Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG

Version 1.1
vom 21.08.2020

Versionshistorie

Datum	Version	Verfasser	Bemerkungen
15.05.2019	1.0	BSI	• Finale Abstimmung im BSI, Herstellung der Barrierefreiheit des Dokuments
03.08.2020	1.1	BSI	• Vereinheitlichung des Glossars und der Bezeichnungen • Ergänzungen zu neu registrierten Anlagen • Ergänzungen zur Selbsterklärung • Darstellung und Anpassung der Prüfthemen, Erläuterungen zu Informationen zum Ablauf der Prüfung • Anforderungen an die Darstellung des Geltungsbereiches • Erläuterungen zum Netzstrukturplan • Einschätzung des Reifegrads von ISMS und BCMS • Mängelliste (in der Mängelliste sollen Mängel nach Thema und Schwere klassifiziert werden)
21.08.2020	1.1	BSI	• Einarbeitung von Kommentierungen aus dem TAK-AS

Alle Funktionsbezeichnungen sind geschlechtsneutral zu verstehen und stehen zur Anwendung für weibliche, männliche und anderweitige Geschlechteridentitäten gleichermaßen zur Verfügung.

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0

E-Mail: kritische.infrastrukturen@bsi.bund.de

De-Mail: de-mail@bsi-bund.de-mail.de

Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Überblick

1.1 Einführung

Eine Kritische Infrastruktur im Sinne des BSI-Gesetzes (BSIG) und der BSI-Kritisverordnung (BSI-KritisV) betreibt, wer festgelegte qualitative und quantitative Kriterien erfüllt. Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) müssen gemäß § 8a Absatz 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.

Nachweispflichtig sind alle Betreiber Kritischer Infrastrukturen gemäß BSI-KritisV, mit Ausnahme der in § 8d Absatz 2 BSIG genannten.

Für jede nachweispflichtige Infrastruktur bzw. Anlage müssen KRITIS-Betreiber Nachweisdokumente beim BSI einreichen. Diese umfassen sowohl allgemeine Informationen über Art und Umfang der durchgeführten Prüfungen als auch eine Liste der aufgedeckten Sicherheitsmängel.

Das BSI kann zudem gemäß § 8a Absatz 3 BSIG „[...] die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln ggf. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder ggf. im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen." Sollten Fragen nicht final geklärt werden können, so kann das BSI sich außerdem durch eigene Vor-Ort-Prüfungen entsprechend § 8a Absatz 4 BSIG einen eigenen Eindruck von Sicherheitsvorkehrungen des KRITIS-Betreibers verschaffen.

1.2 Zielsetzung der Orientierungshilfe

Das vorliegende Dokument soll KRITIS-Betreibern und prüfenden Stellen eine Orientierung geben, was in § 8a Absatz 3 BSIG unter *„auf geeignete Weise"* in Bezug auf eine Prüfung zu verstehen ist und wie die gesetzlichen Anforderungen aus § 8a Absatz 3 BSIG erfüllt werden können. Es beschreibt die Anforderungen an die Beteiligten sowie deren Aufgaben und Zuständigkeiten und liefert Rahmenbedingungen an einen geeigneten Nachweis. Es erläutert den Ablauf der Einreichung von Nachweisen, zu beachtende formale Aspekte und einzuhaltende Fristen.

Im vorliegenden Dokument werden folgende Fragen beantwortet:

- Wie können KRITIS-Betreiber bei der Erfüllung der Nachweispflicht nach § 8a Absatz 3 BSIG vorgehen? Welche Informationen sollten sie wem bereitstellen? (siehe Kapitel 2)
- Welche Aufgaben haben prüfende Stellen? Was sind geeignete prüfende Stellen? (siehe Kapitel 3)
- Welche Aufgaben hat das Prüfteam und welche Kompetenzen sollte es besitzen? (siehe Kapitel 4)

- Wie sollte die Prüfung durchgeführt werden (Prüfgrundlage, -themen, -methoden, Ergebnisse)? (siehe Kapitel 5)
- Wie werden Nachweisdokumente eingereicht und welche Fristen gibt es zu beachten (siehe Kapitel 6)?

1.3 Begriffserklärungen[1]

Die Orientierungshilfe unterscheidet zwischen den Begriffen der ***Prüfung***, dem ***Prüfbericht,*** den ***Nachweisdokumenten*** und dem ***Nachweis***.

Unter dem Begriff ***Prüfung*** werden in diesem Dokument „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ gemäß § 8a Absatz 3 BSIG verstanden. Prüfungen werden durch eine prüfende Stelle mit Hilfe eines Prüfteams vorgenommen und die Ergebnisse werden dem KRITIS-Betreiber vorgelegt.

Der ***Prüfbericht*** ist das Dokument, das die Prüfergebnisse enthält. Der Prüfbericht wird von der prüfenden Stelle erstellt und dem KRITIS-Betreiber vorgelegt. Das BSI kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde (z. B. IT-Sicherheitskonzepte, Prozessdokumentationen, Prüfbericht, Business Continuity Management- und Notfallkonzepte), verlangen.

Als ***Nachweisdokumente*** werden die Formulare und die zugehörigen Anlagen bezeichnet, die der KRITIS-Betreiber **für jede registrierte Anlage (ggf. auch gebündelt)** beim BSI einreicht.

Sie bestehen aus:

- der Bestätigung der prüfenden Stelle, dass der Betreiber die gesetzlichen Anforderungen aus § 8a Absatz 1 BSIG erfüllt und hiervon abweichende Feststellungen als Sicherheitsmängel erfasst sind,
- allgemeinen Informationen über Art und Umfang der durchgeführten Prüfungen,
- den vom BSI bereitgestellten Formularen
  - KI mit Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner sowie
  - P mit Angaben zur Prüfdurchführung mit Zeiten und Umfang (Abschnitt PD), zum Prüfergebnis und zu den aufgedeckten Sicherheitsmängeln (Abschnitt PE) und zur prüfenden Stelle und zum Prüfteam (Abschnitt PS) und
- der Auflistung der Sicherheitsmängel und dem Umsetzungsplan.

Die Gesamtheit der ***Nachweisdokumente*** bildet den ***Nachweis***.

1.4 Rollen und Zuständigkeiten im Nachweisprozess

Von den in dieser Orientierungshilfe beschriebenen Rahmenbedingungen und Umsetzungshilfen sind die Rollen „KRITIS-Betreiber“, „Prüfende Stelle“, „Prüfteam“ und „BSI“ betroffen, die in Abbildung 1 dargestellt sind.

[1] Weitere Begriffserklärungen befinden sich im Glossar

Prüfende Stellen können aufgrund einer entsprechenden Anerkennung oder Akkreditierung oder in Form einer Selbsterklärung ihre Eignung erklären. Auf eine Darstellung dieses Aspekts wird in der Grafik verzichtet, da mit dem BSIG **kein** neues Anerkennungs-/Akkreditierungsverfahren eingeführt, sondern lediglich auf bestehende Verfahren verwiesen wird.

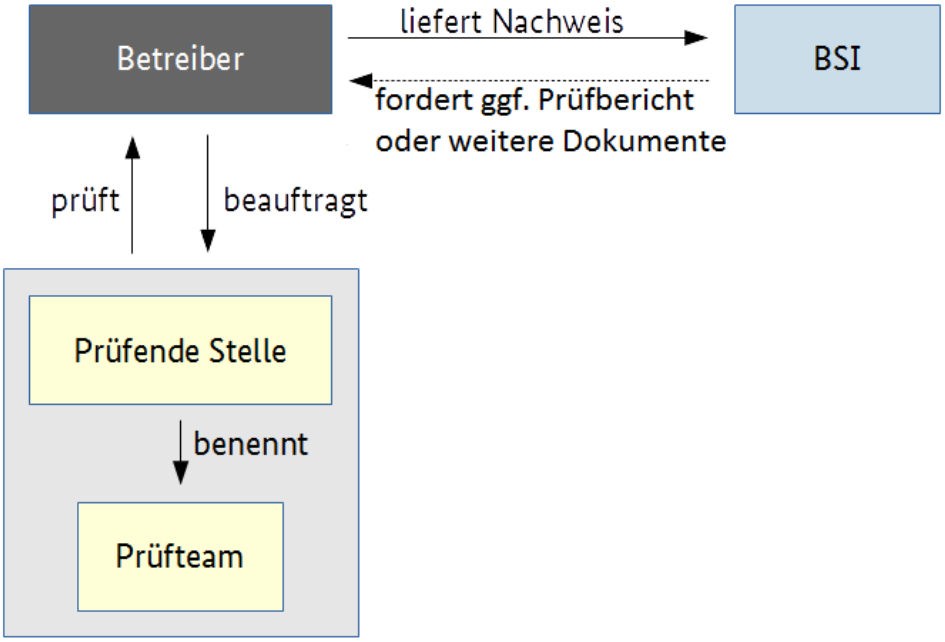

Abbildung 1: Rollen im Nachweisprozess, Quelle: BSI

1.4.1 KRITIS-Betreiber

Die KRITIS-Betreiber im Sinne des BSIG sind gemäß § 8a Absatz 3 BSIG verpflichtet, alle zwei Jahre die Umsetzung angemessener organisatorischer und technischer Vorkehrungen gemäß § 8a Absatz 1 BSIG nachzuweisen. Vorkehrungen sind angemessen, wenn der Aufwand zu den möglichen Folgen einer Störung für die Versorgungsleistung der Bevölkerung im Verhältnis steht. Die Vorkehrungen dienen der Sicherstellung der Funktionsfähigkeit der kritischen Dienstleistungen (kDL) und damit der Aufrechterhaltung der Versorgungsleistung.

Der KRITIS-Betreiber beauftragt eine prüfende Stelle zur Durchführung der zur Erstellung eines Nachweises notwendigen Prüfung.

1.4.2 Prüfende Stelle und Prüfteam

Die prüfende Stelle stellt ein geeignetes, qualifiziertes und unabhängiges Prüfteam (siehe Kapitel 4) zusammen, das die eigentliche Prüfung vorbereitet, durchführt und in einem Prüfbericht dokumentiert. Die Zuständigkeiten der prüfenden Stelle bzgl. Prüfungen und Nachweisen werden detailliert in Kapitel 3 beschrieben.

Die prüfende Stelle trägt gegenüber dem KRITIS-Betreiber die Verantwortung für die korrekte Durchführung der Prüfung (siehe Kapitel 6) sowie für die Korrektheit des Prüfberichts und der zugehörigen Dokumente.

Aufgrund der geteilten Verantwortung der prüfenden Stelle gegenüber dem KRITIS-Betreiber und des KRITIS-Betreibers gegenüber dem BSI ist es empfehlenswert, die Pflichten zwischen prüfender Stelle und KRITIS-Betreiber unmissverständlich durch einen Vertrag zu vereinbaren.

1.4.3 BSI

Das BSI erhält vom KRITIS-Betreiber den Nachweis inklusive der Auflistung der Sicherheitsmängel mit dem zugehörigen Umsetzungsplan zum Umgang mit diesen Mängeln. Der Nachweis enthält darüber hinaus Informationen zur durchgeführten Prüfung, beispielsweise eine Beschreibung des Prüfgegenstands.

Das BSI nimmt den Nachweis des KRITIS-Betreibers entgegen, prüft diesen auf Vollständigkeit und bewertet in einem ersten Schritt, ob dessen Inhalte nachvollziehbar und aussagekräftig genug sind, um eine Einschätzung über die Erfüllung der Anforderungen zu ermöglichen. Offensichtlich fehlende Inhalte und Unterlagen fordert das BSI umgehend nach. Der KRITIS-Betreiber erhält nach Einreichung der vollständigen (also aller zur Nachweisprüfung erforderlichen) Unterlagen per E-Mail eine Empfangsbestätigung mit Angabe der neuen Nachweisfrist für die geprüften Anlagen (siehe Kapitel 6).

Weiterführende Prüfungen zum Nachweis können grundsätzlich bis zur Einreichung des darauffolgenden Nachweises nach verfügbaren Kapazitäten und im Ermessen des BSI erfolgen. Das BSI erteilt keine Bestätigung der inhaltlichen Qualität des Nachweises.

Sofern zum Nachweis keine Rückfragen erforderlich sind bzw. für die weiterführende Prüfung keine weitere Mitwirkung des KRITIS-Betreibers erforderlich ist, erhält der KRITIS-Betreiber nach der o. g. Empfangsbestätigung keine weitere Benachrichtigung zum Vorgang. Das BSI kann aber jederzeit weitere Teile bzw. die gesamte der Prüfung zugrunde liegende Dokumentation anfordern oder – auch anlassunabhängig – Vor-Ort-Prüfungen anberaumen.

2 Der KRITIS-Betreiber

Der KRITIS-Betreiber muss die Umsetzung der Anforderungen gemäß § 8a Absatz 1 BSIG (angemessene Vorkehrungen zur Vermeidung von Störungen unter Einhaltung des Stands der Technik) für seine Anlagen gewährleisten, soweit er hiervon nicht durch § 8d Absatz 2 BSIG befreit wurde. Dazu muss er zunächst einen geeigneten Geltungsbereich für den Prüfgegenstand (Scope) festlegen, die zugrundeliegenden Prozesse feststellen und entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren.

Anschließend muss er regelmäßig (mindestens alle zwei Jahre) einen Nachweis über die Umsetzung der Maßnahmen beim BSI einreichen.

Zum Nachweis der Umsetzung der Maßnahmen muss er eine geeignete prüfende Stelle beauftragen, die die Prüfung einer oder mehrerer Anlagen des KRITIS-Betreibers (Audit, Prüfung oder Zertifizierung) durchführt und dem KRITIS-Betreiber die Ergebnisse in einem Prüfbericht unter Auflistung der aufgedeckten Sicherheitsmängel schriftlich übermittelt.

Im nächsten Schritt reicht der KRITIS-Betreiber den Nachweis beim BSI ein. Nachweise sind dabei für jede Anlage gemäß BSI-Kritisverordnung (BSI-KritisV) zu erbringen. Wenn mehrere Anlagen vergleichbar sind und viele Prüfschritte gemeinsam durchgeführt werden, können die Informationen auch in einem Formular (P oder KI) zusammengefasst werden.

Im folgenden Abschnitt werden folgende Fragen beantwortet:

- Was gehört zum Geltungsbereich? (Abschnitt 2.1)
- Welche Dokumente sollte der KRITIS-Betreiber der prüfenden Stelle zur Durchführung der Prüfung bereitstellen? (Abschnitt 2.2)
- Welche Prüfgrundlagen können herangezogen werden? (Abschnitt 2.3)

2.1 Beschreibung des Prüfgegenstands

Eine geeignete Prüfung muss als Prüfgegenstand den vollständigen und aktuellen Geltungsbereich[2] der Kritischen Infrastruktur, also der Anlage gemäß BSI-KritisV, umfassen. In Vorbereitung auf die Prüfung muss der Geltungsbereich daher genau definiert und beschrieben werden (Abschnitt 5.2). Zusätzlich können wesentliche Punkte dieser Beschreibung auch in den Nachweisdokumenten (z. B. Anlage zu Formular P) aufgeführt werden.

Für die Prüfungsdurchführung und den Nachweis sollten

- die Anlage,
- die vom KRITIS-Betreiber erbrachten Teile der kritischen Dienstleistung,
- die Teile der kritischen Dienstleistung, die von externen Dienstleistern erbracht werden (z. B. Auslagerung, Erbringung durch Mutter-/Tochterkonzern),
- das Zusammenspiel mit anderen Systemen sowie
- die Schnittstellen und Abhängigkeiten

beschrieben werden.

Für die Prüfungsdurchführung sollten zudem alle

- informationstechnischen Systeme,
- Komponenten,
- Prozesse und
- Rollen, Personen und Organisationseinheiten

aufgeführt werden, die für die Funktionsfähigkeit der erbrachten kritischen Dienstleistung erforderlich sind oder die deren Funktionsfähigkeit beeinflussen (können). Ebenfalls sollte der Zusammenhang zwischen diesen Objekten dargestellt werden.

[2] Vgl. „Geltungsbereich“ im Glossar

2.2 Übliche Sicherheitsdokumentation

Damit das Prüfteam die Prüfung für den Nachweis nach § 8a Absatz 3 BSIG ordnungsgemäß durchführen kann, benötigt es einerseits konkrete Unterlagen und andererseits die Möglichkeit, eine Vor-Ort-Prüfung durchführen zu können. Die Vor-Ort-Prüfung beinhaltet notwendigerweise die Inaugenscheinnahme der Technik und Infrastruktur sowie tiefergehende Gespräche mit Mitarbeitern des KRITIS-Betreibers (siehe Kapitel 5).

Für die Dokumentenprüfung sollten KRITIS-Betreiber dem Prüfer z. B. folgende Dokumente bereitstellen[3]:

- Sicherheitskonzept (inkl. Darstellung umgesetzter und geplanter Maßnahmen, insbesondere der branchenspezifischen Maßnahmen und der aus der kDL abgeleiteten KRITIS-Schutzziele)
- Beschreibung des Informationssicherheitsmanagementsystems (ISMS)
- Notfallkonzept und Beschreibung des Continuity Managements
- Dokumente des Asset Managements
- Dokumentation der Prozesse zur baulichen und physischen Sicherheit (z. B. Zutrittskontrolle oder Brandschutzmaßnahmen)
- Dokumentation der personellen und organisatorischen Sicherheit (z. B. Aufzeichnungen über Mitarbeiterschulungen, Sensibilisierungskampagnen, Berechtigungsmanagement)
- Konzepte und Dokumentation zur Vorfallserkennung und -bearbeitung (z. B. Beschreibung zu Incident Management, Detektion von Angriffen, Forensik)
- Konzepte und Dokumentation von Überprüfungen (z. B. Prüfberichte der internen Revision sowie anderer durchgeführter Audits, Übungen, systematische Log-Auswertungen usw.)
- Richtlinien zur externen Informationsversorgung (Einholen von Informationen über Themen, die für die IT-Sicherheit relevant sind)
- Richtlinien zum Umgang mit Lieferanten und Dienstleistern (z. B. Service Level Agreements und andere die Sicherheit betreffende Vereinbarungen mit Dienstleistern)

Die prüfende Stelle kann auch weitere Dokumente als Grundlage der Prüfung heranziehen.

2.3 Wahl der Prüfgrundlage

Der KRITIS-Betreiber wählt in Abstimmung mit der prüfenden Stelle die Prüfgrundlage. Dabei können unter anderem folgende Fälle unterschieden werden, die in Abschnitt 5.1 bzgl. der Durchführung von Prüfungen genauer beschrieben werden, wobei die Fälle sich nicht gegenseitig ausschließen:

- Prüfung auf Grundlage eines geeigneten branchenspezifischen Sicherheitsstandards (B3S) (Abschnitt 5.1.1)
- Prüfung ohne Verwendung eines branchenspezifischen Sicherheitsstandards (B3S) (Abschnitt 5.1.2)
- Berücksichtigung vorhandener Prüfungen oder anderer Prüfgrundlagen (Abschnitt 5.1.3)

[3] Die „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ gibt weitere Informationen zu den benötigten Dokumenten.

3 Die prüfende Stelle

Eine prüfende Stelle ist eine geeignete Institution, die vom KRITIS-Betreiber beauftragt wird festzustellen, ob der KRITIS-Betreiber angemessene Vorkehrungen gemäß § 8a Absatz 1 BSIG getroffen hat.

Damit eine prüfende Stelle als geeignet angesehen werden kann, sollte sie die in diesem Kapitel beschriebenen fachlichen und organisatorischen Anforderungen erfüllen. Die prüfende Stelle stellt insbesondere das Prüfteam zusammen, das die eigentliche Prüfung vornimmt. Das Prüfteam sollte über die in Abschnitt 4.2 beschriebenen Kompetenzen verfügen.

In diesem Abschnitt werden folgende Fragen geklärt:

- Welche Aufgaben hat eine prüfende Stelle? (Abschnitt 3.1)
- Wann ist eine prüfende Stelle geeignet? (Abschnitt 3.2)
- Welche Arten von prüfenden Stellen gibt es? (Abschnitt 3.3)

3.1 Aufgaben

Aufgabe der prüfenden Stelle ist es,

- die Einhaltung der Prozesse und Verfahren zu überprüfen,
- für einheitliche und gleichwertige Prüfungsdurchführungen und Prüfergebnisse Sorge zu tragen,
- das Qualitätsmanagement sicherzustellen,
- Rahmenbedingungen für die Prüfdurchführung festzulegen (Prüfverfahren usw.),
- das Prüfteam zusammenzustellen und die Abdeckung aller Kompetenzbereiche sicherzustellen,
- ausreichend Personal zur Verfügung zu stellen, so dass das Vier-Augen-Prinzip bei der Prüfung beachtet werden kann,
- die Eignung der Prüfer zu bestätigen sowie
- die Kommunikation mit dem KRITIS-Betreiber auf der einen und dem Prüfteam auf der anderen Seite durchzuführen.

Die prüfende Stelle übernimmt die Verantwortung für die Prüfergebnisse, unterzeichnet die Prüfdokumente und sendet diese an den KRITIS-Betreiber.

3.2 Eignung

Eine prüfende Stelle ist geeignet, wenn die folgenden Kriterien erfüllt sind:

- Die prüfende Stelle muss für mindestens einen Mitarbeiter dem BSI gegenüber die zusätzliche Prüfverfahrenskompetenz für § 8a BSIG (siehe Abschnitt 4.3) nachweisen. Wenn einer dieser Mitarbeiter Mitglied des Prüfteams ist, reicht der bereits vorgelegte Nachweis aus. In diesem Fall ist jedoch ein Hinweis erforderlich, dass es sich um einen Mitarbeiter der Prüfstelle handelt.

- Die erforderlichen Prozesse der prüfenden Stelle (z. B. Informationssicherheitsmanagementsystem (ISMS), Qualitätssicherungsverfahren, Dokumentations- und Aufzeichnungsverfahren, Archivierungs- und Backupkonzept, Prüfprozess) müssen eingeführt, umgesetzt und in Konzepten dokumentiert sein.
- Die prüfende Stelle muss jede Prüfung nach einem dokumentierten Prüfprozess durchführen. Das einheitliche Verständnis von Abweichungen ist für die Bewertung der Mängel zwingend erforderlich. Wird ein Sicherheitsmangel als schwerwiegende Abweichung bewertet, sind die Ursachen zu analysieren und nachvollziehbar zu dokumentieren.
- Es muss sichergestellt sein, dass jede Prüfung unabhängig und unparteilich, neutral und weisungsfrei erfolgt.
- Die Einhaltung der ethischen Grundsätze (siehe Anhang A) muss sichergestellt sein.
- Die Art und der Umfang der Prüfungshandlungen und -ergebnisse werden einheitlich, sachlich und ordnungsgemäß dokumentiert.
- Es werden ausreichend kompetente personelle Ressourcen und geeignete Infrastrukturen zur Verfügung gestellt. Eine prüfende Stelle muss
  - mindestens über einen Leiter und einen Stellvertreter verfügen, um geplante und ungeplante Ausfälle der Leitung kompensieren zu können,
  - Prüfungsverfahren in einer angemessenen Zeit durchführen,
  - sichere Infrastruktur, Systeme, Anwendungen und eine sichere IT-Netzstruktur nachweisen können.
- Die prüfende Stelle verfügt über einen festgelegten Prozess zur Ermittlung der Kompetenz des Prüfteams und anderer an der Durchführung von Prüfungen beteiligten Personen (z. B. Fachexperten). Hierfür müssen folgende Kompetenzen im Prüfteam vorhanden sein:
  - belastbares Wissen im Bereich der Informationssicherheit,
  - Branchenkenntnisse und technisches Wissen im Bereich der Erbringung der kritischen Dienstleistungen des geprüften KRITIS-Betreibers,
  - belastbares Wissen im Bereich Managementsysteme und insbesondere Informationssicherheitsmanagementsysteme (ISMS),
  - detaillierte Kenntnisse der Anforderungen an Prüfungen nach § 8a Absatz 3 BSIG.

Damit die Qualität der Prüfergebnisse vergleichbar ist, sollten die Prüfungen im Rahmen der Nachweise auf der Grundlage gängiger Normen und Standards durchgeführt werden. Die Einhaltung der Anforderungen an die prüfende Stelle und die Umsetzung der Prozesse sollte durch eine unabhängige Instanz kontrolliert werden.

In vielen Fällen unterliegen die prüfenden Stellen einem Akkreditierungsregime (siehe Abschnitt 3.3).

Sollte eine prüfende Stelle nicht unter die Auflistung in Abschnitt 3.2 fallen, ist ein individueller Nachweis der Eignung durch eine Selbsterklärung für prüfende Stellen gegenüber dem BSI erforderlich (siehe Abschnitt 3.3.5).

3.3 Geeignete prüfende Stellen

Die prüfende Stelle kann ihre Eignung z. B. nachweisen durch:

- eine Akkreditierung bei der DAkkS zur ISO/IEC 27001-Zertifizierung (akkreditierte Zertifizierungsstellen der DAkkS) (Abschnitt 3.3.1,
- eine Zertifizierung als IT-Sicherheitsdienstleister oder eine Anerkennung als Prüfstelle beim BSI (Abschnitt 3.3.2),
- ein externes Quality Assessment gemäß „Internationalen Standards für die berufliche Praxis der internen Revision“ (IIA)[4] bzw. DIIR-Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ (DIIR)[5] (Abschnitt 3.3.3),
- eine Zulassung als Wirtschaftsprüfungsinstitution beim IDW (Abschnitt 3.3.4) oder
- einen individuellen Nachweis der Eignung durch Selbsterklärung gegenüber dem BSI (Abschnitt 3.3.5).

Zusätzlich ist nachzuweisen, dass die Personen des Prüfteams insgesamt über alle erforderlichen Kompetenzen verfügen (siehe Kapitel 4).

In den folgenden Unterabschnitten werden die Qualifikationen der prüfenden Stellen genauer beschrieben.

3.3.1 Akkreditierte Zertifizierungsstellen der DAkkS

Im Rahmen eines ISO/IEC 27001-Zertifizierungsverfahrens übernimmt die Deutsche Akkreditierungsstelle GmbH (DAkkS) als die nationale Akkreditierungsstelle der Bundesrepublik Deutschland die Funktion der „unabhängigen Instanz“. Eine qualifizierte Zertifizierungsstelle ist für den Bereich ISO/IEC 27001 akkreditiert und muss die Umsetzung und Einhaltung der ISO/IEC 17021-1 und ISO/IEC 27006 gegenüber der DAkkS nachweisen. Damit erfüllen diese Stellen die notwendigen Qualitätsanforderungen.

Eine Übersicht in Deutschland akkreditierter Stellen zur ISMS-Zertifizierung kann auf der Website der DAkkS abgerufen werden.

3.3.2 Zertifizierte IT-Sicherheitsdienstleister oder anerkannte Prüfstellen des BSI

Das BSI bietet eine Zertifizierung von IT-Sicherheitsdienstleistern für verschiedene Geltungsbereiche an. Unabhängig vom jeweiligen Geltungsbereich ist das Ziel der Anerkennung durch das BSI die Sicherstellung der Fachkompetenz, Qualität und Vergleichbarkeit der Konzepte, Vorgehensweisen und Arbeitsergebnisse der Prüfstellen.

---

[4] https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1__20180110.pdf

[5] https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr__3.pdf

Voraussetzung für eine Zertifizierung als IT-Sicherheitsdienstleister ist die Erfüllung der Anforderungen der DIN EN ISO/IEC 17025 in der jeweils gültigen Fassung. Das Verfahren der Zertifizierung bzw. Anerkennung von Prüfstellen ist in einer veröffentlichten Verfahrensbeschreibung festgelegt, die durch einen Begutachtungskatalog ergänzt ist[6].

Diese Stellen erfüllen damit geeignete Qualitätsansprüche.

3.3.3 Interne Revision

Interne Revisionen können ein angemessenes und wirksames Revisionssystem und die Einhaltung der internationalen Standards für die berufliche Praxis der Internen Revision des Institute of Internal Auditors (IIA) durch ein Quality Assessment (QA) nachweisen. Die unabhängige Instanz ist hier die Stelle, die die QA-Prüfungen durchführt. Diesem Verfahren liegen der DIIR[7]-Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ und die IIA-Standards 1300ff zugrunde[8].

Für die Einschätzung der Angemessenheit und Wirksamkeit bei der Prüfung des aktuellen Stands der Technik muss eine Interne Revision bestimmte Qualitätskriterien einhalten. In einem Quality Assessment wird die Einhaltung von konkreten Kriterien überprüft. Die folgenden sechs Mindestanforderungen müssen erfüllt sein:

- Es ist eine offizielle schriftliche, angemessene Regelung für die Durchführung der Revision (Geschäftsordnung, Revisionsrichtlinie o. Ä.) vorhanden.
- Neutralität, Unabhängigkeit von anderen Funktionen sowie uneingeschränktes Informationsrecht der Internen Revision sind sichergestellt und gegenüber dem BSI darzulegen.
- Die Interne Revision verfügt über eine angemessene quantitative und qualitative Personalausstattung.
- Der Prüfungsplan der Internen Revision wird auf Grundlage eines standardisierten und risikoorientierten Planungsprozesses erstellt.
- Art und Umfang der Prüfungshandlungen und -ergebnisse werden einheitlich, sachlich und ordnungsgemäß dokumentiert.
- Die Umsetzung der im Bericht dokumentierten Maßnahmen wird von der Internen Revision durch einen effektiven Follow-up-Prozess überwacht.

Durch die Einhaltung der internationalen Standards ist insbesondere die Unabhängigkeit der Internen Revision sichergestellt. Daneben ist auch der Ethikkodex des IIA für Interne Revisoren verpflichtend. Hier werden die Anforderungen an Rechtschaffenheit, Objektivität, Vertraulichkeit und Fachkompetenz beschrieben[9].

---

6 https://www.bsi.bund.de/dok/10023142

7 DIIR: Deutsches Institut für Interne Revision

8 http://www.diir.de/zertifizierung/quality-assessment/

9 https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1__20180110.pdf

3.3.4 Wirtschaftsprüfungsinstitutionen

Aufgrund der hohen Verantwortung, die eine Wirtschaftsprüfungsinstitution übernimmt, erfüllt sie besondere Berufspflichten, die in der Wirtschaftsprüferordnung (WPO)[10] zusammengefasst sind.

Dies sind u. a. Unabhängigkeit, Verschwiegenheit und berufswürdiges Verhalten.

3.3.5 Selbsterklärung gegenüber dem BSI

Wenn eine prüfende Stelle nicht einem der zuvor beschriebenen anerkannten Akkreditierungsregimes unterliegt, kann sie trotzdem ihre Eignung nachweisen, sofern sie die Einhaltung der genannten Eignungskriterien (siehe Abschnitt 3.3) erfüllt.

Dies kann in einer Selbsterklärung festgehalten und dem BSI dargelegt werden.

Diese Selbsterklärung stellt eine verbindliche Aussage über die Einhaltung der notwendigen Eignungskriterien dar und bedarf daher der Schriftform und der Unterzeichnung durch einen Zeichnungsberechtigten der prüfenden Stelle.

Die notwendigen Angaben können in dem vom BSI bereitgestellten Formular[11] gemacht werden. Sie wird zusammen mit den anderen Nachweisunterlagen an das BSI übermittelt.

Die Selbsterklärung muss sich auf den konkreten Prüfgegenstand beziehen. Eine pauschale Selbsterklärung einer prüfenden Stelle ist nicht ausreichend.

4 Das Prüfteam

Die prüfende Stelle stellt ein Prüfteam zusammen, das mit der konkreten Prüfung bei einem KRITIS-Betreiber beauftragt wird.

Das Prüfteam muss alle erforderlichen Anforderungen zur Erbringung geeigneter Nachweise erfüllen und über die in Abschnitt 4.2 erforderliche Kompetenz verfügen. Grundsätzlich sollte ein Prüfteam aus mindestens zwei qualifizierten Mitarbeitern bestehen, um ein Vier-Augen-Prinzip zu ermöglichen.

Je nach Prüfumfang kann das Prüfteam um weitere Prüfer bzw. Fachexperten (z. B. zur Beisteuerung branchenspezifischer oder anlagenspezifischer Fachkenntnis) erweitert werden. Alle Mitglieder des Prüfteams müssen die im Anhang genannten „ethischen Grundsätze“ befolgen.

4.1 Aufgaben

Ein Prüfteam der prüfenden Stelle führt die Prüfung gemäß einem festgelegten Prüfverfahren durch und erstellt einen Prüfbericht, der die Prüfergebnisse dokumentiert.

---

[10] http://www.gesetze-im-internet.de/wipro/index.html

[11] https://www.bsi.bund.de/dok/13491490

Dabei kann diese Prüfung

- als Einzelprüfung einer geeigneten (internen oder externen) prüfenden Stelle
- oder als Zusatzprüfung z. B. im Rahmen
  - eines internen ISMS-Audits durch interne, unabhängige IS-Revisoren (Erstparteien- oder First-Party-Audit),
  - einer Wirtschaftsprüfung durch qualifizierte Wirtschaftsprüfer oder
  - einer ISO/IEC 27001-Zertifizierung, d. h. eines Zertifzierungs-, Überwachungs- oder Re-Zertifizierungsaudits (nativ oder auf Basis von IT-Grundschutz) durch Auditoren (Drittparteien- oder Third-Party-Audit)

durchgeführt werden.

4.2 Kompetenz und Eignung

Damit Prüfer im Auftrag der KRITIS-Betreiber geeignete Prüfungen und damit geeignete Nachweise zur Erfüllung der gesetzlichen Anforderungen erbringen können, müssen sie über Kompetenzen in den folgenden Bereichen verfügen:

- Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG
- Auditkompetenz
- IT-Sicherheitskompetenz bzw. Informationssicherheits-Kompetenz
- Branchenkompetenz

Ein Prüfer muss nicht alleine über alle diese Kompetenzen verfügen, die geeignete Zusammenstellung eines Prüfteams mit der Abdeckung aller Kompetenzbereiche ist ausreichend. Sofern die erforderlichen Kompetenzen nicht bei den Prüfern selbst vorliegen, kann in das Prüfteam auch ein Fachexperte mit den entsprechenden Kenntnissen aufgenommen werden. Insbesondere bezüglich der Branchenkompetenz kann es hilfreich sein, für unterschiedliche Bereiche auch unterschiedliche Fachexperten hinzu zu ziehen (z. B. als Mitglied des Prüfteams oder im Rahmen von Interviews).

Ein Prüfer muss weisungsfrei und unvoreingenommen die Prüfung durchführen. Er muss die Prüfungsergebnisse nachvollziehbar dokumentieren können. Jedes Prüfteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei Prüfern bestehen („Vier-Augen-Prinzip“). Alle Mitglieder des Teams dürfen aus Gründen der Unabhängigkeit und Neutralität vorher nicht unmittelbar im geprüften Bereich beratend oder auch ausführend, z. B. bei der Erstellung von Konzepten oder der Konfiguration von IT-Systemen tätig gewesen sein. Der Leiter des Prüfteams darf nicht mehr als zwei aufeinanderfolgende Prüfungen bei derselben Anlage durchführen.

Mit dem Betrieb oder der IT-Sicherheit der zu prüfenden Anlage betraute Mitarbeiter des KRITIS-Betreibers oder dessen Dienstleister kommen nicht als Mitglieder des Prüfteams in Betracht. Fachwissen aus diesem Personenkreis kann im Rahmen eines Interviews durch das Prüfteam erhoben werden. Eine Mitwirkung als Bestandteil des Prüfteams und damit an der Bewertung der im Rahmen der Prüfung erhobenen Sachverhalte ist jedoch auszuschließen.

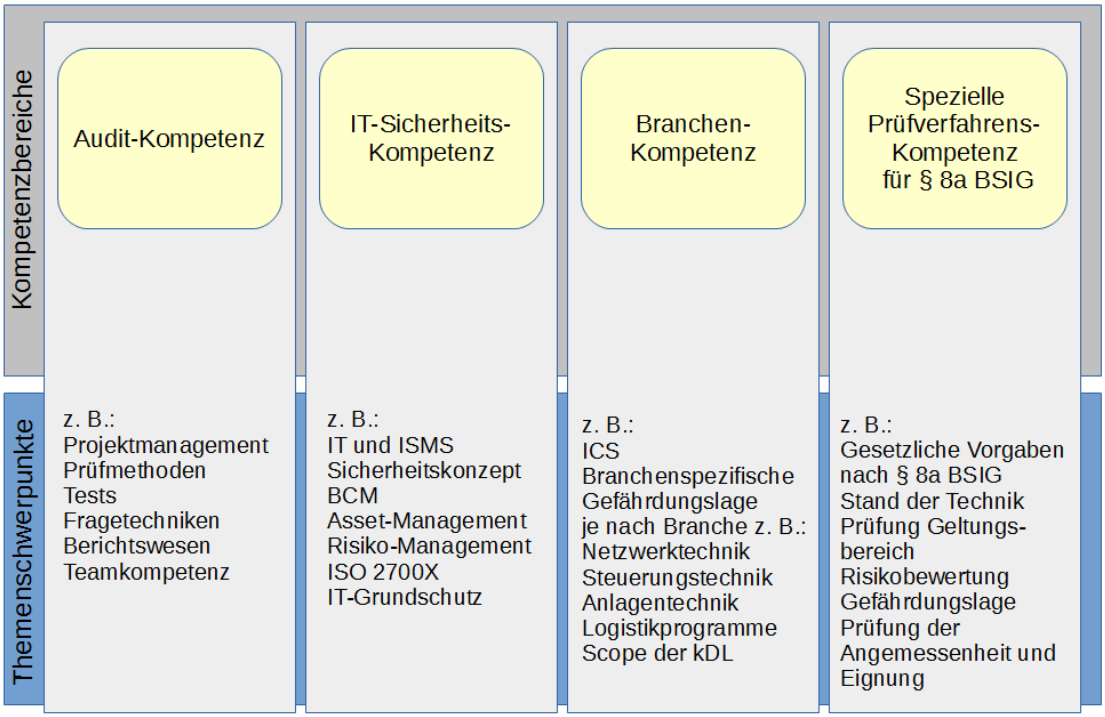

Abbildung 2: Themen der Kompetenzbereiche, Quelle: BSI

Abbildung 2 zeigt, welche Themenschwerpunkte in den jeweiligen Kompetenzbereichen vorhanden sein sollten.

Anmerkung: Die Gesamtkompetenz kann auf mehrere Prüfer verteilt sein. Wichtig ist, dass an jedem Prüfabschnitt auch Prüfer mit der hierfür ausreichenden Kompetenz beteiligt sind.

4.3 Erwerb der zusätzlichen Prüfverfahrenskompetenz

Unter der zusätzlichen Prüfverfahrenskompetenz für § 8a BSIG sind Kenntnisse über die Besonderheiten einer KRITIS-spezifischen Prüfung im Bereich § 8a BSIG zu verstehen. Insbesondere betrifft dies die Bewertung des Geltungsbereichs, den Schutz der Versorgungssicherheit, Einschränkungen in der Risikobehandlung, die Berücksichtigung des „Stands der Technik“ und weitere KRITIS-spezifische Besonderheiten.

Diese Kompetenz kann in einer separaten Schulung erworben werden, in der die besonderen Aspekte und Anforderungen einer Prüfung nach § 8a BSIG ausführlich behandelt werden. Bei dieser Fortbildung handelt es sich um keine Zulassung, Anerkennung oder Zertifizierung eines Prüfers, sondern um eine Zusatzqualifikation.

Der Erwerb der zusätzlichen Prüfverfahrenskompetenz kann dem BSI entweder durch Vorlage einer Teilnahmebescheinigung an einer angemessenen Schulung oder durch das vom BSI bereitgestellte Formular „Selbsterklärung der prüfenden Person zum Nachweis der zusätzlichen Prüfverfahrenskompetenz“[12] nachgewiesen werden.

[12] https://www.bsi.bund.de/dok/13491522

5 Durchführung der Prüfung

Das folgende Kapitel beschreibt, was bei der Durchführung der Prüfung beachtet werden sollte. Hieran sind KRITIS-Betreiber, prüfende Stelle und Prüfteam beteiligt. Es werden Kriterien einer geeigneten Prüfung aufgezählt, für die im Einzelnen aber auch gleichwertige Alternativen entsprechend der Fachkompetenz der prüfenden Stelle möglich sind. Es wird auf folgende Fragen eingegangen:

- Welche Prüfgrundlage liegt zugrunde? (Abschnitt 5.1)
- Welche Prüfthemen sollen geprüft werden? (Abschnitt 5.2)
- Welche Prüfmethoden können verwendet werden? (Abschnitt 5.3)
- Welcher Prüfaufwand ist zu erwarten? (Abschnitt 5.4)
- Wie können Prüfplan und Stichproben aufgestellt werden? (Abschnitt 5.5)
- Welche Inhalte sollte ein Prüfbericht bzw. die Prüfdokumentation haben? (Abschnitt 5.6)
- Welche Mängel müssen erfasst werden und welche Mängelkategorien sollen verwendet werden? (Abschnitt 5.6)

5.1 Prüfgrundlage

Grundsätzlich ist eine Vielzahl an Prüfgrundlagen möglich, sofern diese geeignet sind, die Erfüllung von § 8a Absatz 1 BSIG nachzuweisen.

5.1.1 Prüfung bei Anwendung eines B3S nach § 8a Absatz 2 BSIG

Wenn ein branchenspezifischer Sicherheitsstandard (B3S)[13] mit aktueller Eignungsfeststellung des BSI für den jeweiligen Geltungsbereich vorliegt und dieser vom KRITIS-Betreiber bei der Umsetzung von Maßnahmen angewendet wurde, kann dieser als Referenzdokument zur Erstellung des Prüfplans herangezogen werden. Ein B3S beschreibt sowohl den Geltungsbereich als auch die Mindestanforderungen der umzusetzenden Maßnahmen.

Der KRITIS-Betreiber muss einen geeigneten Geltungs¬bereich für den Prüfgegen¬stand festlegen. Der Prüfer muss zu Beginn der Prüfung überprüfen, ob der Geltungsbereich richtig gewählt wurde. Dafür orientiert er sich an den individuellen Gegebenheiten beim KRITIS-Betreiber vor Ort. Wenn seine Einschätzung stark von der des Betreibers abweicht, muss er mit dem Betreiber eine Vereinbarung über den neuen Prüfgegenstand treffen.

Der Geltungsbereich eines B3S orientiert sich aber typischerweise an den Gegebenheiten der gesamten Branche. Daher ist zu prüfen, ob der Geltungsbereich des B3S den der Prüfung vollständig abdeckt, ggf. sind weitere zusätzliche individuelle Maßnahmen erforderlich. Die Vorgaben des B3S sind sinngemäß auf die zu prüfenden Anlagen abzubilden.

[13] https://www.bsi.bund.de/Stand-der-Technik

5.1.2 Prüfung ohne Anwendung eines B3S

Liegt kein B3S vor oder soll die Prüfung unabhängig von einem B3S erfolgen, muss sichergestellt werden, dass die Anforderungen nach § 8a Absatz 1 BSIG auf andere Weise erfüllt sind. Die Prüfung muss geeignet sein, dies nachzuweisen. Die prüfende Stelle muss vor der Durchführung der Prüfung ein geeignetes Prüfverfahren definieren und es nachvollziehbar dokumentieren. Dieses Prüfverfahren dient dann als Prüfgrundlage.

Anhaltspunkte für ein geeignetes Prüfverfahren können sein:

- die Orientierungshilfe zu branchenspezifischen Sicherheitsstandards (B3S) nach § 8a Absatz 2 BSIG,
- der Katalog zur Konkretisierung der Anforderungen des § 8a Absatz 1 BSIG, [14]
- andere B3S gemäß § 8a Absatz 2 BSIG, deren Eignung vom BSI festgestellt wurde (hierbei ist ggf. der Geltungsbereich des B3S an den zu prüfenden Geltungsbereich anzupassen.),
- einschlägige Standards (z. B. Zertifizierungsschemata für ISO 27001 (nativ oder auf Basis von IT-Grundschutz), ISO/IEC 17021-1, ISO/IEC 27006).

5.1.3 Berücksichtigung vorhandener Prüfungen

Grundsätzlich können vorhandene, geeignete Prüfungen bei der Erbringung des Nachweises berücksichtigt werden, d. h. es besteht die Möglichkeit, für § 8a Absatz 3 BSIG erforderliche Prüfaspekte im Rahmen anderer Prüfungen abzudecken. DamitPrüfungen geeignet sind, müssen sie zum Zeitpunkt der Vorlage gültig sein, d. h. der Prüfgegenstand muss in dieser Form noch Bestand haben. Außerdem müssen die Prüfungen aktuell sein, d. h. sie dürfen zum Zeitpunkt der Einreichung beim BSI nicht älter als ein Jahr sein. Ältere Prüfergebnisse können allenfalls in Form einer Dokumentenanalyse (siehe Abschnitt 5.3) in die Prüfung einfließen, ersetzen aber nicht die aktuelle Prüfung (z. B. aufgrund geänderter Gefahrenlage und Wirksamkeit von Maßnahmen). Noch fehlende Aspekte müssen in den eigenen Prüfplan aufgenommen werden.

Insbesondere ist darauf zu achten, dass der Geltungsbereich die zu prüfende Kritische Infrastruktur vollständig abdeckt und für die Kritische Infrastruktur relevante zusätzliche Rahmenbedingungen berücksichtigt (z. B. Umgang mit Dienstleistern, Einschränkungen in der Risikoakzeptanz). Einen Anhaltspunkt für solche Rahmenbedingungen bietet die „Orientierungshilfe zu branchenspezifischen Sicherheitsstandards“[15].

Die Verantwortung für die vollständige Abdeckung des Geltungsbereichs liegt beim KRITIS-Betreiber. Die Vollständigkeit wird durch die prüfende Stelle ausdrücklich geprüft.

[14] https://www.bsi.bund.de/dok/13824642

[15] https://www.bsi.bund.de/dok/10338482

5.1.3.1 Verwendung von ISO 27001-Zertifikaten für Nachweise

Ein gültiges ISO 27001-Zertifikat ist als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwendbar, sofern einige Rahmenbedingungen eingehalten werden. Dies gilt sowohl für native ISO 27001-Zertifikate als auch für ISO 27001-Zertifikate auf Basis von IT-Grundschutz.

Bei einer ISO 27001-Zertifizierung ist nicht automatisch der gesamte, für den Nachweis nach § 8a BSIG relevante Geltungsbereich erfasst. Der Geltungsbereich des Nachweises muss die Kritische Infrastruktur bzw. die kritische Dienstleistung (kDL) vollständig umfassen (Prozess-Sicht).

Zudem ist der Informationssicherheitsprozess bzgl. der kritischen Dienstleistung mit der „KRITIS-Brille“ zu betrachten. Die Vermeidung von Versorgungsengpässen in der kritischen Dienstleistung ist im Kontext von KRITIS von sehr hoher Bedeutung. Daher muss die kritische Dienstleistung mit dem Fokus der Vermeidung von Versorgungsengpässen der Bevölkerung betrachtet werden.

Im Folgenden wird allgemein auf die Rahmenbedingungen für die Verwendung von ISO 27001-Zertifikaten für Nachweise nach § 8a Absatz 3 BSIG eingegangen:

1. Abgrenzung Geltungsbereich

Der Geltungsbereich muss die betriebenen Anlagen nach BSI-Kritisverordnung umfassen. Die Schnittstellen sind geeignet festzulegen.

2. Erweiterter Geltungsbereich

Der Geltungsbereich muss auf ausgelagerte Bereiche erweitert und eine umfassende Sicherheitsbetrachtung aus KRITIS-Sicht durchgeführt werden. Diese kann an ISO 27001 oder andere vergleichbare Vorgehensweisen angelehnt sein.

Bei einer vorhandenen ISO 27001 Zertifizierung kann diese für einen Nachweis gemäß § 8a Absatz 3 BSIG auf die bisher ungeprüften Teile des Geltungsbereichs ausgeweitet werden. Somit kann eine bzgl. der KRITIS-Schutzziele ergänzende Prüfung des bereits geprüften Bereichs erfolgen. So kann der Nachweis auf Basis des Audits einer Erstzertifizierung, eines Überwachungs- oder Re-Zertifizierungsaudits mit geprüft und Synergieeffekte genutzt werden. Die Prüfergebnisse bilden einen Teil des Nachweises gemäß § 8a Absatz 3 BSIG.

3. Berücksichtigung der KRITIS-Schutzziele

Das BSI-Gesetz fordert, für die betriebsrelevanten Teile der jeweiligen Anlagen dem Schutzbedarf entsprechende angemessene Maßnahmen zu ergreifen.

Das Aufrechterhalten der Versorgungssicherheit der Bevölkerung muss das zentrale Anliegen bei der Informationssicherheitsrisikobehandlung sein. Die Anforderungen, die dabei an die Dienstleistungserbringung gestellt werden, werden auch als KRITIS-Schutzziele bezeichnet. Die KRITIS-Schutzziele der betriebsrelevanten Teile sind geeignet festzulegen. Die KRITIS-Schutzziele (z. B. die Verfügbarkeit der kritischen Dienstleistung) sind in die eigene Risikobetrachtung aufzunehmen und durchgängig in allen Prozessen und Maßnahmenumsetzungen zusätzlich zu betrachten („KRITIS-Brille“).

4. KRITIS-Schutzbedarf

Im Rahmen des Risikomanagements sind die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität in Bezug auf die Aufrechterhaltung der kritischen Dienstleistung zu bewerten.

Eine rein betriebswirtschaftliche Risikobetrachtung ist in der Regel nicht ausreichend (siehe „Umgang mit Risiken"). Als Anhaltspunkt für das Ausmaß eines Risikos für die Allgemeinheit sollten die Auswirkungen auf die Funktionsfähigkeit der Kritischen Infrastruktur und der kritischen Dienstleitung berücksichtigt werden. Bei der Risikobehandlung ist zu berücksichtigen, dass der Aufwand zur Umsetzung der Maßnahmen in angemessenem Verhältnis zum Risikoausmaß für die Bevölkerung steht.

Hinweis: § 8a Absatz 1 BSIG verlangt „[...] Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit [...]". Ein Risikomanagement unter Bewertung von Vertraulichkeit, Integrität und Verfügbarkeit, wie in ISO 27001 oder IT-Grundschutz des BSI üblich ist möglich, solange sichergestellt ist, dass Authentizität bei der Risikobewertung und Maßnahmenauswahl berücksichtigt wird.

5. Umgang mit Risiken

Eine rein betriebswirtschaftliche Betrachtung der Risiken und des Schutzbedarfs ist in der Regel nicht ausreichend. Es muss insbesondere das Ausmaß eines Risikos für die Allgemeinheit, d. h. die Auswirkungen auf die Funktionsfähigkeit der Kritischen Infrastruktur und der kritischen Dienstleitung, berücksichtigt werden. Bei der Maßnahmenauswahl muss auf Angemessenheit geachtet werden, also die möglichen Folgen eines Ausfalls oder einer Beeinträchtigung für die Versorgung der Allgemeinheit im Verhältnis zum Aufwand der Sicherheitsvorkehrungen betrachtet werden.

- Risikoakzeptanz

  Risiken im Geltungsbereich dürfen gemäß § 8a Absatz 1 BSIG nicht akzeptiert werden, sofern Sicherheitsvorkehrungen nach Stand der Technik möglich und angemessen sind. Erst für das dann noch verbleibende Restrisiko ist eine Risikoakzeptanz möglich.

- Versicherbarkeit der Risiken

  Ein Transfer der Risiken, z. B. durch Versicherungen, ist kein Ersatz für die Sicherheitsvorkehrungen gemäß § 8a Absatz 1 BSIG. Auch bei Versicherung oder anderem Risikotransfer sind angemessene Sicherheitsvorkehrungen nach Stand der Technik vorzunehmen. Es steht dem KRITIS-Betreiber aber frei, sich zusätzlich zu versichern.

6. Maßnahmenumsetzung

Grundsätzlich sind alle für die Aufrechterhaltung der kritischen Dienstleistung erforderlichen Maßnahmen im Rahmen der Risikobehandlung umzusetzen. Alle lediglich in Planung befindlichen Maßnahmen, beispielsweise im kontinuierlichen Verbesserungsprozess (KVP), im Umsetzungsplan oder im Risikobehandlungsplan, müssen in die Auflistung der Sicherheitsmängel gemäß § 8a Absatz 3 BSIG aufgenommen werden. Zur Bewertung dieser Mängel sollten auch erklärende Dokumente wie die Mängelbewertung, KVP-Dokumentation und der Umsetzungsplan eingereicht werden.

5.1.3.2 Nutzung eines bestehenden C5-Testates

Grundsätzlich stellt der Anforderungskatalog Cloud Computing (englischer Titel: Cloud Computing Compliance Controls Catalogue, kurz „C5“) einen Mindeststandard der IT-Sicherheit für Cloud Service Provider (CSP) dar. CSP werden innerhalb der kritischen Dienstleistung "Datenspeicherung und Verarbeitung" bei Überschreitung des entsprechenden Schwellenwertes der BSI-Kritisverordnung als Kritische Infrastruktur klassifiziert. Ein bestandenes C5-Testat ist als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwertbar, sofern einige Rahmenbedingungen bei der Testierung eingehalten werden:

1. Geltungsbereich

Der Geltungsbereich der Maßnahmen gemäß § 8a Absatz 1 BSIG sowie der Prüfgegenstand des Nachweises gemäß § 8a Absatz 3 BSIG müssen jeweils die gesamte betriebene Anlage nach BSI-Kritisverordnung (z. B. Serverfarm) umfassen. Damit bei Cloud Service Providern (CSP) für ihre Anlage der Nachweis über den C5 als Teil des Nachweises gemäß § 8a Absatz 3 BSIG ausreicht, muss für alle betriebsrelevanten informationstechnischen Dienste, Systeme, Komponenten oder Prozesse, die nicht über das C5-Testat geprüft werden, ebenfalls ein Nachweis der angemessenen Absicherung unter Berücksichtigung des Stands der Technik erbracht werden. Dies kann über eine Ausweitung des C5-Audits auf die bisher ungeprüften Teile der Anlage des CSP oder über eine zusätzliche Prüfung erfolgen.

2. Berücksichtigung der KRITIS-Schutzziele und KRITIS-Schutzbedarf

Das BSI-Gesetz fordert, für die betriebsrelevanten Teile der jeweiligen Anlagenkategorien dem Schutzbedarf (betrachtet für Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) angemessene Maßnahmen zu ergreifen. Die Vermeidung von Versorgungsengpässen in der kritischen Dienstleistung ist im Kontext von KRITIS von sehr hoher Bedeutung. Daher ist die geeignete Festlegung des Schutzbedarfs der betriebsrelevanten Teile der Anlagenkategorie zu prüfen (vgl. § 8a Absatz 1 BSIG und § 8a Absatz 3 BSIG) und es sollte neben den Anforderungen des C5 darauf geachtet werden, dass die für die kritische Dienstleistung betriebsrelevanten Systeme einer resilienten Architektur unterliegen.

3. Umgang mit Risiken

Das zentrale Anliegen bei der Risikobehandlung muss das Bewahren der Versorgungssicherheit der Gesellschaft bzw. die Einhaltung der mit den Kunden getroffenen Service Level Agreements (SLA) sein. Deshalb sind im Rahmen des Risikomanagements die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität in Bezug auf die Aufrechterhaltung der kritischen Dienstleistung zu bewerten – eine rein betriebswirtschaftliche Betrachtung ist in der Regel nicht ausreichend. Als Anhaltspunkt für das Ausmaß eines Risikos für die Gesellschaft können die Folgen aus der Beeinträchtigung der Funktionsfähigkeit einer betriebenen Kritischen Infrastruktur herangezogen werden.

Außerdem dürfen Risiken im Geltungsbereich gemäß § 8a Absatz 1 BSIG nicht akzeptiert werden, sofern Sicherheitsvorkehrungen nach § 8a Absatz 1 BSIG möglich und angemessen sind. Auch wenn Risiken nicht vollumfänglich beseitigt werden können, müssen die Risiken soweit wie möglich angemessen reduziert werden, bevor eine Akzeptanz zulässig ist.

Weiterhin ersetzt eine Versicherung der Risiken nicht die geforderten Sicherheitsvorkehrungen. Eine angemessene Absicherung nach § 8a Absatz 1 BSIG bleibt erforderlich. Auch wenn Risiken nicht vollumfänglich beseitigt werden können, müssen die Risiken soweit wie möglich angemessen reduziert werden, bevor eine Versicherung zur Risikobehandlung zulässig ist. Der zusätzliche Abschluss von Versicherungen ist davon unbenommen.

Zudem sind die Vorgaben des C5 hinsichtlich der Umsetzung der Maßnahmen einzuhalten. Sind über die Anforderungen des C5 bzgl. der angemessenen Absicherung nach § 8a Absatz 1 BSIG für die Risikobehandlung weitere Maßnahmen zu ergreifen, so müssen diese für den Nachweis nach § 8a Absatz 3 BSIG umgesetzt sein oder sich zum Zeitpunkt des Nachweises in einem erwarteten Fortschrittsstadium befinden. Diese Maßnahmen und Mängel müssen in die Auflistung der Sicherheitsmängel aufgenommen werden.

4. Nachweiserbringung

Nachweise gemäß § 8a Absatz 3 BSIG müssen mindestens alle zwei Jahre erbracht werden. Dabei müssen die zu Grunde gelegten C5-Testate zum Zeitpunkt der Vorlage eines Nachweises aktuell sein, also nicht älter als ein Jahr. Ältere Nachweise können allenfalls in Form einer Dokumentenanalyse in den Nachweis einbezogen werden. Diese Nachweispflicht lässt sich problemlos in die Testierung des C5 integrieren.

Als geeigneter Nachweis ist neben dem aktuellen Testat zusätzlich eine Liste aufgedeckter Sicherheitsmängel einzureichen, siehe Abschnitt 5.7.

5.2 Prüfthemen und Prüfung des Geltungsbereichs

Die Prüfthemen sind in einem B3S im Allgemeinen konkret beschrieben, insbesondere können dort branchenspezifische Anforderungen und/oder Maßnahmen aufgeführt sein, deren Umsetzung sichergestellt werden muss.

Liegt kein B3S vor oder wird zur Prüfung kein B3S verwendet, liefert Anhang E die Prüfthemen, die mindestens zu berücksichtigen sind.

Sofern sich der Nachweis über mehrere Anlagen oder Standorte erstreckt, ist kenntlich zu machen, auf welche Anlagen oder Standorte sich die jeweiligen Prüfthemen und Aussagen beziehen.

Insbesondere die Überprüfung, ob der Geltungsbereich richtig gewählt wurde, ist für die Eignung des Nachweises sehr wichtig. Der Prüfer muss sich hierzu die Prüffrage stellen, ob die Wahl des Geltungsbereichs korrekt ist und auch vollständig die informationstechnischen Systeme, Komponenten und Prozesse umfasst, die zu der zu überprüfenden Anlage der Kritischen Infrastruktur gehören, sowie diejenigen, die auf die Kritische Infrastruktur Einfluss haben.

Dabei muss der Prüfer den Geltungsbereich unter den Prüfaspekten

- der Funktionsfähigkeit der kritischen Dienstleistung,
- der Eignung und Erforderlichkeit und
- der Vollständigkeit

bewerten und überprüfen.

Die Beschreibung der Anlage und der zugehörigen Teile der kritischen Dienstleistung muss nachvollziehbar sein und in ihren Merkmalen mit der registrierten Anlagenkategorie übereinstimmen.

Der Geltungsbereich muss grafisch dargestellt und, soweit zum Verständnis erforderlich, schriftlich beschrieben werden. Die grafische Darstellung soll eine schnell zu erfassende Übersicht darstellen, während die textuelle Beschreibung diese Übersicht mit der nötigen Tiefe an Informationen ergänzt. Sollten Abhängigkeiten oder Schnittstellen zu außerhalb des Geltungsbereiches liegenden Bereichen oder Systemen bestehen, müssen diese in der grafischen Übersicht erkennbar sein und nachvollziehbar beschrieben werden. Gleiches gilt für Teile der kritischen Dienstleistung, die durch Dritte im Auftrag des Betreibers erbracht werden.

Ist die Darstellung des Geltungsbereiches in eine Darstellung eines größeren Bereiches oder Gesamtnetzes eingebettet, müssen die Grenzen des Geltungsbereiches klar kenntlich gemacht sein. Eine Liste mit den hier dargestellten Anforderungen an die Darstellung und Beschreibung des Geltungsbereiches findet sich in Anhang C mit den entsprechenden Punkten ab G01.

Zentrales Element der grafischen Darstellung ist der Netzstrukturplan. In seiner Funktion als Übersicht muss er alle Bereiche der Kritischen Infrastruktur abbilden, sowie Kommunikationsschnittstellen und Abhängigkeiten nach außen aufzeigen. Aus ihm muss hervorgehen, inwiefern einzelne Elemente für die kritische Dienstleistung relevant sind. Die Wahl eines passenden Abstraktionsniveaus ist hierfür unerlässlich. Insbesondere erfasst der Netzstrukturplan alle Systeme, Komponenten und gegebenenfalls Applikationen, die maßgeblich für die Funktionsfähigkeit der kritischen Dienstleistung sind. Zugehörige Prozesse können im Netzstrukturplan erfasst oder separat dargestellt werden. In jedem Fall muss aber eine Zuordnung zwischen Prozessen und zugehörigen notwendigen IT-Systemen, Komponenten und Applikationen möglich sein. Hier ist zudem wichtig, dass die Interaktion der wesentlichen Komponenten miteinander und mit Dritten deutlich wird.

Ähnliche Objekte sollten sinnvoll zu Gruppen zusammengefasst werden, damit der Netzstrukturplan übersichtlich bleibt.

Objekte können dann ein und derselben Gruppe zugeordnet werden, wenn die Objekte alle

- vom gleichen Typ sind,
- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen und
- den gleichen Schutzbedarf aufweisen.

Falls die Systeme, Komponenten oder sonstige Bereiche der Kritischen Infrastruktur auf mehrere Standorte verteilt sind, muss der Geltungsbereich diese Aufteilung widerspiegeln und die Standorte konkret benennen. Ebenso muss er die Anbindungen zwischen den Standorten darstellen.

Ausgelagerte Teile der kritischen Dienstleistung müssen im Geltungsbereich erkennbar sein, ebenso wie die verwendeten Kommunikationsschnittstellen. Zu ihnen zählen auch Wartungsschnittstellen, sofern sie dauerhaft freigeschaltet sind.

Das bedeutet, dass im Netzstrukturplan zumindest die folgenden Schnittstellen dargestellt werden müssen:

- Kommunikationsschnittstellen zu externen Netzen
- Kommunikationsschnittstellen zu Netzen anderer Standorte
- Wartungsschnittstellen, so sie dauerhaft freigeschaltet sind
- Schnittstellen zu ausgelagerten Teilen der Dienstleistung

Für den Fall, dass Elemente des Netzstrukturplans zur Verbesserung der Übersichtlichkeit durch Symbole dargestellt werden, müssen die verwendeten Elemente in einer Legende erläutert werden.

Auch für die Anforderungen an die Darstellung des Geltungsbereiches durch einen Netzstrukturplan kann für eine bessere Übersicht auf eine Listenform zurückgegriffen werden. Eine Liste mit Anforderungen an die Darstellung und Beschreibung des Netzstrukturplan findet sich in Anhang C mit den zugehörigen Punkten ab N01.

Ausführliche Erläuterungen und Beispiele von grafischen Geltungsbereichen sind auf der BSI-Website veröffentlicht.[16]

Die prüfende Stelle prüft die Eignung des Geltungsbereiches im Sinne von § 8a Absatz 3 BSIG und stellt das Ergebnis im Prüfbericht dar.

Anmerkung: Grundsätzlich ist es sinnvoll, dass die prüfende Stelle gemeinsam mit dem KRITIS-Betreiber bereits vor Beauftragung den Geltungsbereich der Prüfung klärt und dass die prüfende Stelle die Aufwandsabschätzung und das Angebot für die Prüfung auf dieser Grundlage erstellt.

5.3 Mögliche Prüfmethoden

Unter „Prüfmethoden“ werden alle für die Ermittlung eines Sachverhaltes verwendeten Methoden verstanden. Während einer Prüfung können unterschiedliche Prüfmethoden genutzt werden, z. B. folgende:

- mündliche Befragung (Interview),
- Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten und Gegenständen,
- Dokumentenanalyse (hierzu gehören auch elektronische Daten),
- technische Vor-Ort-Prüfung bzw. gezielte Beobachtung (z. B. das Funktionieren von Alarmanlagen, Zutrittskontrollen, Anwendungen vorführen lassen),
- Penetrationstests,
- Datenanalyse (z. B. Logfiles, Firewall-Konfiguration, Auswertung von Datenbanken etc.),
- schriftliche Befragung (z. B. Fragebogen) und

[16] https://www.bsi.bund.de/dok/14346464

- Einbeziehung bestehender Nachweise (z. B. Prüfung des Prüfberichts einer in anderem Kontext vorgenommenen Prüfung, siehe auch Abschnitt 5.1.3).

Der Einsatz der unterschiedlichen Prüfmethoden hängt vom konkreten Fall ab und ist durch das Prüfteam festzulegen.

5.4 Aufwand der Prüfung

In die Ermittlung des Prüfaufwands bei der Erstprüfung fließen z. B. ein:

- die Größe des zu prüfenden Geltungsbereichs, gemessen an der Anzahl der Mitarbeiter der Organisation,
- die Kritikalität bzw. der Versorgungsgrad gemäß BSI-KritisV,
- die Komplexität des zu prüfenden Geltungsbereichs,
- die IT-Abhängigkeit und die IT-Durchdringung der kritischen Dienstleistung sowie
- die Frage, ob im Rahmen der Prüfung detaillierte Untersuchungen auf Basis fachlicher/ technischer Tests oder Analysen durchgeführt werden sollen – dies wird in der Regel dann der Fall sein, wenn der KRITIS-Betreiber solche Tests nicht regelmäßig durchführt.

Zur Abschätzung der Komplexität können folgende Fragestellungen herangezogen werden:

- Wie komplex ist die IT-Systemlandschaft (Anzahl der Systeme und Heterogenität der eingesetzten Systeme)?
- Über wie viele Standorte verteilt sich der Untersuchungsgegenstand (Geltungsbereich)?
- Wie viele Netzübergänge gibt es?
- Welche und wie viele IT-Anwendungen werden in der Institution eingesetzt? Werden damit kritische Geschäftsprozesse unterstützt?
- Werden übergeordnete Verfahren eingesetzt, die Einfluss auf Bereiche außerhalb der Institution haben?
- Wie lange ist das Thema Informationssicherheit in der Organisation schon etabliert und wie viel Erfahrung hat die Organisation damit bereits gesammelt? Sind ggf. bereits (Teil-) Systeme zertifiziert?

Die konkrete Prüfdauer ist schwer abzuschätzen, da sich die Anlagen der KRITIS-Betreiber stark unterscheiden.

Jede Prüfung sollte die folgenden sechs Prüfschritte abdecken. Im Allgemeinen sind diese der konkreten Anlage und den branchenspezifischen Besonderheiten anzupassen.

Prüfschritte	Tätigkeit
Schritt 1	Vorbereitung der Prüfung sowie Prüfung der Eignung des Geltungsbereichs
Schritt 2	Erstellung des Prüfplans
Schritt 3	Dokumentenprüfung
Schritt 4	Vor-Ort-Prüfung
Schritt 5	Nachbereitung der Vor-Ort-Prüfung
Schritt 6	Erstellung des Prüfberichtes

Tabelle 1: Orientierung zum relativen Zeitaufwand bei der Durchführung einer Prüfung als Nachweis der Umsetzung der Anforderungen § 8a Absatz 3 BSIG, Quelle: BSI

5.5 Prüfplan und mögliche Stichprobenauswahl

Jeder Prüfung muss ein dokumentierter Prüfplan zugrunde liegen. In diesem werden das Prüfteam, die Prüfobjekte, die Prüfziele sowie die beabsichtigte Prüfmethode im Vorfeld der Prüfung festgelegt. Ebenfalls sollten die Rollen im Prüfteam und die benötigten Ansprechpartner beim KRITIS-Betreiber sowie die zeitlichen Abläufe festgeschrieben werden.

Zu den Nachweisdokumenten gehören Informationen zum Ablauf der Prüfung einschließlich der Prüfthemen und der überprüften Standorte (Anlage PD.B). Es muss möglich sein, anhand dieser Informationen den Prüfablauf nachzuvollziehen.

Mindestens erforderlich sind dafür folgende Informationen zum Prüfablauf (ein Beispiel für eine Tabelle mit Informationen zum Prüfablauf findet sich in Anhang B):

Was?

- Es muss nachvollziehbar sein, welche Themen in der Prüfung konkret behandelt wurden. Wo sinnvoll, können die Themen auch unter einer Gliederungsebene gruppiert werden.
- Sofern sich die Prüfgrundlage aus mehreren Standards/Dokumenten zusammensetzt, ist jedes Prüfthema den entsprechenden Standards/Dokumenten aus der Prüfgrundlage (idealerweise mit Bezug zum entsprechenden Kapitel) zuzuordnen.
- Das Prüfobjekt (Prozess, System, Dokument, KRITIS, etc.) muss dem BSI nachvollziehbar dargelegt werden.

Wie?

- Es muss nachvollziehbar sein, welche Methoden angewandt wurden, um die Prüfergebnisse zu erzielen.

Wer?

- Es muss nachvollziehbar sein, welche Personen des Prüfteams und welche Rollen bzw. Fachbereiche des KRITIS-Betreibers an der (Teil-) Prüfung beteiligt waren.

Wann?

- Es muss ein chronologischer Ablauf der Prüfschritte erkennbar sein.
- Es muss nachvollziehbar sein, welche Themen in der Prüfung zeitlich schwerer gewichtet wurden.

Wo?

- Der Prüfort muss dem BSI nachvollziehbar dargelegt werden. Insbesondere für den Fall, dass in einer Prüfung mehrere Anlagen betrachtet werden, muss klar hervorgehen, auf welche Anlagen/Standorte sich das jeweilige Thema bezieht.

Eine vollständige Prüfung des gesamten Geltungsbereichs ist in der Regel nicht mit wirtschaftlich vertretbarem Aufwand möglich, daher muss der Prüfer eine angemessene Stichprobenauswahl im Prüfplan festlegen. Diese muss mindestens alle kritischen Prozesse umfassen. Bei der Wahl der Stichproben ist risikoorientiert vorzugehen (Berücksichtigung von Wahrscheinlichkeit und Auswirkungen auf die Erbringung der kDL), allerdings ist darauf zu achten, dass in der Gesamtheit der Stichproben eine gute Abdeckung der Anlage oder der Anlagen der Kritischen Infrastruktur, aber auch eine netztopologische Abdeckung erzielt wird. Bereiche mit höheren Risiken sollen stärker berücksichtigt werden. In die Risikobetrachtung sollte insbesondere auch die Auswirkung auf die Versorgung der Bevölkerung mit der kritischen Dienstleistung entsprechend der Größe des KRITIS-Betreibers einbezogen werden (Wie viele Menschen wären von einem Ausfall betroffen? Wie gravierend wäre eine Störung/ein Ausfall?). Die Auswahl der Stichprobe ist zu begründen.

Ein auf mehrere Jahre angelegtes Prüfungskonzept ist zu empfehlen, damit jedes informationstechnische System, jede informationstechnische Komponente und jeder informationstechnische Prozess in absehbarer Zeit mindestens einmal geprüft wird. Die Stichprobe ist vom Prüfer bzw. der prüfenden Stelle zu wählen. Die Verwendung der gleichen Stichprobe über mehrere Prüfungen hinweg ist nicht geeignet. Im Prüfplan sollten vorherige Prüfungen berücksichtigt werden, um mittel-/langfristig eine vollständige Abdeckung aller Komponenten/Prozesse zu erreichen. Insbesondere ist die Mängelliste aus den letzten Prüfergebnissen (Prüfberichten) bei der Stichprobenauswahl im Prüfplan zu berücksichtigen.

Anmerkung: Die Normen ISO 19011, ISO/IEC 27007 und ISO/IEC 27008 können für die Planung und Durchführung einer Prüfung Hinweise geben.

5.6 Dokumentation des Prüfergebnisses im Prüfbericht

Der Prüfbericht über die Umsetzung der Anforderungen nach § 8a Absatz 1 BSIG sollte

- ein eigenständiges Dokument sein,
- in deutscher oder englischer Sprache verfasst werden, alle Inhalte müssen nachvollziehbar sein,
- eine eindeutige Bezeichnung und Versionsverwaltung haben,
- alle für die Bewertung relevanten Metainformationen enthalten (z. B. Geltungsbereich der Untersuchung, Prüfziel, Zeitpunkt, Ort und Dauer der Prüfung, prüfende Stelle und Prüfteam, Prüfergebnisse usw.),
- alle Prüfschritte nachvollziehbar und wiederholbar dokumentieren und die Prüfentscheidungen begründet darlegen.

Insbesondere sind Sicherheitsmängel und -empfehlungen im Prüfbericht zu dokumentieren. Eine Beschreibung der Mindestanforderungen an die Beschreibung der Sicherheitsmängel sowie ein Muster einer Mängelliste stellt das BSI auf seinen Webseiten[17] und in der Tabelle 3 im Abschnitt 5.7.4 Mängelliste bereit.

5.6.1 Einschätzung des Reifegrads von ISMS und BCMS

Im Rahmen der Nachweiserbringung sollte regelmäßig eine Bewertung der Wirksamkeit des Managementsystems für Informationssicherheit (ISMS) einer Institution vorgenommen werden. Dies kann mithilfe eines Reifegradmodells erfolgen. Ein Reifegradmodell ermöglicht, den Fortschritt des ISMS nachvollziehbar über die Jahre hinweg zu dokumentieren, ohne sich dabei in Einzelmaßnahmen zu verlieren. Es stellt eine weitere potenzielle Kennzahl zur Steuerung der Informationssicherheit in einer Institution dar.

Ebenso müssen das betriebliche Kontinuitätsmanagement (Business Continuity Management System, BCMS) und die sich daraus ergebenden Anforderungen und Maßnahmen regelmäßig auf ihre Effizienz und Effektivität überprüft werden.

Abschnitt PE im Nachweisdokument P sieht daher eine Benennung des Reifegrads von ISMS und BCMS vor.

Bei den Angaben zu den Reifegraden handelt es sich ausschließlich um eine oberflächliche Einschätzung des Prüfteams. Dabei sollen die Reifegrade von ISMS und BCMS ausdrücklich nur innerhalb des Geltungsbereiches der Prüfung, also mit Blick auf die Sicherstellung der kritischen Dienstleistung, beurteilt werden. Die Einteilung in Reifegrade in diesem Nachweisformular orientiert sich an klassischen Reifegradmodellen, eine Reifegradbestimmung nach wissenschaftlichen Methoden ist jedoch nicht gefordert. Vielmehr soll das Prüfteam eine grobe Einschätzung zur Frage, wie stark die Prozesse für das ISMS und das BCMS bereits im Unternehmen verankert sind und gelebt werden, in Form der Reifegrade abgeben.

Für die Einschätzung des Reifegrads des geprüften ISMS und BCMS ist die folgende Auflistung zu verwenden.

ISMS-Reifegrad

- Reifegrad 1: Ein ISMS ist zwar geplant, aber bisher nicht etabliert.
- Reifegrad 2: Ein ISMS ist weitestgehend etabliert.
- Reifegrad 3: Ein ISMS ist etabliert und dokumentiert.
- Reifegrad 4: Zusätzlich zum Reifegrad 3 wurde das ISMS regelmäßig auf Effektivität überprüft.
- Reifegrad 5: Zusätzlich zum Reifegrad 4 wurde das ISMS regelmäßig verbessert.

[17] https://www.bsi.bund.de/dok/11282222

BCMS-Reifegrad

- Reifegrad 1: Ein BCMS ist zwar geplant, aber bisher nicht etabliert.
- Reifegrad 2: Ein BCMS ist weitestgehend etabliert.
- Reifegrad 3: Ein BCMS ist etabliert und dokumentiert.
- Reifegrad 4: Zusätzlich zum Reifegrad 3 wurde das BCMS regelmäßig überprüft und beübt.
- Reifegrad 5: Zusätzlich zum Reifegrad 4 wurde das BCMS regelmäßig verbessert.

Zur Beurteilung, ob die Reifegrade 4 oder 5 erreicht werden, ist der Blick auf die in der Vergangenheit durchgeführten Maßnahmen bzw. Überprüfungen zu richten. Damit ergibt sich implizit, dass ein neu eingerichtetes ISMS oder BCMS, in dem Prozesse zur Messung und zur kontinuierlichen Verbesserung zwar verankert sind, aber bisher noch nicht mehrfach durchlaufen wurden, diese Reifegrade noch nicht erreichen kann.

5.7 Sicherheitsmängel, Umsetzungsplan und Mängelliste

5.7.1 Sicherheitsmängel

Zu jeder geprüften Sicherheitsvorkehrung gemäß § 8a Absatz 1 BSIG sind die festgestellten Sachverhalte im Prüfbericht aufzunehmen und hinsichtlich des Umsetzungsstatus zu bewerten. Wird eine Abweichung zu den Anforderungen gemäß § 8a Absatz 1 BSIG festgestellt, handelt es sich um einen Sicherheitsmangel, der in der Mängelliste zu dokumentieren und in Bezug auf die Erbringung der kritischen Dienstleistung zu bewerten ist. Grundsätzlich sind alle Feststellungen, die ein Risiko darstellen oder eine korrigierende Maßnahme benötigen, die nicht ohne Zeit- oder Ressourcenaufwand umgesetzt werden können, in den Prüfbericht und der Mängelliste aufzunehmen.

Die Sicherheitsmängel sowie deren Bewertung in Bezug auf die Erbringung der kritischen Dienstleistung werden von der prüfenden Stelle erfasst.

5.7.2 Mängelkategorien

Zur Die Sicherheitsmängel sind durch die prüfende Stelle in zwei Dimensionen zu klassifizieren:

1) Betroffenes Thema der IT-Sicherheit (siehe Anhang E)

2) Schwere des Mangels

Für die Klassifizierung der Schwere der Sicherheitsmängel sind Mängelkategorien zu definieren und im gesamten Prüfbericht einheitlich zu verwenden. Jede prüfende Stelle kann dabei ein für ihre Prüfung übliches Bewertungsschema wählen. In der Mängelliste des Nachweisdokuments, das an das BSI gesendet wird, müssen jedoch einheitliche Mängelbewertungen vorgenommen werden. Daher muss der Prüfer (sofern seine Mängelkategorien von den Mängelkategorien dieser Orientierungshilfe abweichen) seine Kategorien auf die in Tabelle 2 festgelegten Kategorien abbilden.

Für alle Sicherheitsmängel sind die Ursachen zu analysieren und nachvollziehbar zu dokumentieren.

Kategorie	Definition	Prüfbericht / Mängelliste
Schwerwiegende/r oder erhebliche/r Abweichung/ Sicherheitsmangel	Eine „schwerwiegende Abweichung“ stellt eine **gravierende** Gefährdung bzw. ein gravierendes Risiko dar. Eine „erhebliche Abweichung“ stellt eine große Gefährdung bzw. ein großes Risiko dar. Es besteht akuter Handlungsbedarf. Die Abweichung muss umgehend bzw. zeitnah **beseitigt** werden, da die Vertraulichkeit, die Integrität, die Authentizität oder die Verfügbarkeit der kDL stark gefährdet ist und erheblicher Schaden zu erwarten ist.	Aufnahme in den Prüfbericht und Aufnahme in die Mängelliste des Nachweises
Geringfügige/r Abweichung/ Sicherheitsmangel	Eine „ geringfügige Abweichung“ stellt eine Gefährdung bzw. ein Risiko dar. Es besteht kein akuter Handlungsbedarf. Die zugrundeliegende Abweichung muss mittelfristig beseitigt werden. Die Vertraulichkeit, Integrität, die Authentizität oder Verfügbarkeit der kDL kann beeinträchtigt werden.	Aufnahme in den Prüfbericht und Aufnahme in die Mängelliste des Nachweises
Empfehlung	Eine „Empfehlung“ stellt einen Verbesserungshinweis dar. Durch die Umsetzung der Empfehlung kann die Sicherheit erhöht werden.[18] Empfehlungen können sein: - Verbesserungsvorschläge für die Umsetzung von Maßnahmen - ergänzende Maßnahmen , die sich in der Praxis bewährt haben, oder - Kommentare hinsichtlich der Angemessenheit und Wirksamkeit von Maßnahmen.	Aufnahme in den Prüfbericht, Aufnahme in die Mängelliste empfohlen
Keine Abweichung	Es liegt kein Sicherheitsmangel vor, wenn die Anforderungen vollständig erfüllt werden und alle Maßnahmen vollständig, wirksam und angemessen umgesetzt sind. Es gibt keine ergänzenden Hinweise.	Aufnahme in den Prüfbericht, keine Aufnahme in die Mängelliste

Tabelle 2: Mängelkategorien

5.7.3 Risikobetrachtung und Umsetzungsplan

Jeder Sicherheitsmangel muss einer Risikobetrachtung unterzogen werden. In einem Umsetzungsplan müssen die konkret umzusetzenden Maßnahmen, die dafür Verantwortlichen, die geplanten Termine für die Behebung der Mängel sowie deren Umsetzungsstatus benannt werden.

Die umzusetzenden Maßnahmen, die dafür Verantwortlichen, die geplanten Termine für die Behebung der Mängel sowie deren Umsetzungsstatus werden vom KRITIS-Betreiber beschrieben.

[18] Eine teilweise oder nicht umgesetzte Maßnahme bzw. Anforderung darf nur dann als Sicherheitsempfehlung eingestuft werden, wenn das Prüfteam davon ausgehen kann, dass mittelfristig nicht mit einer Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit der kDL zu rechnen ist.

5.7.4 Mängelliste

Die Mängelliste fasst schließlich die Sicherheitsmängel sowie deren Klassifizierung, die Risikobetrachtung und den Umsetzungsplan übersichtlich zusammen und stellt außerdem den Status der Umsetzung dar.

Die Mindestanforderungen an eine solche Mängelliste sind unten beschrieben. Ein Muster für eine Mängelliste inklusive Umsetzungsplan findet sich in Anhang D.

Die Mängelliste ist Teil der Nachweisdokumente gemäß § 8a Absatz 3 BSIG und muss als Anlage zu den Nachweisformularen vom KRITIS-Betreiber an das KRITIS-Büro des BSI übersendet werden.

Der Prüfer bzw. KRITIS-Betreiber muss dem BSI ausreichend Informationen zur Bewertung der jeweiligen Sicherheitsmängel und zu deren Behebung zur Verfügung stellen (siehe Abschnitt 5.7.4.1 „Mindestanforderungen an eine Mängelliste“).

Grundsätzlich muss die Mängelliste, die dem BSI als Teil des Nachweises zur Verfügung gestellt wird, ohne weitere Dokumente die Mängel nachvollziehbar beschreiben. Insbesondere ist darauf zu achten, dass Abkürzungen vermieden werden oder hinreichend erklärt werden.

Die Mängelliste im Umsetzungsplan kann außerdem vom Betreiber um eine Spalte Kommentare erweitert werden, um eine eventuell abweichende Stellungnahme des Betreibers aufzunehmen.

Beispiel: Im Operationsbereich eines Krankenhauses sind bei den Medizingeräten keine automatischen Bildschirmsperren aktiviert. Der Prüfer hat dies als geringfügige Abweichung klassifiziert. Der Betreiber kann dann aber kommentieren, dass dies ein besonders zutrittsgeschützter Bereich ist, wo eine automatische Bildschirmsperre sogar kontraproduktiv sein kann.

5.7.4.1 Mindestanforderungen an eine Mängelliste

Wesentlich ist, dass dem BSI ausreichende Informationen zur Bewertung der jeweiligen Sicherheitsmängel zur Verfügung stellen, damit das BSI entscheiden kann, ob die vom Betreiber im Umsetzungsplan vorgesehenen Schritte zur Behebung der Mängel angemessen und ausreichend sind.

a. Jeder Sicherheitsmangel muss nachvollziehbar in seiner Art beschrieben sein. Für das BSI muss ersichtlich sein, warum der beschriebene Umstand einen Sicherheitsmangel darstellt. Für gängige Sicherheitsmängel ist eine einfache Beschreibung in der Regel ausreichend; für Sicherheits-mängel an „exotischeren“ Systemen sind regelmäßig weitergehende Erläuterungen notwendig.
b. Das BSI muss nachvollziehen können, wie die (potenzielle) Auswirkung des Sicherheitsmangels auf Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für das Funktionieren der Kritischen Infrastruktur notwendig sind, aussieht.

c. Die Einschätzung des Risikos für die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für das Funktionieren der Kritischen Infrastruktur notwendig sind, muss für das BSI nachvollziehbar sein. Die Mängelliste muss zur Einschätzung des Risikos der Klassifizierung folgen, die in Tabelle 2: Mängelkategorien beschrieben ist.

d. Das BSI muss nachvollziehen können, ob ein Sicherheitsmangel sachgerecht vom Betreiber adressiert wird. Daher sind vom Betreiber ein Zeitplan und eine Handlungsskizze beizufügen.

Eine Muster-Mängelliste stellt das BSI im Download-Bereich auf seinen KRITIS-Webseiten zusätzlich zu dem Muster in Anhang D bereit[19].

6 Der Nachweisprozess nach § 8a Absatz 3 BSIG

KRITIS-Betreiber haben nach § 8a Absatz 3 BSIG mindestens alle zwei Jahre die Erfüllung der Anforderungen nach § 8a Absatz 1 BSIG auf geeignete Weise nachzuweisen.

6.1 Berechnung der Nachweisfristen

Das BSIG legt fest, dass KRITIS-Betreiber Vorkehrungen und Maßnahmen zur Umsetzung von § 8a Absatz 1 BSIG treffen müssen. Hierüber sind dem BSI gegenüber alle zwei Jahre entsprechende Nachweise zu erbringen.

6.1.1 Erstmaliger Nachweis nach Überschreitung der Schwellenwerte

Für Kritische Infrastrukturen, die erstmalig unter die Regelungen des BSIG fallen, muss der Nachweis nach § 8a Absatz 3 BSIG innerhalb von zwei Jahren erbracht werden. Die Pflicht zur Umsetzung der Sicherheitsmaßnahmen gemäß § 8a Absatz 1 BSIG sowie die Meldepflicht von Vorfällen gemäß § 8b Absatz 4 BSIG besteht dahingegen unverzüglich.

Sofern der KRITIS-Betreiber neben schon registrierten Anlagen durch die jährliche Prüfung neue Anlagen registriert, kann er, sofern die jeweiligen Nachweisfristen nicht überschritten werden, die Gesamtheit aller Anlagen in einem Nachweis zusammenfassen.

6.1.2 Folgenachweise und deren Umsetzungsfristen

KRITIS-Betreiber, die bereits unter das BSIG fallen und mindestens einen Nachweis nach § 8a BSIG erbracht haben, müssen auch weiterhin alle zwei Jahre einen Folgenachweis erbringen. Das Nachweisverfahren ist dabei prinzipiell lückenlos, d. h. mit der Einreichung eines Nachweises schließt sich sofort die Pflicht zur Erbringung des Folgenachweises an. Bei der Berechnung der Fristen ist der Zeitpunkt der vorherigen Einreichung zu betrachten.

[19] https://www.bsi.bund.de/dok/11282222

Erweist sich ein Nachweis im Laufe der Überprüfung im BSI als unvollständig, so dass Nachlieferungen erfolgen müssen, ändert dies nichts an der einmal berechneten Frist für den folgenden Nachweis.

Fristberechnung eines Folgenachweises:

Wird ein Nachweis eingereicht, so erfolgt stets eine taggenaue Berechnung der Frist für den Folgenachweis anhand des Einreichungsdatums. Das Einreichungsdatum wird dem Betreiber in der Empfangsbestätigung mitgeteilt. Die Frist zur Einreichung des Folgenachweises berechnet sich aus dem Einreichungsdatum (E-Mail-Eingang oder Poststempel) zuzüglich zwei Jahre. Es ist für die Fristberechnung unerheblich, ob bei der Einreichung tatsächlich alle notwendigen Nachweisdokumente eingereicht wurden (siehe Abschnitt 6.2.2 „Welche Nachweisdokumente sind einzureichen?“) oder später noch Dokumente nachgeliefert werden.

Beispiel:

- Ablauf der Frist zur Erbringung des Nachweises gemäß § 8a Absatz 3 BSIG 1: 01.04.2020
- Einreichung der Nachweisdokumente: 16.03.2020
- Ablauf der Frist zur Erbringung des Folgenachweises gemäß § 8a Absatz 3 BSIG: 16.03.2022

Ein KRITIS-Betreiber kann jederzeit vor Ablauf der Nachweisfrist seine Nachweisdokumente einreichen. Falls ein KRITIS-Betreiber beispielsweise seine Nachweispflicht nach § 8a Absatz 3 BSIG seinem jährlichen ISO 27001-Auditzyklus anpassen und die Audits gemeinsam durchführen möchte, kann er seine Nachweise auch jährlich einreichen. Die gesetzliche Zweijahresregel stellt eine Minimalanforderung dar.

6.2 Einreichung der Nachweisdokumente

KRITIS-Betreiber müssen gegenüber dem BSI die Erfüllung der Anforderungen aus § 8a Absatz 1 BSIG durch die entsprechenden Nachweise bestätigen. Damit das BSI die Eignung der Prüfung und die Angemessenheit der Vorkehrungen zur Vermeidung von Störungen sowie die Schwere der aufgedeckten Sicherheitsmängel bewerten kann, müssen die Nachweisdokumente alle erforderlichen Informationen enthalten.

6.2.1 Wer reicht Nachweisdokumente ein?

Die KRITIS-Betreiber übermitteln dem BSI dazu für jede Anlage Informationen über Art und Umfang der durchgeführten Prüfung sowie eine Auflistung der in der Prüfung aufgedeckten Sicherheitsmängel. Diese Nachweisdokumente sind beim BSI in schriftlicher Form einzureichen. Eine digitale, maschinenlesbare Kopie muss dem BSI zur Verfügung gestellt werden.

6.2.2 Welche Nachweisdokumente sind einzureichen?

Um alle erforderlichen Informationen über Art und Umfang der durchgeführten Prüfung übersichtlich darzustellen und den Vorgang der Erfassung zu vereinfachen, stellt das BSI Nachweisformulare (Formulare KI und P) bereit und empfiehlt, diese bei der Einreichung der Nachweisdokumente zu verwenden. Die Formulare inklusive der notwendigen Anlagen bilden den Grundstein der Nachweise, die von den KRITIS-Betreibern an das KRITIS-Büro des BSI gesandt werden.

Formular KI enthält Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner beim Betreiber. Formular KI ist vom KRITIS-Betreiber auszufüllen und zu unterschreiben.

Formular P umfasst Angaben zur Prüfdurchführung (Abschnitt PD), zum Prüfergebnis und zu den aufgedeckten Sicherheitsmängeln (Abschnitt PE) sowie zur prüfenden Stelle und zum Prüfteam (Abschnitt PS). Formular P wird von der prüfenden Stelle ausgefüllt und unterschrieben.

Bei der Einreichung der Nachweise muss darauf geachtet werden, dass die Anlagenbenennung den zuvor im BSI registrierten Anlagen entspricht.

Die genannten Formulare, die Mindestanforderungen an eine Mängelliste und ggf. benötigte Selbsterklärungen sind auf der BSI-Website[20] veröffentlicht.

Anmerkung: Grundsätzlich ist es sinnvoll, die zusammen mit Formular P einzureichenden Anlagen (Dokumente) ebenfalls mit Betreiber-ID und ihrer Bezeichnung zu versehen. Dateien sollten entsprechend benannt werden.

Vorschlag für den Aufbau des Dateinamens: <Betreiber-ID>_Anlage_PD.A).

Hat ein KRITIS-Betreiber mehrere Anlagen, so kann er die Nachweisdokumente für alle Anlagen gebündelt beim BSI einreichen. Sollten die in den Formularen vorgesehenen Felder zur Benennung der Anlage nicht ausreichen, so können die Anlagen auf einem gesonderten Blatt zusammengetragen werden. Wichtig ist, dass die Anlagen wie im BSI registriert benannt werden. Die Nachweisdokumente für einzelne Anlagen können auch separat eingereicht werden.

Ein KRITIS-Betreiber muss stets für alle seine Anlagen, die sich im aktuellen Nachweisprozess befinden, die Nachweisdokumente erbringen und einreichen.

Bei der Einreichung der Nachweisdokumente ist die Vorlage des Prüfberichtes zunächst noch nicht zwingend erforderlich. Erst auf Nachfrage des BSI muss ein KRITIS-Betreiber den ausführlichen Prüfbericht als Nachlieferung beim BSI einreichen.

[20] https://www.bsi.bund.de/dok/13085734

6.2.3 Wie können Nachweisdokumente eingereicht werden?

Nachweisdokumente sind im KRITIS-Büro als zentrale Anlaufstelle beim BSI einzureichen. Diese Nachweisdokumente sind in schriftlicher Form einzureichen. Eine digitale, maschinenlesbare Kopie muss dem BSI zur Verfügung gestellt werden. Prinzipiell können Nachweise sowohl per Post als auch per E-Mail an das KRITIS-Büro (kritis-buero@bsi.bund.de) gesendet werden. Das BSI empfiehlt, für eine vertrauliche Übermittlung der Nachweisdokumente per E-Mail, diese zu verschlüsseln. Das benötigte öffentliche S/MIME-Zertifikat bzw. der PGP-Schlüssel des KRITIS-Büros werden im Download-Bereich auf den Webseiten des BSI bereitgestellt[21].

6.2.4 Rückmeldungen und Empfangsbestätigung des BSI

Ein KRITIS-Betreiber erhält vom BSI eine Empfangsbestätigung für die eingereichten Nachweisdokumente, sobald diese erfolgreich auf Vollständigkeit überprüft wurden. Die Empfangsbestätigung gibt an, zu welchem Datum und zu welchen Anlagen Nachweisdokumente erbracht wurden und gilt als formaler Beleg, dass der KRITIS-Betreiber seiner gesetzlichen Pflicht zur Einreichung der Nachweisdokumente gemäß § 8a Absatz 3 BSIG nachgekommen ist. Sie enthält außerdem das Datum, an dem der KRITIS-Betreiber den Folgenachweis zu erbringen hat (siehe Abschnitt 6.1.2).

Sofern zum Nachweis keine Rückfragen erforderlich sind bzw. für die weiterführende Prüfung keine weitere Mitwirkung des KRITIS-Betreibers erforderlich ist, erhält der KRITIS-Betreiber nach der o. g. Empfangsbestätigung keine weitere Benachrichtigung zum Vorgang. Das BSI kann aber jederzeit weitere Teile bzw. die gesamte der Prüfung zugrunde liegende Dokumentation und den Prüfbericht anfordern oder – auch anlassunabhängig – Vor-Ort-Prüfungen anberaumen.

Weiterführende Prüfungen zum Nachweis können grundsätzlich bis zur Einreichung des darauffolgenden Nachweises nach verfügbaren Kapazitäten und im Ermessen des BSI erfolgen. Da in diesem Verfahren kein Abschluss der Nachweisprüfung vorgesehen ist, erteilt das BSI keine Bestätigung über den Abschluss der Nachweisprüfung.

6.2.5 Nachlieferungen

Im Verlauf der Nachweisprüfungen kann es sein, dass das BSI bestimmte Unterlagen nachfordert. Auch nach Versand der Empfangsbestätigung behält sich das BSI vor, jederzeit weitere benötigte Unterlagen nachzufordern. Nachforderungen sind in der Regel mit einer Einreichungsfrist verbunden, die individuell von Art und Umfang der Nachlieferung abhängt.

Nachlieferungen haben keinen Einfluss auf die Berechnung der Frist für den Folgenachweis.

[21] https://www.bsi.bund.de/dok/12211872

6.2.6 Prüfungen durch das BSI

Das BSI hat gemäß § 8a Absatz 4 BSIG die Möglichkeit, bei KRITIS-Betreibern zu überprüfen, ob diese die Anforderungen nach § 8a Absatz 1 BSIG erfüllen. Auslöser für eine Prüfung können Unstimmigkeiten der gemäß § 8a Absatz 3 BSIG eingereichten Unterlagen sein, die das BSI beim Betreiber klären möchte, oder die Auswahl der Anlage als Prüfungsobjekt erfolgte im Rahmen einer zufälligen Stichprobenauswahl. Ein wesentlicher Bestandteil dieser Überprüfungen ist eine Vor-Ort-Prüfung beim Betreiber.

7 Dokumenten-/Anlagenübersicht

Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG sollte folgende Dokumente beinhalten:

- Nachweisdokument KI inkl. Unterschrift des Betreibers
- Nachweisdokument P inkl. Unterschrift und Stempel der prüfenden Stelle
- Anlage PD.A: Beschreibung und grafische Darstellung des Geltungsbereichs der Prüfung in einem Netz-/Anlagenplan
- Anlage PD.B: Prüfplan
- Anlage PE.A: Liste der Sicherheitsmängel inkl. Umsetzungsplan zur Behebung der Mängel
- Anlage PS.A: Nachweis über die zusätzliche Prüfverfahrenskompetenz für § 8a BSIG
  - **a)** für (mindestens) einen Prüfer des Prüfteams
  - **b)** für einen mit der Prüfung betrauten Mitarabeiter der prüfenden Stelle (sofern nicht bereits durch a) abgedeckt)
- Anlage PS.B: Formlose Unabhängigkeitserklärung für alle Mitglieder des Prüfteams

Optionale Anlage

- Anlage PD.C: Beschreibung der Prüfgrundlage (sofern kein oder nur teilweise ein B3S verwendet wurde)

Anhang A

Ethische Grundsätze

Um Vertrauen in eine objektive Prüfung zu schaffen, ist die Einhaltung der „Ethischen Grundsätze“ notwendig. Die „Ethischen Grundsätze“ müssen sowohl von den Prüfern als auch von der prüfenden Stelle eingehalten werden. Sie umfassen folgende Prinzipien:

- **Rechtschaffenheit und Vertrauenswürdigkeit**
  Die Rechtschaffenheit begründet Vertrauen und schafft damit die Grundlage für die Zuverlässigkeit eines Urteils. Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während einer Prüfung erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Prüfung eine wichtige Arbeitsgrundlage. Prüfer beachten den Wert und das Eigentum der erhaltenen Informationen und legen diese nicht ohne entsprechende Befugnis offen, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.
- **Fachkompetenz**
  Prüfer übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben und setzen diese bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.
- **Objektivität und Sorgfalt**
  Ein Prüfer hat ein Höchstmaß an sachverständiger Objektivität und Sorgfalt beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Aktivitäten oder Geschäftsprozesse zu zeigen. Die Beurteilung aller relevanten Umstände hat mit Ausgewogenheit zu erfolgen und darf nicht durch eigene Interessen oder durch Andere beeinflusst werden.
- **Sachliche Darstellung**
  Ein Prüfer hat die Pflicht, seinem Auftraggeber wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehören die objektive und nachvollziehbare Darstellung der Sachverhalte in den Prüfberichten, die konstruktive Bewertung der dargestellten Sachverhalte und die konkreten Empfehlungen zur Verbesserung der Maßnahmen und Prozesse.
- **Nachweise und Nachvollziehbarkeit**
  Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Schlussfolgerungen und Ergebnissen zu kommen, ist die eindeutige und folgerichtige Dokumentation der Sachverhalte. Hierzu gehört auch eine dokumentierte und nachvollziehbare Methodik (Prüfplan, Bericht), mit der das Prüfteam zu seinen Schlussfolgerungen kommt.
- **Unabhängigkeit und Neutralität**
  Ein Prüfer muss weisungsfrei und unvoreingenommen die Prüfung durchführen. Er muss die Prüfungsergebnisse nachvollziehbar dokumentieren können. Jedes Prüfteam sollte zur

Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei Prüfern bestehen („Vier-Augen-Prinzip“). Alle Mitglieder des Teams dürfen aus Gründen der Unabhängigkeit und Neutralität vorher nicht unmittelbar im geprüften Bereich beratend oder auch ausführend, z. B. bei der Erstellung von Konzepten oder Konfiguration von IT-Systemen, tätig gewesen sein.

Anhang B

Beispiel für Tabelle mit Informationen zum Prüfablauf

Datum	**Uhrzeit (von-bis)**	**(Stand-) Ort**	**Prüfthemen**	**Verweis auf Prüfgrundlage**	**Prüfmethode**	**Prüfobjekt *(Funktionen / Abteilungen / Bereiche / Prozesse / System / IT-Verbund)***	**Beteiligte Prüfer**	**Prozess- bzw. Fachverantwort-liche**
Prüftag	*Zeitspanne des Prüf-themas*	*Standort des Prüfobjektes. Der Standort/ Anlage muss dem Geltungs-bereich zuzuordnen sein.*	*Geprüftes Thema bzw. Themen-gebiet*	*Auflistung der konkret verwendeten Kapitel/ Bausteine der Prüfgrundlage*	*Eine Auflistung der angewandten Prüfmethoden: z. B. Begehung, Dokumenten-prüfung, Interview…*	*Prüfobjekte 1-n* *Pro Themenkomplex ist eine neue Zeile auszufüllen*	*Eine Auflistung der an dem Prüfthemen beteiligten Prüfer*	*Prozess- bzw, Fachverantwort-liche des KRITIS-Betreibers für das Prüfthema*
02.12.19	11:00-12:00	Betriebsleit-zentrale Musterstadt	Technische Information ssicherheit	ISO 27001 A.7.1, B3S Kap. 5	Inaugenschein-nahme, Dokumenten-prüfung	Dokumente: • Absicherung_von_Netz-übergängen.docx • Zonenkonzept.docx Systeme: • VPN-Konzentrator • Firewall-Cluster	Max Mustermensch	Netzwerk-administrator

Anhang C

Anforderungen an die Beschreibung und Darstellung des Geltungsbereiches (als Hilfestellung zu Abschnitt 5.2)

- G01: Die Anlage ist erkennbar und nachvollziehbar beschrieben.
- G02: Die vom Betreiber erbrachten Teile der kDL sind erkennbar und nachvollziehbar beschrieben.
- G03: Die Darstellung enthält alle wesentlichen Merkmale der Anlagenkategorie.
- G04: Alle für die kDL maßgeblichen Prozesse sind erfasst.
- G05: Alle für die kDL maßgeblichen Systeme, Komponenten und ggf. Applikationen sind erfasst.
- G06: Alle Bereiche der KRITIS gehen aus dem eingereichten Geltungsbereich hervor.
- G07: Die Grenzen des Geltungsbereiches sind klar erkennbar.
- G08: Die Schnittstellen zu außerhalb des Geltungsbereich liegenden Prozessen, Systemen, Komponenten und ggf. Applikationen sind erkennbar und nachvollziehbar beschrieben.
- G09: Die Abhängigkeiten zu außerhalb des Geltungsbereich liegenden Prozessen, Systemen, Komponenten und ggf. Applikationen sind erkennbar und nachvollziehbar beschrieben.
- G10: Durch Dritte betriebene Teile der KRITIS sind erkennbar und nachvollziehbar beschrieben.
- G11: Der Geltungsbereich ermöglicht eine Zuordnung zwischen Prozessen und zugehörigen notwendigen Systemen, Komponenten und ggf. Applikationen.
- G12: Der Geltungsbereich ist in einem Netzstrukturplan dargestellt.
- G13: Zum Verständnis notwendige schriftliche Ergänzungen zum Netzstrukturplan wurden vorgenommen.

Anforderungen an die Darstellung des Geltungsbereiches durch einen Netzstrukturplan (als Hilfestellung zu Abschnitt 5.2)

- N01: Der Netzstrukturplan bietet einen Überblick über den Geltungsbereich.
- N02: Alle maßgeblichen Systeme, Komponenten und ggf. Applikationen sind dargestellt.
- N03: Das Abstraktionsniveau ist passend gewählt worden.
- N04: Die Relevanz einzelner Elemente des Netzstrukturplans für die kDL ist ersichtlich.
- N05: Alle Kommunikationsschnittstellen nach außen sind dargestellt.
- N06: Wartungsschnittstellen sind abgebildet, sofern sie dauerhaft freigeschaltet sind.
- N07: Der Netzstrukturplan gibt eine ggf. existierende Aufteilung in Standorte wieder.
- N08: Die IT-Anbindungen verschiedener Standorte zueinander sind dargestellt.
- N09: Ausgelagerte Dienstleistungen sind dargestellt.
- N10: Funktionale Bezeichnungen und Legenden liegen nötigenfalls vor und sind verständlich.

Anhang D

Muster für eine Mängelliste

Mängelliste						**Umsetzungsplan**[22]			
ID[23]	**Mangelbeschreibung**[24]	**Klassifizierung des Mangels**[25]		**KRITIS-Bezug**[26]	**KRITIS-Risiko**[27]	**Maßnahmen**	**Verantwortliche**	**Termin**	**Status**
		Thema	**Schwere**						
1	Die Unter-nehmens-richtlinie zur Passwort-komplexität wird auf den ERP-Systemen nicht angewendet. User, aber insbesondere Ad-ministratoren sind orga-nisatorisch verpflichtet, komplexe Kennwörter zu verwenden. Dies wird jedoch nicht technisch durchgesetzt.	Technische Informations-sicherheit	Gering-fügige Ab-weichung	ERP-System zur Behandlung/Bestel-lung/ Distribu-tion/Inverkehr-bringen	Eine Übernahme eines privilegierten Kontos kann erhebliche Auswirkungen auf die Verfügbarkeit der kDL haben, jedoch ist der administrative Zugriff nur aus einem isolierten und gesicherten Adminnetz möglich. Nicht privilegierte Konten haben ein-geschränkte Rechte und können nur geringe Störungen hervorrufen. Anomalien würden von einem SIEM erkannt und zeitnah kontrolliert werden.	Die Übernahme der Kennwortrichtlinien wird als Change beim ERP-Hersteller beauftragt	IT-SiBe, ERP-Hersteller, ERP-Administration	Q3 2018	50%
2	…	…		…	…	…	…	…	…

Tabelle 3: Muster für eine Mängelliste mit Umsetzungsplan

[22] Umsetzungsplan: Handlungs- und Zeitplan zur Behebung; ggf. mit Zuständigkeit

[23] ID: Eine eindeutige Referenz oder Kennung, um die Kommunikation über die Mängel zu erleichtern

[24] Mangelbeschreibung: Eine verständliche Beschreibung des Sicherheitsmangels mit zusammenfassender Überschrift

[25] Klassifizierung des Mangels: Zur thematischen Klassifizierung des Mangels dienen die in Anhang E dargestellten Kategorien, eine Mehrfachauswahl ist möglich.

[26] KRITIS-Bezug: Eine Benennung des Teils der KRITIS inklusive einer konkreten Referenz auf die geprüfte Anlage, auf den der Sicherheitsmangel sich konkret auswirkt, bzw. auswirken kann. Bei weitreichenden Auswirkungen beschränkt auf die wichtigsten Teilsysteme oder eine überblicksartige Beschreibung

[27] KRITIS-Risiko: Eine Bewertung des Sicherheitsmangels, beschreibend in Worten oder als Klassifikation, für die Erbringung der kritischen Dienstleistung

Anhang E

Für die thematische Klassifizierung von Mängeln sollen folgende Kategorien genutzt werden:

1. Informations-Sicherheits-Management-System (ISMS)
2. Asset Management
3. Continuity- und Notfallmanagement für die kDL
4. Technische Informationssicherheit
   - 4.1 Absicherung von Netzübergängen
   - 4.2 Sichere Interaktion im Internet
   - 4.3 Sichere Software (insbesondere Vermeidung von offenen Sicherheitslücken)
   - 4.4 Sichere und zuverlässige Hardware
   - 4.5 Sichere Authentisierung
   - 4.6 Verschlüsselung
   - 4.7 Sonstiges
5. Personelle und organisatorische Sicherheit
6. Bauliche/physische Sicherheit
7. Vorfallserkennung und -bearbeitung
8. Überprüfung im laufenden Betrieb
9. Lieferanten, Dienstleister und Dritte
10. Branchenspezifische Technik und (Kern-)Komponenten (Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung)

Glossar

Begriff	Definition
Abweichung	Nichtkonformität. Auftretende Sicherheitsmängel werden als Abweichung aufgefasst.
angemessen	Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
Anlage	Kritische Infrastruktur gemäß Definition in der BSI-KritisV
Branchenspezifischer Sicherheitsstandard (B3S)	Gemäß § 8a Absatz 2 BSIG haben Betreiber Kritischer Infrastrukturen und ihre Branchenverbände die Möglichkeit, branchenspezifische Sicherheitsstandards (B3S) zur Gewährleistung der Anforderungen gem. § 8a Absatz 1 BSIG vorzuschlagen.
Gefundene Sicherheitsmängel	Im Rahmen der Prüfung gefundene, nicht oder nur teilweise umgesetzte notwendige Maßnahmen. Gefundene Sicherheitsmängel sind entsprechend mit „Schweregraden“ zu versehen (siehe Mängelkategorien).
Geltungsbereich	Der Geltungsbereich des Nachweises umfasst die Kritische Infrastruktur bzw. die kritische Dienstleistung (kDL) vollständig (siehe Kapitel 2 „Prüfgegenstand“). Er beschreibt alle zugehörigen Prozesse, Systeme, Komponenten und Organisationseinheiten.
Kompetenz	Angelernte Fähigkeit, die die Ausübung einer bestimmten Tätigkeit ermöglicht.
KRITIS-Betreiber	Betreiber einer Kritischen Infrastruktur gemäß § 2 Absatz 10 BSIG, § 1 Absatz 2 BSI-KritisV).
Kritische Dienstleistung (kDL)	Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der Öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten.
Kritische Infrastruktur	siehe Definition im BSIG bzw. Konkretisierung in der BSI-KritisV

Begriff	Definition
Maßnahmen	Die gemäß BSI-Gesetz umzusetzenden angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen gemäß § 8a Absatz 1 BSIG. Zu diesen Vorkehrungen gehören auch infrastrukturelle und personelle Maßnahmen. Besonders kritische Prozesse bedürfen besonderer Sicherheitsmaßnahmen.
Nachweis	Die Gesamtheit der Nachweisdokumente bildet den Nachweis.
Nachweisdokumente	Die Nachweisdokumente bestehen aus den Formularen KI und P sowie den zugehörigen Anlagen, Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie der zur Bearbeitung erforderlichen Informationen.
Prüfbericht	Dokument der prüfenden Stelle, welches die Audit-, Prüfungs- oder Zertifizierungsergebnisse enthält.
Prüfende Stelle	Institution, die das Prüfteam zusammenstellt, welches einen Teil des Nachweises erbringt, indem geprüft wird, ob der KRITIS-Betreiber die Maßnahmen gemäß § 8a Absatz 1 BSIG umgesetzt hat.
Prüfgegenstand	Der Prüfgegenstand umfasst die informationstechnischen Systeme, Komponenten und Prozesse, Rollen bzw. Personen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind bzw. auf diese Einfluss haben.
Prüfplan	Dokument, in dem der Prüfer vor Prüfungsbeginn die Rahmenbedingungen für die Prüfung festlegt. Inhalt sind das Prüfverfahren bzw. die Prüfmethoden und eine festgelegte Stichprobenprüfung.
Prüfteam	Von der prüfenden Stelle zusammengestelltes Team, welches über die benötigen Kompetenzen verfügt, um zu prüfen, ob der KRITIS-Betreiber die Maßahmen gemäß § 8a Absatz 1 BSIG umgesetzt hat.
Prüfung	Geeigneter Nachweis der Umsetzung der Maßnahmen beim KRITIS-Betreiber. Sie wird durch unabhängige und qualifizierte Prüfer einer prüfenden Stelle durchgeführt. Unter Prüfungen versteht man Audits, Prüfungen und Zertifizierungen gemäß § 8a Absatz 3 BSIG.
Prüfverfahren	Methode, nach der die prüfende Stelle die Nachweise erbringt.