnachweisplanertool die Ermittlung eines nach Fallzahl, Fachabteilung und Forschungs- und Lehre-Anteil differenzierten Prüftagekontingentes. Dieses Prüftagekontingent wurde durch eine Expertenbefragung festgelegt. Es umfasst den maximalen Aufwandsrahmen der §8a Prüfung in Prüfungstagen. Der Kostenrahmen für die Prüfung ergibt sich dann aus den jeweilig angebotenen Prüftagessätzen der prüfenden Stellen für eine §8a Prüfung mit entsprechend qualifiziertem Prüfteam. Das Prüftagekontingent stellt eine Prüftageaufwandsobergrenze dar. Der prüfenden Stelle bleibt es vorbehalten nach Vertragsabschluss das Prüftagekontingent auf Basis von vorliegenden Zertifikatsnachweisen oder Redundanzprüfungsaspekten (zentrales Rechenzentrum) zu reduzieren, soweit dies begründet werden kann. Hierzu muss der KRITIS-Betreiber der prüfenden Stelle nach Vertragsabschluss entsprechende Pflicht- und Ergänzungsdokumente (siehe hierzu auch den B3S) zur Verfügung stellen.

Wichtig ist das Verständnis des unterlegten Prüfungskonzeptes bei der Auswahl des Prüfreferenzrahmens der Prüfung. Da die Brache „medizinische Versorgung“ im Kontext der Erbringung der kritischen Dienstleistung (kDL) sehr heterogene IT-Strukturen aufweist und es daher keine allgemeingültigen „Standard“ bei der Absicherung des kDL-Betriebes gibt, kann als Prüfungsgrundlage kein starrer Prüfrahmen im Sinne einer Checkliste vorgegeben werden. Der vom Betreiber ausgewählte Prüfungsrahmen ist somit immer als Referenzprüfungsrahmen zu verstehen, dessen Controls im spezifischen Betreiberkontext vom Prüfteam subjektiv zu bewerten sind.

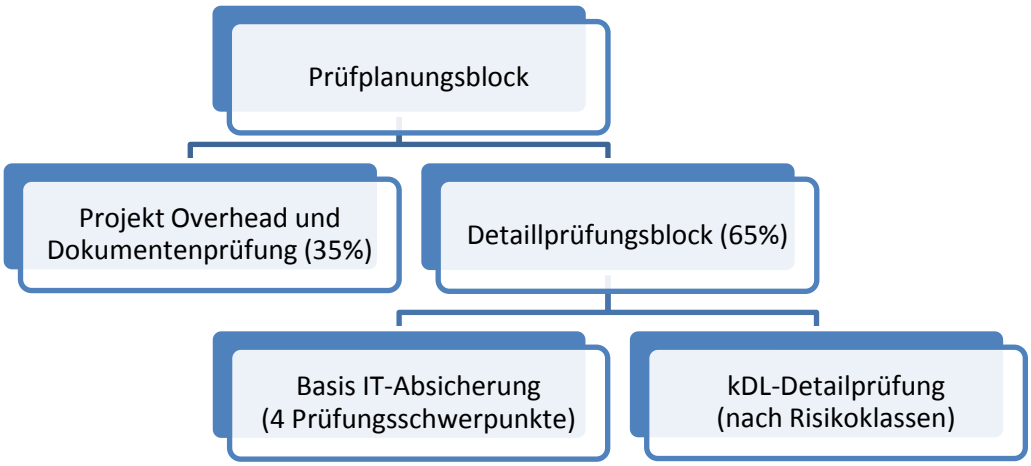
Der **Prüfplanungsblock** selbst teilt sich in die Aspekte „**Projekt-Overhead und Dokumentenprüfung**“, der ca. 35 % des – nach ggf. erfolgter Korrektur des Prüftagekontingentes durch die prüfende Stelle - ermittelten Prüftagekontingents umfasst, sowie den **Detailprüfungsblock**, der ca. 65 % des entsprechenden Prüftagekontingentes umfasst.

Der **Detailprüfungsblock** (Vorortprüfung bzw. Realitätscheck) ist als Prüfplanstruktur so aufgebaut, dass in der Vorortprüfung zwei weitere Prüfschwerpunkte gesetzt werden. Der erste Prüfungsschwerpunkt bezieht sich auf die Basis-IT-Absicherung, der zweite Prüfungsschwerpunkt fokussiert die kDL-relevanten IT-Systeme (kDL-Detailprüfung).

Bezüglich der **Basis-IT-Prüfung** sind vom Prüfteam wiederum vier Prüfschwerpunkte zu setzen, die aus den Grundkapiteln des BSI-Grundschutzkompendiums als Prüfungsrefrenzkontext ausgewählt werden können. In der **kDL-Detailprüfung** ergibt sich bezogen auf kDL-relevante IT-Systeme, differenziert nach der Risikobewertung der IT-Systeme in Bezug auf die kDL-Relevanz (Risikoanalyse) eine weitere Dreiteilung. Von 4 kDL-relevanten Hauptsystemen mit hoher kDL-Risiko-Einstufung (Risikoklasse 1), sind mindestens 3 Controls aus dem vom Betreiber gewählten Prüfreferenzrahmen durch

das Prüfteam mit einem Prüftageaufwand von 5% des Detailprüfungskontingentes zu prüfen. Im zweiten Block sind, soweit das Prüfteam es so festlegt, weitere 4 Systeme aus der Risikoanalyse mit jeweils zwei auszuwählenden Controls aus dem Prüfungsreferenzrahmen zu prüfen, bei denen der Prüfungszeitanteil in Prozent durch das Prüfteam selber festgelegt wird. Der dritte Block legt weitere zwei Systeme aus dem Risikoanalyseportfolio mit einem auszuwählenden Control aus dem Prüfungsreferenzrahmen fest. Zudem kann das Prüfteam hier zwei Prüfschwerpunkte mit einem entsprechenden Prüftagekontingentanteil eigener Wahl (also z. B. Dokumentenprüfung ISO-Zertifizierung) in Prozent festlegen. Es bietet sich an, dass das Prüfteam die drei Blöcke der kDL-Detailprüfung gemäß Risikoklassifizierung strukturiert. Dies ist jedoch lediglich eine Empfehlung, da das Prüfteam in der Prüfschwerpunktbildung im gesetzten Rahmen frei ist.

Die Aufteilung des Prüfplanungsblocks ist im folgenden Schaubild dargestellt:



Um den Abstimmungsaufwand bei der Festlegung des frei vergebbaren Prüftagekontingentes im Detailprüfungsblock nicht ausufern zu lassen, darf das Prüfteam in seiner Prüfplanfestlegung max. 5% von dem im Detailprüfungsblock vorgesehenen Prüftagekontingentanteil nach unten abweichen. Eine Ausweitung des Prüftagekontingentes über den gesetzten Rahmen ist jedoch nicht zugelassen. Das Prüfnachweisplanertool unterstützt diesen zeitbezogenen Planungsprozess mit einem Korrekturhinweisfeld in der letzten Prüfnachweisplanerzeile.

Sicherheitshinweis

Das Prüfnachweisplanertool arbeitet in Excel konsequent mit Excel-Funktionen und HTML-Links und nicht mit Makros oder VisualBasic-Code. Hierdurch wird sichergestellt, dass eine Weitergabe und Nutzung des Tools auch vor dem Hintergrund der in der Branche getroffenen Sicherheitsmaßnahmen in Bezug auf die Nutzung Office-Dokumenten möglich ist. Lediglich ein verstecktes Hilfstabellenblatt ist im Prüfnachweisplanertool nicht unmittelbar einsehbar. Dieses dient dazu, die im Tabellenblatt „Risikoanalyse“ vom Betreiber eingetragenen Änderungen für die Auswahlboxen im Tabellenblatt „Prüfnachweisplaner“ aufzubereiten. Hierzu sind nach einer Änderung im Tabellenblatt „Risikoanalyse“ das Speichern und der Neuaufruf des Prüfnachweisplanertools notwendig.

Da das Prüfnachweisplanertool für sensible Betreiberkontexte erstellt wurde, ist unbedingt darauf zu achten, dass keine Marko-Warnungen oder ähnliches beim Aufruf erscheinen. Sollte dies der Fall sein, ist das Prüfnachweisplanertool aller Voraussicht nach manipuliert worden!

Das Prüfnachweisplanertool ist ansonsten in Bezug auf die Veränderungen von Tabellenblattstrukturen und den Aufbau der Excel-Arbeitsmappe gegen Manipulation passwortgeschützt. Jeder Nutzer des Prüfnachweisplanertools ist dennoch dazu angehalten, das Tool nur aus „sicheren Quellen“ entgegenzunehmen bzw. abzurufen, da der Passwortschutz unter Excel nur bedingt als verlässliche Manipulationshürde gelten kann.

Tabellenblatt: „Workflow“

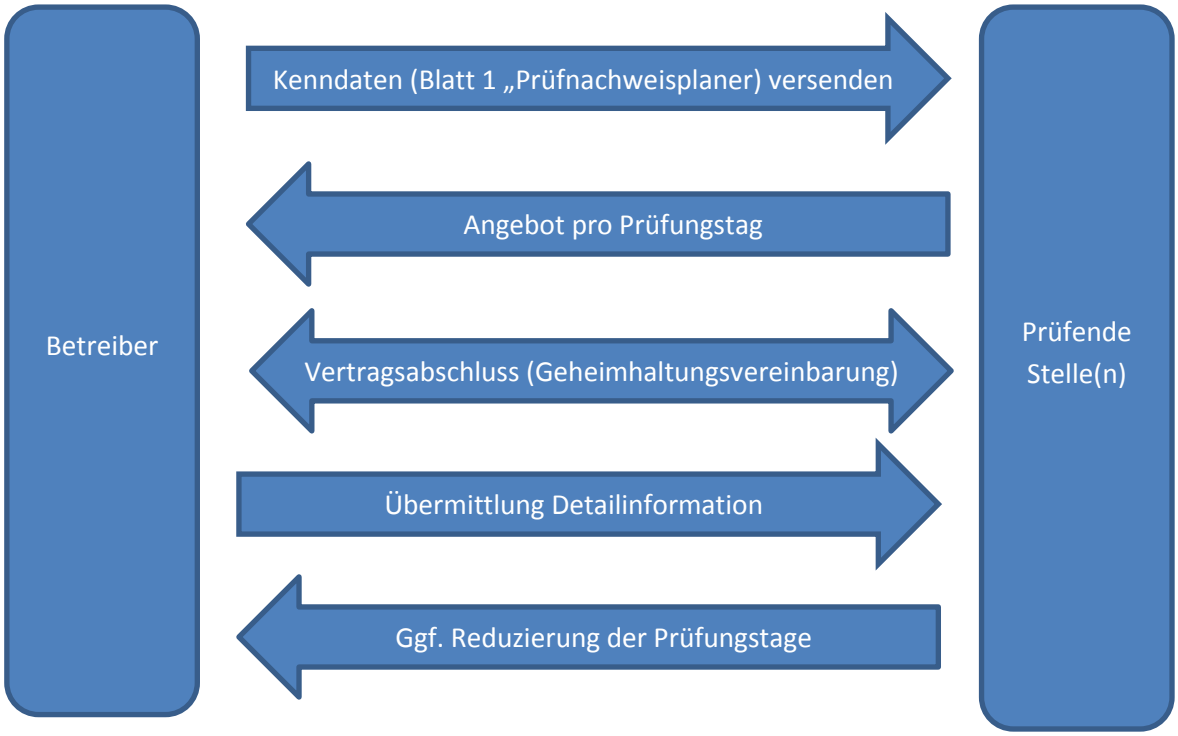
Aufgabe: Das Tabellenblatt „Workflow“ hat die Aufgabe, dem KRITIS-Betreiber, der prüfenden Stelle und dem Prüfteam einen Überblick über den gedachten Verfahrensablauf und den Umgang mit dem Prüfnachweisplanertool zu geben. Im Wesentlichen ist es eine Aufruf- und Orientierungshilfe, mit der – je nach Prozessschritt – per HTML-Link an die entsprechende prozessrelevante Stelle im Prüfnachweisplanertool verzweigt werden kann.

Detailinformation:

BAK-Prüfnachweisplaner-Tool §8a BSIG	
KRITIS-Branche "medizinische Versorgung"	
BAK Handlungsempfehlung	
TLP-Green — Vers. 1.1/12-2018 — © BAK "medizinische Versorgung"	
Workflow-Steuerungspanel	
Betreiber	
Rahmenvorgaben für die Prüfplanerstellung §8a mit Hilfe des Prüfplaners lesen.	Rahmenvorgaben
Prüftagekontingent anhand von Fallzahl/Fachabteilungszahl/Forschungs & Lehre-Auftrag ermitteln und in die Prüfnachweisplaner Tabelle eintragen. Prüfungsgrundlage als Prüfungs-Referenzrahmen auswählen. Die nach Angebotsannahme an die "Prüfende Stelle" zu übermittelnden, grundsätzlich vorzulegenden Prüfungsdokumente, Vorprüfungsplanungen und Zertifizierungsnachweisdokumente u.ä. benennen und eintragen.	Betreibereingaben
Detailinformationen zu den wählbaren Prüfreferenzkatalogen.	Info-Prüfreferenzkataloge
Fertig ausgefülltes "Blatt 1: Betreibereingaben" des Prüfnachweisplaners in Papier oder PDF-From ausdrucken, zeichnen/signieren und an mögliche, zur Prüfung befähigte Anbieter (Prüfenden Stellen) im Angebotseinholungsverfahren übermitteln. Hierbei für das ermittelte Prüftagekontingent den Tagessatzpreis pro Prüfungstag mit dem Verweis auf eine spätere, nach Dokumentenprüfung mögliche Prüfungstagereduktion durch die "Prüfenden Stellen" einholen, um Vergleichbarkeit zu gewährleisten. Geheimhaltungsregelung und Verweis auf Teil 06 des B3S als Vertragsgrundlage nicht vergessen und Qualifikationsnachweise von "Prüfender Stelle" und Prüfteam einfordern.	Blatt 1 "Betreiberangaben" drucken
In "Blatt 1" benannte, grundsätzlich geforderte Prüfungsdokumente wegen Sicherheitsrelevanz bei der Angebotseinholung noch nicht übermitteln!	
Rücklauf/Angebotsabgabe abwarten!	
Riskomatrix gemäß betreiberspezifischer Risikomatrix ausfüllen und "Prüfnachweisplaner"-Excel-Sheet sowie die notwendigen und zusätzlichen Prüfungsdokumente für die die Abgabe an die "Prüfende Stelle" vorbereiten.	Risikomatrix ausfüllen
Nach dem Angebotszuschlag vorbereiteten Prüfnachweisplaner & Dokumente an "Prüfende Stelle" übermitteln. Auf Geheimhaltungsvereinbarung achten!	
Prüfende Stelle	
Rahmenvorgaben für die Prüfplanerstellung §8a mit Hilfe des Prüfplaners lesen.	Rahmenvorgaben
Sichten der vom Betreiber mitgelieferten verpflichtend und zusätzlich zur Verfügung gestellten Dokumente. Anschließend erstellen des Prüfplans nach gewählter Prüfungsreferenz, Rahmenvorgaben und B3S Teil06, sowie festlegen des ggf. möglichen Aufwandsabschlages auf Basis von Dritt-Zertifikatsnachweisen, Redundanzprüfpotential u.ä..	Eingaben "Prüfende Stelle"
Das fertige "Blatt2 ff." in Papier oder PDF-From ausdrucken, zeichnen/signieren, und gemeinsam mit den Prüfteamdaten, Terminvorschlägen/Zeitplan, Rückfragen und Dokumentenanforderungen an den Betreiber übermitteln.	Blatt 2 ff. "Prüferangaben" drucken
Durchführung der Prüfung, Erstellen und übermitteln der §8a Prüfungsfeststellung sowie der nötigen Unterlagen für die Meldung an das BSI.	Eingabe "Prüffeststellung"
Prüffeststellung in Papier oder PDF-From ausdrucken, zeichnen/signieren. Ein überführen des Formates, z.B. in MS Word u.ä. zur erweiterten Bearbeitung ist zulässig.	Prüffeststellung drucken
Abschlußbesprechung und Übergabe der erstellten §8a Dokumente an den Betreiber.	

Das Tabellenblatt weist drei Bereiche auf. Der erste Bereich entspricht dem Betreiber-Workflow. Nach dem lesen der Rahmenvorgaben, gibt der Betreiber seine Kenndaten im Tabellenblatt „Prüfnachweisplaner“ ein, druckt diese aus und schickt den Ausdruck in elektronischer (PDF) oder Papierform an die prüfende Stelle. Basierend auf dem ermittelten Prüftagekontingent dient dieser Ausdruck dazu, ein Angebot über den Preis pro Prüfungstag von der prüfenden Stelle einzuholen. Der Prüftagepreisbezug ist notwendig, da vor der Offenlegung von z. T. sensiblen Details zur IT-Absicherung des KRITIS-Betreibers, erst ein bindender Vertrag mit Geheimhaltungsvereinbarung abgeschlossen werden muss. Erst nach Abschluss eines bindenden Vertrages, sollten der prüfenden Stelle z. T. sensible Prüfungsunterlagen übermittelt werden. Erst auf Basis der übermittelten Unterlagen kann die prüfende Stelle dann ggf. das Prüftagekontingent auf Basis von Betreibervorleistungen/ Zertifizierungen nach billigem Ermessen reduzieren, sodass die Ausweisung des Prüftagespreis und nicht des Gesamtpreises in der Angebotserstellung und im Angebotsvergleich ausschlaggebend ist.

Die Schritte von der Angebotseinholung bis zum Vertragsabschluss sind in folgendem Schaubild dargestellt:



Der zweite Bereich im Workflow-Tabellenblatt bezieht sich auf die vom Betreiber zu erstellende Risikoanalyse. Hier verzweigt der Workflow in das entsprechende Risikoanalyse-Tabellenblatt, welches dazu dient, das Ergebnis der Risikoanalyse des Betreibers einzutragen. Basierend auf diesen Eintragungen ergibt sich anschließenden Prüfplanungsprozess durch das Prüfteam das Prüfungsgrundgerüst im Tabellenblatt „Prüfnachweisplaner“. Erst nach dem Vertragsabschluss mit der prüfenden Stelle und dem Ausfüllen des Risikoanalyse-Tabellenblattes, sollte die Excel-Arbeitsmappe mit dem Prüfteam zusammen mit den geforderten, prüfungsrelevanten Unterlagen ausgetauscht werden.

Da es sich in jedem Fall um sicherheitskritische Informationen handelt, muss der Austausch von Dokumenten und Informationen zwischen Betreiber und prüfender Stelle/Prüfteam durch Verschlüsselung der Kommunikationswege abgesichert werden.

Der dritte Bereich des Workflow-Blattes skizziert den Workflow des Prüfteams der prüfenden Stelle. Nach Erhalt des vom Betreiber vorausgefüllten Prüfnachweisplanertools und lesen der Rahmenvorgaben, verzweigt der Workflow in den Bereich des Tabellenblattes „Prüfnachweisplaner“ der vom Prüfteam auszufüllen bzw. einzutragen ist. Dies definiert den Prüfplan, der im Kontext des vorgegebenen Prüfreferenzrahmens und der im Tabellenblatt „Risikoanalyse“ ausgewiesenen IT-Systeme vom Prüfteam festgelegt wird. Dieser Teil kann später ebenfalls in elektronischer (PDF) oder Papierform ausgedruckt und nachfolgenden Prüfteams zur Orientierung über die Schwerpunkte der §8a Vorprüfungen vorgelegt werden. Gemäß BSIG hat der Betreiber keine Verpflichtung, die Gesamtprüfungsfeststellung einer Vorprüfung an die nachfolgende prüfende Stelle zu übermitteln. Sinnvoll ist es jedoch, wenn bis zu vier vorhergehende Prüfpläne sowie die an das BSI übermittelten Mängelnachweise an die jeweiligen Prüfteams übermittelt werden.

Während der Prüfungsdurchführung soll im Workflow das Tabellenblatt „Prüffeststellung“, welches nach der Festlegung des Prüfplans vorausgefüllt ist, zur strukturierten Prüffeststellungsdokumentation genutzt werden. Da Excel in der Textverarbeitung Schwächen hat, kann das vorausgefüllte Tabellenblatt auch in ein Worddokument kopiert und dort ausgefüllt werden. Aus der Prüffeststellungsdokumentation für den Betreiber leitet sich dann die an das BSI zu übermittelnde „Mängelnachweis“ durch die prüfende Stelle ab. Das Prüfnachweisplanertool hat hier die Aufgabe, die Kommunikation zwischen Betreiber und Prüfteam zu strukturieren und das Prüfteam bei der Erstellung eines strukturierten Prüffeststellungsnachweises zu unterstützen. Es hat jedoch nicht die Aufgabe, die vom BSI vorgegebenen Anlagen zum Prüfnachweis automatisiert zu erzeugen.

Tabellenblatt: Prüfnachweisplaner

Aufgabe: Das Tabellenblatt „Prüfnachweisplaner“ hat mehrere Segmente, welche den Workflow in der Angebotseinholung und der Prüfplanung unterstützen sollen. In blauen Farbtönen ist hierbei der Betreiber-Teil gehalten, während der Teil für prüfende Stelle bzw. Prüfteam in grünen Farbtönen gehalten ist. Eine Eingabe von Daten ist nur in grau, eine Auswahl aus Katalogen nur in orange hinterlegten Zellen erforderlich und möglich.

Detailinformation: „Betreiberteil: Ermittlung des Prüftagekontingentes“

	A	B	C	D	E	F	G	H	I	J
1	Zurück									
2	Prüfumfang und Prüfplanungs-Sheet: "medizinische Versorgung" (Blatt 1)									
3	Festlegung des Prüfkontingentes									
4	TEIL A: vom Betreiber auszufüllen!									
5	Name und Anschrift des KRITIS-Betreibers:	Prüfkrankenhausadresse						Prüfjahr:	2019	
6	Tabelle zur Ermittlung des Prüftagekontingentes nach Betreiberkomplexität:		Voll-Stationäre Fälle							
7		Anzahl Fachabteilung	30000-40000	40001-50000	50001-60000	60001-70000	>70000			
8	Fachabteilungen nach §301-Datenübermittlung	<=20	10	10	11	11	12			
9		<=30	11	11	12	12	13			
10		<=40	12	12	13	13	14			
11		<=50	13	13	14	14	15			
12		<=60	14	14	15	15	16			
13		>60	15	15	16	16	25			
14	Forschung und Lehre-Faktor	Hebefaktor Normalkrankenhaus	1,0	1,0	1,1	1,2	1,3			
15	Universitätsklinikumsfaktor	Hebefaktor Universitätsklinika	1,2	1,2	1,3	1,4	1,6			
16										
17		Bitte den passenden Wert für das Prüftagekontingent für Ihr Klinikum aus obiger Tabelle auswählen:	14	Hebefaktor Forschungs und Lehre:	1,1	hell graue Felder zur Texteingabe! Orange Auswahlfelder! Löschen im Eingabeteil: "rechte Maustaste" & "Inhalte löschen" im Eingabefeld				
18				Begründung durch "Prüfende Stelle":						
19	Übertrag "Prüfende Stelle"	Reduktion in Prüftagen durch Vorzertifizierung & Redundanzprüfungspotential	0,0							
20	Prüfkontingent in Prüftagen (PRT)		15,4							
21	*) PRT=Prüftage als Gesamtumfange der Prüfung, unabhängig von der Zusammensetzung des Prüfteams									

Der erste logische Block des Prüfnachweisplaners weist den Betreiber und das Prüfungsjahr aus und definiert anhand der Parameter „Vollstationäre Fälle“ und „Anzahl der Fachabteilungen“ das Basisprüftagekontingent für den KRITIS-Betreiber in Tabellenform. Im obigen Bildschirmfoto ergibt sich für einen fiktiven Betreiber bei 43000 stationären Fällen und einer Fachabteilungszahl von 45 Fachabteilungen, z.B. ein Basisprüfungstagekontingent von „14“ Tagen. Um der zusätzlichen Komplexität des IT-Betriebes eines KRITIS-Betreibers mit Forschungs- und Lehreaktivitäten bzw. Universitätsklinika gerecht zu werden, muss dieses Basisprüfungstagekontingent mit einem Hebefaktor bei Forschung- und Lehre- bzw. Universitätsbetrieb bewertet werden. Das Basisprüfungstagekontingent und der Hebefaktor sind hierbei in die hierfür vorgesehenen Felder in „Zeile 17“ so einzutragen, wie sie in der Tabelle vorgegeben sind. Im Beispielfall also mit „14“ für das Basisprüftagekontingent und einem Hebefaktor von „1,1“für ein Lehrkrankenhaus. Hieraus ergibt sich ein Prüftagekontingent von „15,4“ Prüftagen für den fiktiven Betreiber.

Achtung: Es handelt sich um ein Prüftagekontingent und nicht um ein Personentagekontingent! Das Prüftagekontingent muss von der prüfenden Stelle in einer Mischkalkulation auf die für die Prüfung nach §8a nötigen Personentage und somit eine Durchschnittstagessatz über alle geforderten Prüfungsqualifikationen zur §8a Prüfung umgerechnet werden.

Soweit die prüfende Stellen Vorleistungen des Betreibers oder Redundanzprüfungsanteile bei der Prüfung mehrerer KRITIS-Krankenhäuser eines KRITIS-Betreibers anerkennt (siehe **Detailinformation: „Grundüberprüfung des Informationsverbundes/ISMS“**) und im Eingabeteil für das Prüfteam ausweist, wird die Prüftagereduktion im Prüfnachweisplanertool später im Betreiberteil in „Zeile 19“ ausgewiesen.

Detailinformation: „Betreiberteil: Auswahl des Prüfreferenzkataloges“

23	Auswahl des Prüfreferenzkataloges	
24	**Prüfkatalog Allgemeine Prüfung**	*Dieser Prüfkatalog definiert die Prüf-Controls im Blatt 2 der prüfenden Stellen. **ACHTUNG:** Löschen der Auswahl führt nicht dazu, dass das der Prüfplaner zurückgesetzt wird. Eintragungen im Prüfplanungsteil bleiben erhalten und müssen ggf. manuell ("rechte Maustaste"&"Inhalte löschen") berichtigt werden.*
25	**B3S_ISMS**	**ggf. Zusätzliche Kommentare oder Anmerkungen zum gewählten Prüfkatalog**

Im Block „**Auswahl des Prüfreferenzkataloges**“ wählt der Betreiber den Prüfungsreferenzkatalog aus nach dem die §8a Prüfung erfolgen soll. Er kann hier in einem orange hinterlegten Auswahlfeld in „Zeile 25“ zwischen „B3S_ISMS“, „ISO27001_ISO27002“, „ISO27001_ISO27799“, „BSI_Grundschutz“ und „IDW_PS_330“ auswählen. Diese Auswahl legt die Prüfungs-Controls für den Detailprüfungsteil des Prüfnachweisplanertools fest. Die Vielfalt der auszuwählenden Prüfreferenzkataloge ist hierbei der Vielfalt der in der „medizinischen Versorgung“ anzutreffenden ISMS- und Zertifizierungsansätze geschuldet. Das Prüfnachweisplanertool geht an dieser Stelle über die Umsetzung des B3S-ISMS und des B3S-Maßnahmenkataloges hinaus, um erweiterte Zertifizierungsbemühungen eines KRITIS-Betreibers zu unterstützten.

Detailinformation: „Betreiberteil: Anlagen gemäß B3S“

27	**Anlagen gemäß B3S:**	
28	**Übersicht Informationsverbund**	Informationsverbund Gesundheitshaus Berlin.pdf, Stand: 1.2.2019
29	**Risikobewertung kDL-Systeme**	Risikobewertung kDL-Systeme Gesundheitshaus Berlin.pdf, Stand 1.2.2019
30	**IT-Sicherheitskonzept**	IT-Sicherheitskonzept Gesundheitshaus Berlin, Stand 6.8.2018
31	**ISMS Dokumentenplan**	ISMS-Dokumentenplan Gesundheitshaus Berlin, Stand: 1.2.2019
32	**Ergänzende Unterlagen:**	Vorangegangene Prüfpläne, Zertifzierunsbelege u.ä.
33	ISO 27001 Zertifikzierung	ISO 27001 Zertifzierung des zentralen Rechenzentrums vom 12.11.2018, TÜV Rheinland.
34	ISO 27001 Zertifikzierung	Statement of Applicability ISO 27001 Zertifzierung
35	Prüfplan §8a BSIG 2017	2017 Prüfplandokument & BSI Mängelfestellungsbogen
36	Prüfplan §8a BSIG 2015	2015 Prüfplandokument & BSI Mängelfestellungsbogen
37		
38		

Der Block „**Anlagen gemäß B3S**“ soll sicherstellen, dass der Betreiber die für eine Prüfung sinnvollen Pflichtdokumente in seiner Prüfungsvorbereitung und in der Kommunikation mit der prüfenden Stelle und dem Prüfteam nicht vergisst. Zudem ist dieser Teil – der schon in der Angebotsphase auszufüllen ist – wichtig, um der prüfenden Stelle zu signalisieren, welche zusätzlichen, prüfungsrelevanten Aspekte durch die prüfenden Stelle/das Prüfteam nach Angebotszuschlag noch zu berücksichtigen sind. Hierunter fallen insbesondere einschlägige Teilzertifizierungen und Redundanzprüfungsanteile.

Achtung: Auch wenn die Dokumente hier schon in der Angebotsphase benannt und den angefragten prüfenden Stellen in der Übersicht bekannt gegeben werden, dürfen diese Dokumente erst nach bindendem Vertragsabschluss mit Geheimhaltungsvereinbarung an die prüfenden Stelle, die den Zuschlag erhalten hat, übermittelt werden.

Detailinformation: „Grundüberprüfung des Informationsverbundes/ISMS“

	A	B	C	D	E	F	G	H	I	J
43			Zurück							
44	Prüfplanfestlegung "Prüfende Stelle" (Blatt 2)									
45	TEIL B1.1: von der Prüfenden Stelle auszufüllen/Sheet "Rahmenvorgaben" beachten									
46	Grundüberprüfung des Informationsverbundes/ISMS, ca. 35% des Gesamtprüfvolumens.									
47	Name und Anschrift der "Prüfenden Stelle":	Name und Adresse der prüfenden Stelle								
48	Übertrag: Prüfreferenzkatalog Allgemeine Prüfung	B3S_ISMS		hell graue Felder zur Texteingabe! Orange Auswahlfelder! Löschen im Eingabeteil: "rechte Maustaste" & "Inhalte löschen" im Eingabefeld						
49		Reduktion in Prüftagen durch Vorzertifizierung & Redundanzprüfungspotential	3,0	Aufgrund der voliegenden Unterlagen zur ISO27001 Zertifizierung des zentralen IT-Rechenzentrumsbetriebes, kann der Prüftageumfang um 3 Tage reduziert werden. Es ergibt sich ein Gesamtprüftageaufwand von 12.4 Prüftagen.						
50	Prüfkategorie		Aufwand in PRT	Kommentar:						
51	Prüfungsvorbereitung: Sichtung und Analyse der IT-Sicherheitsleitlinie, IT-Sicherheitskonzept, kDL-Scopes, ISMS Dokumentenübersicht, Prüfungs-Scopes der vorangegangenen Dokumenten	5% des Gesamtvolumens nach Orientierungshilfe	1,00	Prüfung der Pflichtdokumente: Informationsverbund, Risikoanalyse, IT-Sicherheitskonzept, ISMS-Dokumentenplan						
52	Stichprobenartige Dokumentenprüfung nach	12,5 % des Gesamtvolumens, insgesamt 25% des Gesamtvolumens nach Orientierungshilfe	2,00	2.1 Organisation der Informationssicherheit						
53	mindestens 4 Prüfschwerpunkte!			3 Meldepflichten nach §8b (4) BSI-Gesetz						
54				4 Fortführungsmanagement für kDL						
55				9 Vorfallerkennung und Behandlung						
56				8 Personelle und organisatorische Sicherheit						
57				13.13 Beschaffungsprozesse						
58										
59										
60	Prüfplanfestlegung 10 % des Gesamtvolumens	(5% des Gesamtvolumens nach Orientierungshilfe)	1,00	Anmerkungen/Kommentare						
61	PMO/Audit-Report/Mängelliste erstellen	(10% des Gesamtvolumens nach Orientierungshilfe)	1,00	Anmerkungen/Kommentare						
62	Summe der festen PTR-Tage	40%	5,00	graue Felder zur Texteingabe! Orange Felder sind Auswahlfelder!						

Das Tabellensegment erlaubt es der prüfenden Stelle eine Reduktion des Prüftagekontingentes auf Basis von Betreibervorleistungen/ Zertifizierungen oder Redundanzprüfungsanteilen bei einem Betreiberverbund einzutragen und zu begründen, bzw. auf entsprechende Begründungsdokumente zu verweisen. In Abhängigkeit von dem sich nach einer ggf. gewährten Prüfragereduktion ergebenden Prüftagekontingent, definieren sich in diesem Tabellenteil die für den Prüfungsoverhead und die Schwerpunkte in der Dokumentenprüfung des ISMS vorgegebenen Prüfzeitenanteile. Die prüfende Stelle hat hier zudem die Prüfschwerpunkte in der ISMS-Dokumentenprüfung gemäß gewähltem Prüfungsreferenzkatalog festzulegen und dokumentieren. Die Auswahl erfolgt hierbei anhand der in Orange gekennzeichneten Vorauswahlfelder. Die jeweiligen Auswahlmöglichkeiten können im Überblick im jeweiligen Tabellenblatt für den Prüfreferenzkatalog des Prüfnachweisplaner-Tools eingesehen werden, um eine bessere Übersicht über die möglichen Prüfschwerpunkte zu ermöglichen.

Detailinformation: „Detailprüfung kDL-Systeme“

65	Detailprüfung kDL-Systeme ca. 65 % des Gesamtprüfvolumens (Blatt 3)		
66	Stichproben	*Vorgabe aus TEIL 06 BSI: Infrastruktur & 4 kDL-relevante IT_Systeme - 3 Prüfschwerpunkte aus gewähltem Prüfreferenzkatalog als Detailprüfungsmindestumfang!*	
67		*Erster Prüfabschnitt: Basis-IT-Prüfung 20%, z.B. in Form eines Infrastruktur/Dokumenten-Assessments*	
68		*Zweiter Prüfabschnitt: kDL-bezogene Systemprüfung nach B3S-Kritikalität (Krit.1.=40%, Rest frei)Begehung & technische Stichprobe, Realitätscheck der Interviews*	
69	Übertrag: Prüfreferenzkatalog Detailprüfung	B3S_SecurityCheck	*Details siehe Sheet-Tabs!*

Das Tabellensegment Detailprüfung dient lediglich der Information über den für die kDL-Detailprüfung gewählten Detailteil des Prüfreferenzkataloges. Der Eintrag des Informationsfeldes ergibt sich aus dem vom Betreiber gewählten Prüfreferenzkatalog. Dieser Eintrag erlaubt es die entsprechenden Auswahl-Controls aus dem Prüfreferenzkatalog zuzuordnen.

Detailinformation: Basis-Infrastruktur-Prüfung

71	Prüfplan Detailprüfung vor Ort/Realitätsabgleich						
72	TEIL B1.2: von der "Prüfenden Stelle" auszufüllen						
73	Basis-Infrastruktur-Prüfung	MUSS-Prüfumfang: insg. 4 Prüfschwerpunkte	Prüfschwerpunkt gemäßt Basis-IT-Prüfraster (s.u.). Das Grundschutzkompendium ist hierbei als Diskussionsbasis/Referenzprüfkatalog im Prüfablauf zu sehen und nicht als "Muss-Prüfungskatalog" zu verstehen, der zu erfüllen ist.		Prozentanteil an der Detailprüfung	PRT-Tage Realitäts-abgleich	Kommentar:
74		Prüfschwerpunkte	INF.2 Rechenzentrum sowie Serverraum		5%	0,6	
75		Prüfschwerpunkte	INF.7 Büroarbeitsplatz		5%	0,6	
76		Prüfschwerpunkte	INF.9 Mobiler Arbeitsplatz		5%	0,6	
77		Prüfschwerpunkte	INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume		5%	0,6	
78	Summe Basis-IT-Prüfung	mindest Umfang	20%	2,4			

Das Tabellensegment „**Basis-Infrastruktur-Prüfung**“ erlaubt es der prüfenden Stelle vier Prüfschwerpunkte gemäß dem BSI-Grundschutzkatalog auszuwählen. Es handelt sich hierbei jedoch nicht um eine Prüfung nach BSI-Grundschutz. Die Prüfschwerpunktsetzung soll im Prüfungsgespräch mit dem Betreiber einen Rahmen setzen, in dem der Betreiber dem Prüfteam seine spezifischen Lösungen im Kontext der gewählten Prüfungsschwerpunkte erklärt. Das BSI-Grundschutzkompendium kann hierbei als Gesprächsgrundlage genutzt werden. Für die jeweiligen Prüfschwerpunkte in Bezug auf die Basis-Infrastruktur-Prüfung werden jeweils 5% des veranschlagten Prüftagekontingentes vorgesehen.

Detailinformation: „kDL-Systeme: Kritikalitätsklasse 1“

79	kDL-Systeme: Kritikalitätsklasse 1	MUSS-Prüfumfang: insg. 4 Prüfschwerpunkte Systembezeichnung gemäß Risikoanalyse/B3S-Informationsverbundsanalyse		Prüfkatalog-Controls	Prozentanteil an der Detailprüfung	PRT-Tage Realitäts-abgleich	Kommentar:
80	mind. 3, Prüfschwerpunkte	1 - Apothekensystem		D Vermeidung von offenen Sicherheitslücken	5%	0,8	
81				F Logdatenerfassung und -auswertung			
82				H Bewältigung von Sicherheitsvorfällen			
83	mind. 3, Prüfschwerpunkte	1 - Krankenhausinformationssystem (KIS)		D Vermeidung von offenen Sicherheitslücken	5%	0,8	
84				J Gewährleistung der Verfügbarkeit nötiger Ressourcen			
85				B Abwehr von Schadprogrammen			
86	mind. 3, Prüfschwerpunkte	1 - Laborinformationssystem (LIS)		H Bewältigung von Sicherheitsvorfällen	5%	0,8	
87				C Inventarisierung der IT-Systeme			
88				A Absicherung von Netzübergängen			
89	mind. 3, Prüfschwerpunkte	1 - Dokumenten-Management-System / Enterprise-Content-Management		A Absicherung von Netzübergängen	5%	0,8	
90				D Vermeidung von offenen Sicherheitslücken			
91				I Sichere Authentisierung			
92		mindest Umfang	20%	3,2			

Das Tabellensegment kDL-Detailprüfung „**kDL-Systeme: Kritikalitätsklasse 1**“ bietet der prüfenden Stelle die Möglichkeit aus dem Portfolio der IT-Systeme, die vom Betreiber im Tabellenblatt „Risikoanalyse“ bewertet wurden, vier IT-Systeme für eine Stichprobenprüfung auszuwählen. Die drei geforderten Schwerpunkte der Prüfung in Form von Referenzprüfkatalog-Controls wählt er in der Spalte „Prüfkatalog-Controls“ aus. Der Prüfungszeitanteil am Prüftagekontingent pro ausgewähltem IT-System beträgt 5%.

Detailinformation: weitere kDL-Systeme

	kDL-Systeme: vorzugsweise Kritikalitätsklasse 2	KANN-Prüfumfang, innerhalb des Prüfkontingentes Systembezeichnung gemäß Risikoanalyse/B3S-Informationsverbundsanalyse		Prüfkatalog-Controls	Prozentanteil an der Detailprüfung	PRT-Tage Realitäts-abgleich	Kommentar:
93							
94	mind. 2, Prüfschwerpunkte	1 - Patientenmanagementsystem (PDMS/Intensivdatenverwaltung)		A Absicherung von Netzübergängen	4%	0,5	
95				B Abwehr von Schadprogrammen			
96	mind. 2, Prüfschwerpunkte	1 - elektronische Patientenakte		A Absicherung von Netzübergängen	4%	0,5	
97				E Sichere Interaktion mit dem Internet			
98	mind. 2, Prüfschwerpunkte	2 - Rufsysteme		D Vermeidung von offenen Sicherheitslücken	3%	0,4	
99				J Gewährleistung der Verfügbarkeit nötiger Ressourcen			
100	mind. 2, Prüfschwerpunkte	2 - IT-basierte Diagnose und Therapie-Systeme (allgemein)		H Bewältigung von Sicherheitsvorfällen	3%	0,4	
101				D Vermeidung von offenen Sicherheitslücken			
102	kDL-Systeme: vorzugsweise Kritikalitätsklasse 3 und frei wählbare Prüfschwerpunkte	Prüfumfang: variabel innerhalb des Prüfkontingentes Systembezeichnung gemäß Risikoanalyse/B3S-Informationsverbundsanalyse		Prüfkatalog-Controls	Prozentanteil an der Detailprüfung	PRT-Tage Realitäts-abgleich	Kommentar:
103	mind. 1, Prüfschwerpunkt	3 - Bettenterminals		D Vermeidung von offenen Sicherheitslücken	2%	0,2	
104	mind. 1, Prüfschwerpunkt	3 - Versorungs- und Entsorgungstechnik (IT-gesteuert)		A Absicherung von Netzübergängen	2%	0,2	
105	Zusatzprüfung, frei wählbar	ISO27001 Dokumentenprüfung		Zusatzaufwand	3%	0,4	
106	Zusatzprüfung, frei wählbar				0%	0	
107	Summe der dynamischen PRT-Tage		61%	7,40			
108	Gesamtaufwand in PRT	12,4	12,4	OK			

Die Tabellensegmente „**kDL-Systeme: vorzugsweise Kritikalitätsklasse 2**“ und „**kDL-Systeme: vorzugsweise Kritikalitätsklasse 3 und frei wählbare Prüfschwerpunkte**“ ermöglichen es dem Prüfteam flexibel weitere IT-Systeme zum Prüfschwerpunkt aus dem Portfolio der risikobewerteten IT-Systeme zu erklären. Die Detailprüfschwerpunkte ergeben sich auch hier aus dem gewählten Prüfreferenzkatalog mit jeweils zwei bzw. einem Control. Weiterhin können zwei Positionen im Prüfplanungsrahmen frei gewählt werden. Die jeweiligen Prüfzeiten werden als Prozentanteil des Gesamtprüftagekontingentes eingetragen. Die erfolgt solange, bis das Prüftagekontingent erschöpft ist. Um den Abgleich der gewählten Prüfzeiten mit dem Gesamtprüftagekontingent zu erleichtern, weist die „Zeile 108“ das Gesamtkontingent und die verplante Prüfzeit aus. Des Weiteren wird mittels eines Hilfsfeldes ausgewiesen, ob der Abweichungsrahmen von 5% der Gesamtprüfzeit eingehalten wird. Zeigt das in Grün unterlegte Feld ein „OK“ einspricht die Prüfplanung den Rahmenvorgaben.

Tabellenblatt: “Rahmenvorgaben“

Aufgabe: Das Tabellenblatt „Rahmenvorgaben“ fasst die wesentlichen Vorgaben zur Nutzung des §8a Prüfnachweisplanungstools vor dem Hintergrund der durch den BAK „medizinische Versorgung“ definierte Branchenvorgabe für einen §8a Prüfnachweis aus.

Detailinformationen:

	Prinzipieller Aufbau Tabellenblatt "Prüfnachweisplaner"
1	"Ausdruckbereich/Blatt 1" (ab Zeile 2) ist vom Betreiber auszufüllen und definiert den Prüfumfang in Prüftagen (PRT) und den generell gewählten Prüfreferenzkatalog
2	"Ausdruckbereich/Blatt 2" (ab Zeile 44) ist von der "Prüfenden Stelle" auszufüllen und definiert den Prüfplan für die allgemeine ISMS-Prüfung durch das Audit-Team
3	"Ausdruckbereich/Blatt 3" (ab Zeile 65 ff.) ist von der "Prüfenden Stelle" auszufüllen und definiert den Prüfplan für die spezielle, kDL-bezogenen Prüfung durch das Audit-Team

	Tabellenblatt "Risikoanalyse"
	Das Tabellenblatt "Risikoanalyse" ist vom Betreiber auszufüllen. Es gibt generell im Krankenhausbetrieb wichtige IT-Systeme zur Risikobewertung durch den Betreiber vor und erlaubt die Eingabe weiterer, für den kDL-Betrieb wichtiger IT-Systeme im spezifischen Betreiberkontext, gemäß der kDL-Risikoanalyse des Betreibers. Die Tabelle dient - nach Änderung und Neuaufruf des Prüfnachweisplaner-Tools - als Auswahlfeldvorgabe im Tabellenblatt "Prüfnachweisplaner".

	Tabellenblatt "Prüfungsfeststellungen"
	Das Tabellenblatt "Prüfungsfeststellung" ist von der prüfenden Stelle auszufüllen und gibt die Prüfungsfeststellungen der jeweiligen §8a Prüfung im Betreiberkontext wieder. Hierbei werden die im Prüfnachweisplanerblatt ausgewählten Prüfplanungsschwerpunkte referenziert. Das Tabellenblatt "Prüfungsfeststellung" ist als Hilfe in der Prüfnachweisführung gedacht und kann durch Überführen, z.B. in ein MS Word-Dokument als Basis für die geforderte "Prüfungsfeststellungs-Mängelliste" in der Meldung an das BSI genutzt werden.

	Rahmenvorgaben Prüfnachweisführung:
1	Das **Prüftagekontingent** ergibt sich durch Übernehmen der Zahlenwerte aus der **Betreiberklassifikationstabelle nach Fallzahl/a und Fachabteilung sowie Forschungs- und Lehre-Gewichtung** aus dem Tabellenblatt "Prüfnachweisplaner". Das kaufmännische Runden des ermittelten Prüftagekontingentwertes ist, so sinnvoll, erlaubt. Dieses Prüftagekontingent gilt unabhängig von der Anzahl der Prüfteammitglieder als **Gesamtprüftagevorgabe**. Der sich auf dem Kreuzungspunkt der "Tabelle zur Ermittlung des Prüftagekontingentes nach Betreiberkomplexität" im Prüfplaner-Tabellenblatt ergebenden Prüftagekontingentwert, sowie den jeweilige Hebefaktor "Forschung und Lehre" muss mit dem in der Tabelle angezeigten Wert, also z.B. "14" und "1,1", in das jeweilige Eingabefeld des Prüfnachweisplaners eingetragen werden, so zutreffend.
2	**Fachabteilungen** nach letztveröffentlichtem bzw. öffentlich zugänglichen Qualitätsreport: "https://www.deutsches-krankenhaus-verzeichnis.de"
3	**Das Prüftagekontingent darf nicht überschritten werden**. Eine **Unterschreitung der Planungswerte von max. 5%** ist möglich, sollte aber vermieden oder begründet werden.
4	Der gewählte Prüfkatalog ist als **"Referenz-Prüfkatalog " und somit als Prüfdiskussionsbasis** zu verstehen. Es geht darum, den Prüfrahmen zu definieren und den vom Betreiber zu einem Control angestrebten Lösungsansatz im Kontext der Aufrechterhaltung der kDL zu bewerten. Es geht nicht um einen Prüfkatalogprüfung in Form einer Checkliste, der die IT-Sicherheitsmaßnahme statisch vorgibt, und vom Betreiber dem Wortlaut nach umzusetzen ist.

5	Die Prüfung teilt sich in eine allgemeine, weitgehend organisatorisch-regelungsfokussierte **"ISMS-Schwerpunktprüfung"** ("Ausdruckbereich/Blatt 2", ca. 35% des Prüftagekontingentes) mit mindestens **4 zu wählenden Schwerpunkten** aus dem gewählten Prüfkatalog , einer **"technischen Basis-Infrastrukturprüfung"** nach **4 ausgewählten Controls des BSI-Grundschutz-Kompendiums** ("Ausdruckbereich/Blatt3.1") sowie einer "k**DL-bezogenen Schwerpunktprüfung**" ("Ausdruckbereich/Blatt3.2") auf. Der technisch- und kDL-bezogene Realitätsüberprüfungsanteil (Vorort-Prüfung) soll hierbei ca. 65% des Gesamtprüfungsumfangs ausmachen.
6	Die **branchenspezifische, kDL-bezogene Schwerpunktprüfung erfolgt risikobasiert auf Basis der Risikoanalyse des Betreibers**, der den im Informationsverbund betriebenen IT-Systemen eine entsprechende Risikoeinstufung in Bezug auf die Relevanz des Systems für die Aufrechterhaltung der kDL im Tabellenblatt "Risikoanalyse" zugewiesen hat. Die Definition der **Risikoklassifikation nach drei Risikoklassen (Klasse1: "kurzfristig verzichtbar", Klasse 2: "mittelfristig verzichtbar", Klasse 3: "längerfristig verzichtbar")**, kann dem Tabellenblatt "Risikoanalyse" entnommen werden.
7	Die **branchenspezifische, kDL-bezogene Schwerpunktprüfung** umfasst zwingend 4 kDL-relevante Informationssysteme der **Risikobewertungsklasse 1 mit jeweils 3 Schwerpunkt-Controls** aus dem ausgewählten Detailprüfkatalog sowie Prüfungen von Systemen der vom Betreiber mit **Risikoklasse 2 bewerteten Systeme mit zwei Schwerpunkt-Controls** aus dem gewählten Detailprüfkatalog und sowie einer Prüfung von **Risikoklasse 3 Systemen oder frei wählbaren Prüfschwerpunkten nach dem noch verfügbaren Prüftage-Kontingent**.
8	Der **Prüfumfang der Risikoklasse 2 und Risikoklasse 3 Systeme bzw. für die freien Prüfschwerpunkte** soll so gewählt werden, dass die Wahl des Zeitkontingents für die Prüfungsschwerpunkte entsprechend der Risikoklassifikation gewichtet wird. Die Prüfungsvorgabe ist bei Klasse2/3 Systemen als Empfehlung zu verstehen. Es können demzufolge hier auch weitere Risikoklasse-1-Systeme geprüft werden.
9	Die für die einzelnen Prüfschwerpunkte ausgewiesenen **Prüftagekontingente sind Richtwerte**, Über- oder Unterschreitungen des Prüfaufwandes in einem begründbaren Rahmen sind erlaubt.
10	Die im Tabellenblatt ausgeweisenen "Ausdruckbereiche/ Blatt 1 bis Blatt 3" dienen der **Angebotseinholung und der Kommunikation** zwischen mit Betreiber, der aktuellen "Prüfenden Stelle", dem Prüfteam und den nachprüfenden "Prüfenden Stellen" bzw. den nachprüfenden Prüfteams im Zeitverlauf.
11	Das Excel-Tabellenblatt kann **nicht nur für eine Prüfplanung nach B3S** herangezogen werden. Auch andere Prüfgrundlagen, ISO27001&ISO27002, ISO27001&ISO27799, BSI Grundschutz und IDW_PS_330, sind möglich.
12	Die Prüfplanung nach dieser Excel-Arbeitsmappe kann auch **Grundlage für eine Zertifizierung gemäß ISO o.ä. sein, soweit die "Prüfende Stelle" dies bestätigt**.
13	Eine **Reduktion des Prüftagekontingentes** ist im Ermessen der "Prüfenden Stelle" möglich, wenn der zu prüfende KRITIS-Betreiber entsprechende **Fremdzertifikate** (ISO270001 o.ä.) vorlegen kann. Die "Prüfende Stelle" ist gehalten diese Fremdzertifikate anzuerkennen, soweit sie im Scope und im Statement of Applicability (SOA) passen. Der hierzu nötige Prüfaufwand ist nach der Gesamtkontingentsreduktion in der Detailprüfungsplanung auszuweisen. Soweit ein KRITIS-Betreiber nur eine Teilzertifzierungvorweisen kann, ist dies ebenfalls in der Prüfplanung entsprechend zu berücksichtigen.
14	Eine **Reduktion des Prüftagekontingentes** ist im Ermessen der "Prüfenden Stelle" möglich, wenn der zu prüfende KRITIS-Betreiber zentrale IT-Einrichtungen betreibt, bei denen ggf. eine **Doppelprüfung** ausgewiesen würde, soweit mehrere Betriebsstätten des Betreibers unter die KRITIS-Verordnung fallen. Hierzu muss der Betreiber jedoch für alle Betriebsstätten seines Verbundes die gleiche "Prüfende Stelle" beauftragen. Die "Prüfende Stelle" wiederum, muss in der Detailplanung ausweisen, dass die zentrale IT-Einrichtung anteilig für jeden Betreiber mit geprüft wurde.

Tabellenblatt: “Risikoanalyse“

Aufgabe: Das Tabellenblatt „Risikoanalyse“ dient dazu, in der Regel kDL-relevante IT-Systeme eines Krankenhauses vorzudefinieren. Diese IT-Systeme definieren den Scope der kDL-Detailprüfung im Prüfnachweisplanertool, können jedoch flexibel, je nach Betreibersituation risikobewertet, aus dem Scope entfernt oder durch weitere IT-Systeme ergänzt werden.

Detailinformation:

1	Zurück	
2	**Risikobewertungsmatrix kDL-relevante IT-Systeme**	
3	**RisikoKlassen**	
4	**Klasse 1:** Die Störung eines Systems der Klasse 1 führt bereits nach kurzer Zeit zu relevanten Mehrbelastungen der Organisationseinheiten, einer Einschränkung der medizinischen Leistungserbringung. Darüber hinaus ist bei einem längeren Ausfall mit wirtschaftlichen Folgen zu rechnen. Die konkrete Zeitspanne ist im Einzelfall den Gegebenheiten vor Ort angemessen anzupassen.	**1**
5	**Klasse 2:** Systeme, deren Störung über einen mittleren Zeitraum durch die Organisation (Notfallkonzepte) beherrscht werden können, ohne dass eine relevante Einschränkung der medizinischen Leistungserbringung zu befürchten ist, werden als Systeme der Klasse 2 bezeichnet.	**2**
6	**Klasse 3:** Die Einordnung als System der Klasse 3 erfolgt für diejenigen Systeme im Krankenhaus, für die längere Störungszeiten durch die Organisation ohne relevante Einschränkung der medizinischen Leistungserbringung beherrschbar sind.	**3**
7	**Klasse 0:** Bitte Klasse "0" bei den Vorgabesystemen wählen, wenn eine Differenzierung der betreffenden IT-Systeme im freien Eingabeteil erfolgt, z.B. weil mehrere PACS oder Laborsysteme usw. im Einsatz sind.	**0**
8	**Nach Änderungen Excel-Sheet speichern, schliessen, neuaufrufen um Auswahllisten zu aktualisieren! Im Eingabeteil erfolgt löschen eines Eintrages auf dem Eingabefeld mit "rechter Maustaste" & "Inhalte löschen"**	
9	**Auswahlkatalog**	**kDL-relevante Systeme im Informationsverbund**	**Risikoklasse**
10	**1 - Krankenhausinformationssystem (KIS)**	Krankenhausinformationssystem (KIS)	**1**
11	**1 - Laborinformationssystem (LIS)**	Laborinformationssystem (LIS)	**1**
12	**1 - Dokumenten-Management-System / Enterprise-Content-Management**	Dokumenten-Management-System / Enterprise-Content-Management	**1**
13	**1 - Radiologieinformationssystem (RIS)**	Radiologieinformationssystem (RIS)	**1**
14	**1 - Picture Archive and Communication System (PACS)**	Picture Archive and Communication System (PACS)	**1**
15	**1 - OP-Planungssystem**	OP-Planungssystem	**1**
16	**1 - Blut- und Transfusionsprodukteverwaltung**	Blut- und Transfusionsprodukteverwaltung	**1**
17	**3 - Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransp**	Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)	**3**
18	**1 - Heil- und Hilfsmittelversorgungssysteme**	Heil- und Hilfsmittelversorgungssysteme	**1**
19	**1 - Apothekensystem**	Apothekensystem	**1**
20	**1 - elektronische Patientenakte**	elektronische Patientenakte	**1**
21	**1 - Patientenmanagementsystem (PDMS/Intensivdatenverwaltung)**	Patientenmanagementsystem (PDMS/Intensivdatenverwaltung)	1
22	**1 - netzgebundene medizintechnische Systeme (allgemein)**	netzgebundene medizintechnische Systeme (allgemein)	1
23	**1 - Telemedizinsysteme**	Telemedizinsysteme	1
24	**1 - Telemetriesysteme**	Telemetriesysteme	1
25	**1 - Teleradiologiesysteme**	Teleradiologiesysteme	1
26	**1 - netzgebundene Alarmierungssysteme (allgemein)**	netzgebundene Alarmierungssysteme (allgemein)	1
27	**2 - IT-basierte Diagnose und Therapie-Systeme (allgemein)**	IT-basierte Diagnose und Therapie-Systeme (allgemein)	2
28	**2 - Rufsysteme**	Rufsysteme	**2**
29	**2 - Dienstelefonie/Festnetz**	Dienstelefonie/Festnetz	2
30	**1 - Dienstelefonie/Mobil**	Dienstelefonie/Mobil	1
31	**2 - Fax-Betrieb**	Fax-Betrieb	2
32	**3 - Rohrpostsysteme**	Rohrpostsysteme	3
33	**3 - Wechselsprechtechnik**	Wechselsprechtechnik	3
34	**1 - Mobile Devices im Behandlungsprozess**	Mobile Devices im Behandlungsprozess	1

Der erste Teil des Tabellenblattes „Risikoanalyse“ gibt ein Portfolio von branchenspezifisch relevanten IT-Systemen für die Erbringung der kritischen Dienstleistung „stationäre, medizinische Versorgung“ und eine entsprechende Risikobewertung vor. Während das IT-Systemportfolio an dieser Stelle nicht veränderbar ist, kann die Risikobewertung durch den Betreiber mittels der orange unterlegten Auswahlfelder verändert werden. Dies ist z. B. dann sinnvoll, wenn einem IT-System in der Risikobewertung des Betreibers eine andere Risikoklassifikation zugeordnet worden ist. Wird ein aufgeführtes IT-System vom Betreiber gar nicht betrieben, kann es mit der Risikoklassifikation „0“ deaktiviert werden. Hier ist eine entsprechende Begründung in der eigenständigen Risikobewertung des Betreibers zu vermerken. Wird ein System in mehreren Varianten betrieben, kann der Eintrag im fest vorgegebenen IT-Systemportfolio ebenfalls mit der Auswahl Risikoklasse „0“neutralisiert werden. In diesem Fall müssen die jeweiligen, zusätzlichen IT-Systeme gemäß Betreiberrisikobewertung im Tabellenblatt ab Zeile 48 ergänzt werden.

Achtung: Änderungen an der Risikoklassifikation sind leider nur durch gezielte Anwahl der Auswahloptionen in den Auswahlfeldern möglich. Bei Eingabe einer Ziffer wird ein Excel-Fehler ausgewiesen.

Ergänzungen des IT-Systemportfolios entsprechend der Risikoanalyse- und Bewertung des Betreibers können im unteren Teil des Tabellenblattes gemacht werden ab Zeile 48. Hierzu wir der Name eines IT-Systems in das jeweilige Eingabefeld eingetragen und eine Risikobewertungsziffer gemäß Risikobewertung ausgewählt. Wird hier keine Risikobewertung vorgenommen, erhält das System automatisiert die Risikoklassifikation „1“, besonders kDL-kritisch. Maximal können 100 IT-Systempositionen gefüllt werden. Die Risikoklassifikationsziffern dienen gleichzeitig als Sortierkriterium in den Auswahlfeldern des Prüfnachweisplaner-Tabellenblattes.

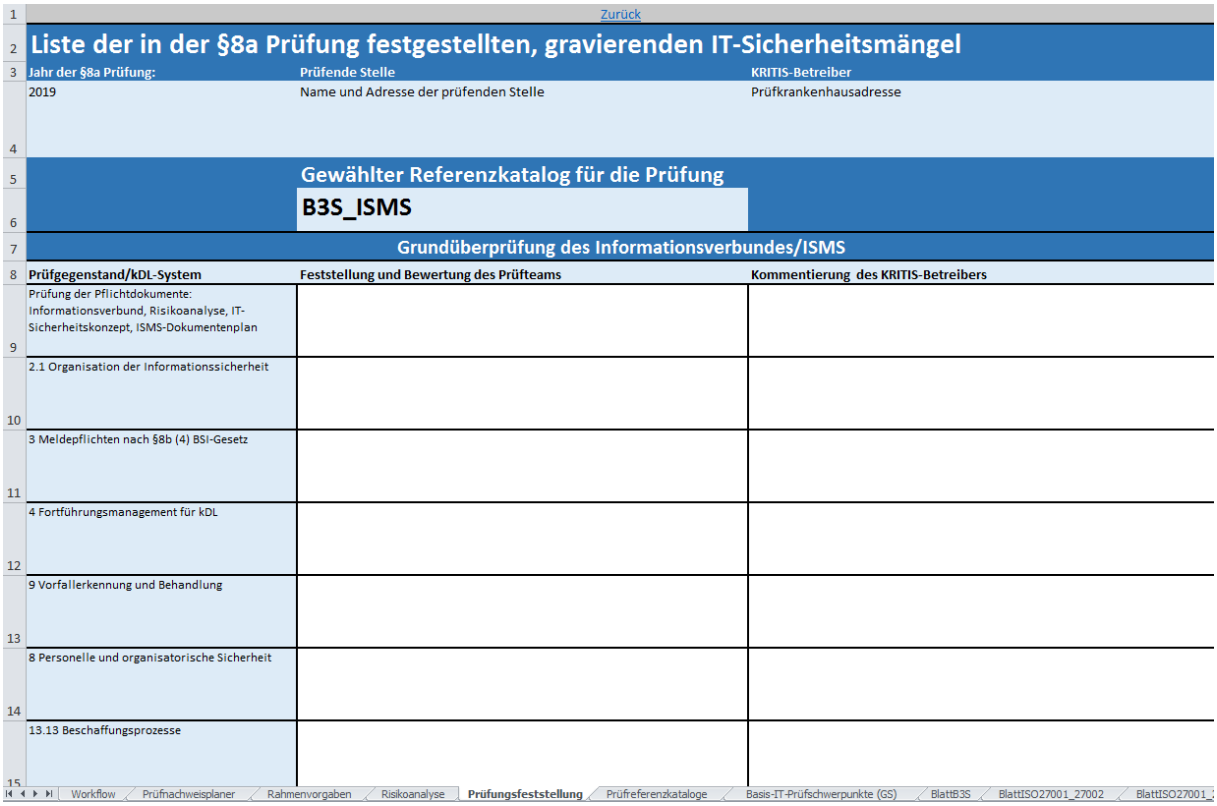
35	**3 - Bettenterminals**	Bettenterminals	3
36	**1 - Energieversorgung (IT-gesteuert, IT-benötigt)**	Energieversorgung (IT-gesteuert, IT-benötigt)	1
37	**2 - Wasserversorgung (IT-gesteuert, IT-benötigt)**	Wasserversorgung (IT-gesteuert, IT-benötigt)	2
38	**2 - Wärme/Heizungssysteme (IT-gesteuert)**	Wärme/Heizungssysteme (IT-gesteuert)	2
39	**1 - Klima/Kühlung (IT-gesteuert, IT-benötigt)**	Klima/Kühlung (IT-gesteuert, IT-benötigt)	1
40	**1 - Lichttechnik (IT-gesteuert, IT-benötigt)**	Lichttechnik (IT-gesteuert, IT-benötigt)	1
41	**1 - Gase (IT-gesteuert)**	Gase (IT-gesteuert)	1
42	**1 - Transportanlagen/Aufzüge (IT-gesteuert/IT-Zugangsberechtigt)**	Transportanlagen/Aufzüge (IT-gesteuert/IT-Zugangsberechtigt)	1
43	**3 - Versorungs- und Entsorgungstechnik (IT-gesteuert)**	Versorungs- und Entsorgungstechnik (IT-gesteuert)	3
44	**3 - Videoüberwachung (IT-gesteuert)**	Videoüberwachung (IT-gesteuert)	3
45	**1 - Zugangs- und Schließsysteme (IT-gesteuert)**	Zugangs- und Schließsysteme (IT-gesteuert)	1
46	**1 - Gebäudeleittechnik/Gebäudeautomationstechnik (IT-gesteuert)**	Gebäudeleittechnik/Gebäudeautomationstechnik (IT-gesteuert)	1
47	**3 - Liegenschaftsverwaltungssystem**	Liegenschaftsverwaltungssystem	3
48	**2 - Schliesssystem Zentralklinikum**	Schliesssystem Zentralklinikum	2
49	**1-Schliesssystem OP-Trakt**	Schliesssystem OP-Trakt	
50	-		
51	-		
52	-		
53	-		

Achtung: Nach einer Änderung am IT-Systemportfolio oder einer neu Bewertung des IT-Systemrisikos per Auswahlfeld, muss der Prüfplaner gespeichert, geschlossen und neu gestartet werden, um eine Aktualisierung aller abhängigen Auswahlfelder in der Prüfnachweisplaner-Tabelle und in der Prüffeststellungstabelle zu erreichen.

Tabellenblatt: “Prüfungsfeststellung“

Aufgabe: Das Tabellenblatt Prüfungsfeststellung gibt einen formatierten Rahmen für die Erfassung der Prüfungsfeststellung des Prüfteams vor. Hierbei werden die Controls des gewählten Prüfplans aus dem Prüfnachweisplaner-Tabellenblatt entsprechend übertragen.

Detailinformation:



1	Zurück		
2	**Liste der in der §8a Prüfung festgestellten, gravierenden IT-Sicherheitsmängel**		
3	**Jahr der §8a Prüfung:**	**Prüfende Stelle**	**KRITIS-Betreiber**
4	2019	Name und Adresse der prüfenden Stelle	Prüfkrankenhausadresse
5		**Gewählter Referenzkatalog für die Prüfung**	
6		**B3S_ISMS**	
7	**Grundüberprüfung des Informationsverbundes/ISMS**		
8	**Prüfgegenstand/kDL-System**	**Feststellung und Bewertung des Prüfteams**	**Kommentierung des KRITIS-Betreibers**
9	Prüfung der Pflichtdokumente: Informationsverbund, Risikoanalyse, IT-Sicherheitskonzept, ISMS-Dokumentenplan		
10	2.1 Organisation der Informationssicherheit		
11	3 Meldepflichten nach §8b (4) BSI-Gesetz		
12	4 Fortführungsmanagement für kDL		
13	9 Vorfallerkennung und Behandlung		
14	8 Personelle und organisatorische Sicherheit		
15	13.13 Beschaffungsprozesse		

Workflow | Prüfnachweisplaner | Rahmenvorgaben | Risikoanalyse | **Prüfungsfeststellung** | Prüfreferenzkataloge | Basis-IT-Prüfschwerpunkte (GS) | BlattB3S | BlattISO27001_27002 | BlattISO27001_

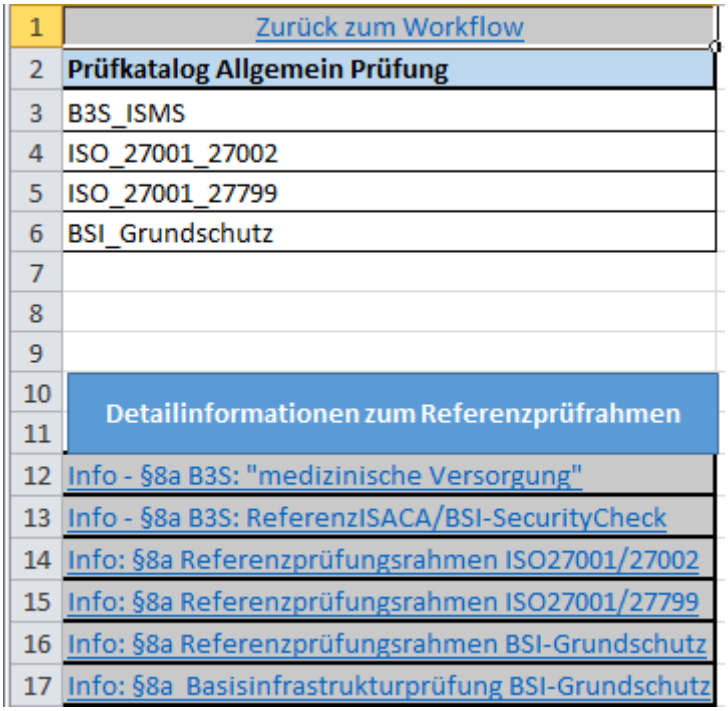
Das Tabellenblatt Prüfungsfeststellung dient der formatierten Dokumentation der Prüfungsfeststellung durch das Prüfteam sowie einer Dialogbewertung der getroffenen Prüfungsentscheidung durch den Betreiber. Die primäre Idee hierbei ist, bei Meinungsverschiedenheiten in der Bewertung eines Sachverhaltes beide Bewertungen, die Bewertung des Prüfteams und die Bewertung des Betreibers, gelten zu lassen und an das BSI zu übermitteln. Da ein vorab festgelegter IT-Sicherheitsstandard im Krankenhausumfeld derzeit nicht zu definieren ist und oftmals Konfigurationsentscheidungen an medizinisch-organisatorischen Aspekten und nicht nur an IT-technischen Aspekten orientiert sind, soll hierdurch ein möglichst konfliktfreier Prüfungsfeststellungsprozess ermöglicht werden.

Da Excel in der Textverarbeitung Schwächen hat, kann das vorausgefüllte Tabellenblatt auch in ein Worddokument kopiert und dort ausgefüllt werden. Aus der Prüffeststellungsdokumentation für den Betreiber leitet sich dann die an das BSI zu übermittelnde „Mängelnachweis“ durch die prüfende Stelle ab. Das Prüfnachweisplanertool hat hier jedoch die Aufgabe die Kommunikation zwischen Betreiber und Prüfteam zu strukturieren und das Prüfteam bei der Erstellung eines strukturierten Prüffeststellungsnachweises zu unterstützen. Es hat nicht die Aufgabe, die vom BSI vorgegebenen Anlagen zum Prüfnachweis automatisiert zu erzeugen.

Tabellenblatt: “Prüfreferenzkataloge“

Aufgabe: Das Tabellenblatt „Prüfreferenzkatalog“ fasst die dem Prüfnachweisplanertool unterlegten Prüfreferenzkataloge zusammen und erlaubt die Navigation durch die so definierten Prüfungs-Grundlagen

Detailinformation: „Prüfreferenzkataloge“



Die genannten Prüfreferenzkataloge sind im Prüfnachweisplanertool nicht vollständig abgebildet, sondern z. T. so angepasst worden, dass der Prüfreferenzkatalog auf die Problemstellung der Absicherung der kDL „medizinische Versorgung“ fokussiert ist. Soweit möglich und nötig sind Quellenangaben zur primären Herkunft der Referenzkataloge aufgeführt. Die folgende Darstellung gibt ein Beispiel zum Aufbau eines solchen Referenzkatalogs, der als Grundlage für die Auswahlfelder des Tabellenblattes „Prüfnachweisplaner“ dient.

Tabellenblatt: “BlattISO27001_27002“

	A
1	Zurück
2	**Name: ISO_27001_27002**
3	A.5 IS-Management
4	A.6 IS-Organisation
5	A.7 Personal
6	A.8 Asset Management
7	A.9 Zugangssteuerung System- /Netzadministration
8	A.10 Kryptographie
9	A.11 Physische und umgebungsbezogene Sicherheit - Standortsicherheit
10	A.12 IT-Betrieb
11	A.13 Kommunikationssicherheit
12	A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
13	A.15 Lieferantenbeziehungen (Procurement)
14	A.16 Handhabung von Informationssicherheitsvorfällen
15	A.17 Informationsssicherheitsaspekte beim Business Continuity Management (Notfallmanagement)
16	A.18 Compliance
17	
18	
19	**Name: ISO_27002**
20	**5 Sicherheitsleitlinien**
21	5.1 Managementausrichtung zur Informationssicherheit
22	5.1.1 Informationssicherheitsleitlinien
23	5.1.2 Überprüfung der Informationssicherheitsleitlinien
24	**6 Organisation der Informationssicherheit**
25	6.1 Interne Organisation
26	6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit
27	6.1.2 Aufgabentrennung
28	6.1.3 Kontakt zu Behörden
29	6.1.4 Kontakt mit Interessengruppen
30	6.1.5 Informationssicherheit im Projektmanagement
31	6.2 Mobilgeräte und Telearbeit
32	6.2.1 Leitlinie zu Mobilgeräten
33	6.2.2 Telearbeit
34	**7 Personalsicherheit**
35	7.1 Vor der Anstellung
36	7.1.1 Überprüfung
37	7.1.2 Arbeitsvertragsklauseln
38	7.2 Während der Anstellung
39	7.2.1 Verantwortung des Managements
40	7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit
41	7.2.3 Disziplinarverfahren
42	7.3 Beendigung und Wechsel der Anstellung

Schlussbemerkung:

Eine solche Ausfüllhilfe kann immer nur grundlegende Aspekte des Umgangs mit dem Prüfnachweis-planertool abdecken. Für unklare Beschreibungen oder Schreibfehler entschuldigt sich das Auto-renteam im Vorhinein und freut sich über entsprechende Korrekturhinweise und Verbesserungshin-weise an den BAK „medizinische Versorgung“.