Bundesamt
für Sicherheit in der
Informationstechnik

Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG

Version 0.9.02

vom 30.06.2017

Versionshistorie

Datum	Version	Verfasser	Bemerkungen
07.10.16	0.9	BSI	
20.10.16	0.9.01	BSI	Kleinere Layout- und Rechtschreibkorrekturen
30.06.17	0.9.02	BSI	Kapitel 5.4 Aufwand der Prüfung Ergänzungen NIS-RL Umsetzungsgesetz

Bundesamt für Sicherheit in der Informationstechnik

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

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

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

Inhaltsverzeichnis

1 Überblick

1.1 Managementzusammenfassung

Betreiber Kritischer Infrastrukturen im Sinne der BSI-KritisV sind gemäß den Neuregelungen nach § 8a (1) BSIG verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung (BSI-KritisV) *„[...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen [...]* ihrer *informationstechnischen Systeme, Komponenten und Prozesse“* nach Stand der Technik zu treffen und dies gemäß § 8a (3) BSIG gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geeignet durch „[...] Sicherheitsaudits, Prüfungen oder Zertifizierungen [...]“ (im weiteren Verlauf der Orientierungshilfe „Prüfung(en)“ genannt) nachzuweisen. Der Betreiber übermittelt dem BSI für jede Anlage zum Einen die Auflistung der durchgeführten Prüfungen und zum Anderen eine Liste der aufgedeckten Sicherheitsmängel (im weiteren Verlauf der Orientierungshilfe „Nachweisdokument“ genannt).

Das BSI kann die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse (im weiteren Verlauf der Orientierungshilfe „Prüfbericht“ genannt), sowie in Abstimmung mit den zuständigen Aufsichtsbehörden die Beseitigung der Sicherheitsmängel verlangen .

Wurde die Eignung eines branchenspezifischen Sicherheitsstandard (B3S) gemäß § 8a (2) BSIG vom BSI festgestellt, können Betreiber dieser Branche sich bei der Umsetzung von § 8a (1) BSIG und damit auch bei der Durchführung der zugehörigen Prüfung an diesem Standard orientieren. Die Vorstellungen des BSI an einen B3S sind in der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG[1]“ (im Folgenden „Orientierungshilfe B3S“ genannt) beschrieben.

1.2 Zielsetzung der Orientierungshilfe

Das vorliegende Dokument soll Betreibern einer Kritischen Infrastruktur, prüfenden Stellen und Aufsichtsbehörden eine Orientierung geben, wie die gesetzlichen Anforderungen gemäß § 8a (3) BSIG erfüllt werden können. Es liefert Rahmenbedingungen an ein geeignetes Nachweisdokument. Zusätzlich hilft es den Autoren branchenspezifischer Sicherheitsstandards (B3S) bei der Erarbeitung des B3S-Kapitels zum Thema Prüfungen (siehe Kapitel 7 „Nachweisbarkeit der Umsetzung“ der Orientierungshilfe B3S).

Im vorliegenden Dokument werden folgende Fragen beantwortet:

- Wie können Betreiber bei der Erfüllung der Nachweispflicht nach § 8a (3) BSIG vorgehen? Welche Informationen sollten sie wem bereitstellen? (Kapitel 2)
- Welche Aufgaben haben prüfende Stellen? Was sind geeignete prüfende Stellen? (Kapitel 3)
- Welche Kompetenzen sollte das Prüfteam nachweisen können? (Kapitel 4)
- Wie sollte die Prüfung durchgeführt werden (Prüfgrundlage, -themen, -methoden, Umfang, Ergebnisse, Vergleichbarkeit)? (Kapitel 5)

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html

Anmerkung:

Sofern anerkannte B3S Anforderungen stellen, die von denen der nachfolgenden Kapitel abweichen, gehen diese spezielleren Anforderungen des B3S vor.

Begriffserklärungen:[2]

Die Orientierungshilfe unterscheidet zwischen der **Prüfung**, dem **Prüfbericht** und dem **Nachweisdokument**.

Unter dem Begriff **Prüfung** werden in diesem Dokument „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ gemäß § 8a (3) BSIG verstanden. Prüfungen werden durch eine prüfende Stelle vorgenommen und die Ergebnisse werden dem Betreiber vorgelegt.

Der **Prüfbericht** ist das Dokument, das die Prüfergebnisse enthält. Der Prüfbericht wird von der prüfenden Stelle erstellt und dem Betreiber vorgelegt. Das BSI kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen.

Als Nachweisdokument werden die Formulare bezeichnet, die der Betreiber pro Anlage beim BSI einreicht. Es besteht aus einer Aufstellung der durchgeführten Prüfungen, der Auflistung der Sicherheitsmängel und weiterer für die Bearbeitung erforderlicher Informationen.

1.3 Rechtliche Grundlage und zeitliche Rahmenbedingungen

Die rechtliche Grundlage der Nachweiserbringung gegen über dem BSI, ergibt sich aus § 8a (3) BSIG[3,4]

Anmerkung:

Die vorliegende Orientierungshilfe will eine Orientierung geben, was im § 8a (3) BSIG unter *„auf geeignete Weise“* in Bezug auf eine Prüfung zu verstehen ist. Die Orientierungshilfe macht keine Vorgaben im Sinne des § 8a (4) BSIG.

Auszug aus dem BSIG:

> *„(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. 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.*
> *(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt*
>
> 1. *im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*
> 2. *im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*

2 Weitere Begriffserklärungen befinden sich im Glossar in Kapitel 7
3 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
4 Siehe https://www.gesetze-im-internet.de/bsig_2009/

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt ***die Ergebnisse***[5] *der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen:*

1. *die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und*
2. *im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.*

Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücken und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist die berechtigte Zweifel an der Einhaltung der Anforderungen nach Absatz 1 begründeten.

(5) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.“§

1.

1.4 Rollen und Zuständigkeiten im Nachweisprozess

Von den in dieser Orientierungshilfe beschriebenen Rahmenbedingungen und Umsetzungshilfen sind die Rollen „Betreiber“, „prüfende Stelle“, „Prüfteam“, „BSI“ und „Aufsichtsbehörde“ betroffen, die in Abbildung 1 dargestellt sind. Eine Kurzbeschreibung der Rollen erfolgt in den nächsten Abschnitten, eine ausführlichere Betrachtung in den nachfolgenden Kapiteln.

5 Fett markiert sind die Änderungen des BSIG, die sich aufgrund des NIS-RL-Umsetzungsgesetzes ergeben haben.

Prüfende Stellen können dabei durch anerkennende Stellen oder akkreditierende Stellen anerkannt oder akkreditiert sein. Auf eine Darstellung dieses Aspekts wird in der Grafik verzichtet, da mit dem IT-SiG **kein** neues Anerkennungs-/Akkreditierungsverfahren eingeführt wird, sondern lediglich auf bestehende Verfahren referenziert wird. Die Anerkennungsstellen haben somit keine eigene Rolle im Rahmen der Umsetzung des § 8a (3) BSIG.

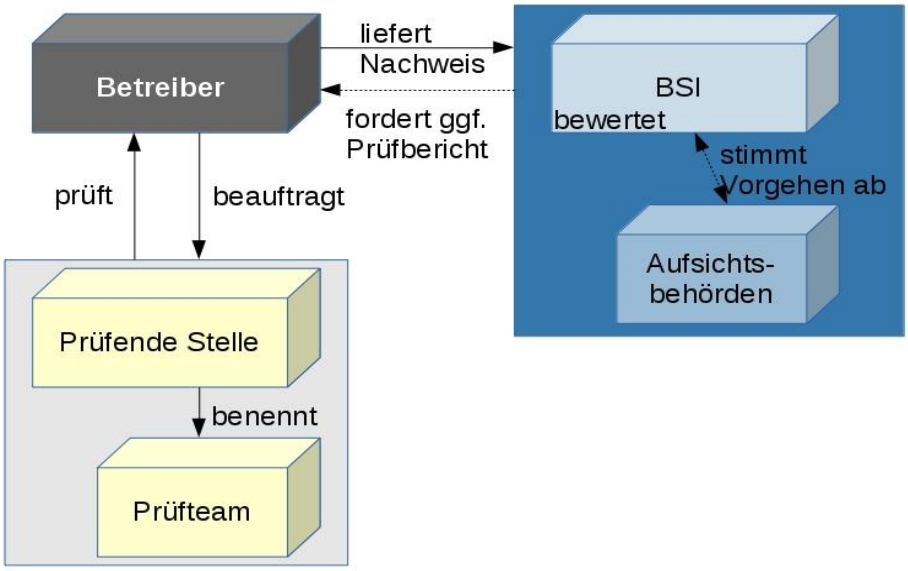

Abbildung 1: Rollen im Nachweisprozess, Quelle: BSI

1.4.1 Betreiber

Die Betreiber Kritischer Infrastrukturen im Sinne des BSIG sind gemäß § 8a (3) BSIG verpflichtet, alle zwei Jahre die Erfüllung der Umsetzung wirksamer und angemessener organisatorischer und technischer Maßnahmen gemäß § 8a (1) BSIG nachzuweisen. Die Maßnahmen dienen der Sicherstellung der Funktionsfähigkeit der Kritischen Infrastruktur, insbesondere der kritischen Dienstleistungen (kDL).

Die Betreiber sollten zunächst geeignete Maßnahmen umsetzen, anschließend eine prüfende Stelle mit einer Prüfung beauftragen, dann bei der Prüfung als Ansprechpartner Auskunft geben und letztlich ein Nachweisdokument an das BSI übersenden.

Die Zuständigkeiten der Betreiber bzgl. Prüfungen und Nachweisen werden detailliert in Kapitel 2 beschrieben. Ihre Aufgaben bei der Unterstützung der prüfenden Stelle bzw. des Prüfteams während der Durchführung der Prüfung werden darüber hinaus in Kapitel 5 beschrieben. Jeder KRITIS-Betreiber trägt die Verantwortung für die Korrektheit des Nachweisdokuments.

1.4.2 Prüfende Stelle und Prüfteam

Mit der Prüfung der Umsetzung der Maßnahmen gemäß § 8a BSIG beauftragt der KRITIS-Betreiber eine prüfende Stelle. Diese 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 die Verantwortung für die korrekte Durchführung der Prüfung (Kapitel 5) sowie für den Prüfbericht inkl. der Dokumente, die sie für das Nachweisdokument bereitstellen muss.

1.4.3 BSI

Das BSI erhält vom KRITIS-Betreiber das Nachweisdokument, inklusive der Mängelliste aus dem Prüfbericht und weitere Informationen zur durchgeführten Prüfung.

Das BSI nimmt das Nachweisdokument des Betreibers entgegen, prüft dieses auf Vollständigkeit und bewertet dessen Inhalte. Das BSI entscheidet auf Grundlage der vorliegenden Informationen, ob diese ausreichen oder ob eine Übermittlung des gesamten Prüfberichts mit allen Prüfergebnissen erforderlich ist.

Erkenntnisse über häufig auftretende Mängel oder Sicherheitsprobleme fließen ggf. über die individuelle Betrachtung der Nachweisdokumente hinaus und ausschließlich anonymisiert in die allgemeine Lagebewertung (z. B. Liste der häufigsten Sicherheitsmängel in der Branche) und in Sicherheitsempfehlungen ein. Diese Bewertungen und Empfehlungen sollen helfen, Risiken bei anderen Betreibern vorzubeugen und bei eingetretenen Sicherheitsvorfällen geeignet zu beraten. Diese Information erhalten registrierte KRITIS-Betreiber über die auf Basis des § 8b BSIG angelegten Informationskanäle.

1.4.4 Aufsichtsbehörden

Liegt ein besonders relevanter Sicherheitsmangel vor, stimmt das BSI zusammen mit den zuständigen Aufsichtsbehörden das weitere Vorgehen ab. Das BSI kann in diesem Fall im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes bzw. im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Mängel verlangen [6].

Da die Aufsichtsbehörden erst im Rahmen der Bewertung der Sicherheitsmängel beteiligt werden, wird ihre Rolle in dieser Orientierungshilfe nicht weiter betrachtet.

1.5 Nachweisdokument

Gegenüber dem BSI wird die Erfüllung der Anforderungen aus § 8a (1) BSIG durch ein Nachweisdokument belegt. Damit das BSI die Eignung der Prüfung, die Angemessenheit und Wirksamkeit der Vorkehrungen zur Vermeidung von Störungen sowie die Schwere der aufgedeckten Sicherheitsmängel bewerten kann, sollte das Nachweisdokument die nachfolgend aufgeführten Informationen enthalten.

Das BSI stellt Formulare[7] bereit, in denen die Betreiber die Information übermitteln können, die zum Nachweis erforderlich sind. Diese Formulare umfassen die folgenden Blätter:

- Blatt KI: Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner

6 § 8a (3) BSIG

7 Das Nachweisdokument mit den Blättern befindet sich auf den Webseiten des BSI unter www.bsi.bund.de/Nachweise .

- Blatt PS: Angaben zur Eignung der prüfenden Stelle und zum Prüfteam
- Blatt PD: Angaben zur Prüfdurchführung
- Blatt PE: Angaben zum Prüfergebnis und zu den aufgedeckten Sicherheitsmängeln

Das Blatt KI ist vom KRITIS-Betreiber auszufüllen und zu unterschreiben. Es bildet zusammen mit den Blättern PS, PD und PE, die von der prüfenden Stelle auszufüllen und zu unterschreiben sind, das Nachweisdokument. Es wird vom KRITIS-Betreiber an das KRITIS-Büro des BSI gesandt.

2 Der Betreiber

Der Betreiber muss die Umsetzung der Anforderungen gemäß § 8a (1) BSIG (angemessene Vorkehrungen zur Vermeidung von Störungen unter Berücksichtigung des Stands der Technik) für seine Anlagen gewährleisten. Dazu muss er zunächst einen geeigneten Scope festlegen und die zugrundeliegenden Prozesse feststellen und dann entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren.

Zum objektiven Nachweis der Umsetzung der Maßnahmen muss er anschließend eine geeignete prüfende Stelle beauftragen, die eine Prüfung (Audit, Prüfung oder Zertifizierung) durchführt und dem Betreiber die Ergebnisse in einem Prüfbericht unter Auflistung der aufgedeckten Sicherheitsmängel übermittelt.

Im nächsten Schritt reicht der KRITIS-Betreiber dann mindestens alle zwei Jahre das Nachweisdokument (siehe Abschnitt 1.5) beim BSI ein. Nachweisdokumente sind dabei für jede Anlage gemäß BSI-Kritisverordnung separat einzureichen.

In diesem Abschnitt werden folgende Fragen beantwortet:

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

2.1 Beschreibung des Prüfgegenstandes (Scope)

Eine geeignete Prüfung muss als Prüfgegenstand den vollständigen Scope[8] der Kritischen Infrastruktur, also der Anlage gemäß BSI-KritisV, umfassen. In Vorbereitung auf die Prüfung sollte der Scope daher genau definiert und beschrieben werden[9]. Die Vollständigkeit der zugrundeliegenden Informationen bestätigt der Betreiber in Blatt KI. Zusätzlich sind wesentliche Punkte dieser Beschreibung später auch im Blatt PD des Nachweisdokuments aufzunehmen.

8 Scope siehe auch Kapitel 7 Glossar
9 Weitere Information finden sich in der Orientierungshilfe zum B3S, Kapitel 1: Geltungsbereich

Für die Prüfungsdurchführung und das Nachweisdokument sollten

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

beschrieben werden.

Für die Prüfungsdurchführung sollen zudem alle

- informationstechnischen Systeme,
- Komponenten,
- Prozesse und
- Rollen bzw. Personen

aufgeführt werden, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur erforderlich sind oder deren Funktionsfähigkeit beeinflussen (können).

2.2 Übliche Sicherheitsdokumentation

Damit das Prüfteam die Prüfung nach § 8a (3) BSIG ordnungsgemäß durchführen kann, benötigt es der Erfahrung nach einerseits konkrete Unterlagen und andererseits die Möglichkeit einer Vor-Ort-Prüfung mit Inaugenscheinnahme von Technik sowie der Möglichkeit zu Gesprächen mit Mitarbeitern des Betreiber (siehe hierzu auch Kapitel 5).

Für die Dokumentenprüfung sollten Betreiber dem Prüfer z. B. folgende Dokumente bereitstellen[10]:

- Konzept und Dokumentation des Risikomanagements inkl. Risikoanalyse
- 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)

10 Die Orientierungshilfe zum B3S gibt weitere Informationen zu den benötigten Dokumenten.

- Konzepte und Dokumentation von Überprüfungen (z. B. Prüfberichte der internen Revision sowie anderer durchgeführter Audits, Übungen, systematische Log-Auswertungen usw.)
- Richtlinien zur externen Informationsversorgung
- Richtlinien zum Umgang mit Lieferanten und Dienstleistern (z. B. Service Level Agreements und andere die Sicherheit betreffende Vereinbarungen mit Dienstleistern)
- Sicherheitskonzept (inkl. Darstellung umgesetzter und geplanter Maßnahmen), insbesondere der branchenspezifischen Maßnahmen.

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

Die o. g. Dokumente benötigt das Prüfteam. Das BSI kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen.

2.3 Wahl der Prüfgrundlage

Der Betreiber wählt in Abstimmung mit der prüfenden Stelle die Prüfgrundlage. Dabei können folgende Fälle unterschieden werden, die in Abschnitt 5.1 bzgl. der Durchführung von Prüfungen genauer beschrieben werden:

- Prüfung auf Grundlage eines vom BSI anerkannten 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)

Der Betreiber hat die Möglichkeit, der prüfenden Stelle bereits vorhandene Prüfgrundlagen zur Verfügung zu stellen. Die prüfende Stelle entscheidet, ob und zu welchem Grad diese in die Prüfung einfließen können.

3 Die prüfende Stelle

Eine prüfende Stelle ist eine „geeignete“ Institution, die vom KRITIS-Betreiber beauftragt wird festzustellen, ob der Betreiber wirksame und angemessene Vorkehrungen zur Vermeidung von Störungen gemäß § 8a (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 Kapitel 4 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)

In einem B3S kann jede Branche konkretisieren, welches Anforderungsniveau an die prüfende Stelle erforderlich ist bzw. ausreicht, und dabei ggf. zusätzliche branchenspezifische Anforderungen an die prüfende Stelle festlegen.

3.1 Aufgaben

Aufgabe der prüfenden Stelle ist es,

- die Einhaltung der Prozesse und Verfahren festzustellen,
- für einheitliche und gleichwertige Prüfungsdurchführung und Prüfergebnisse Sorge zu tragen,
- die Qualitätsprüfung vorzunehmen,
- Rahmenbedingungen für die Prüfdurchführung festzulegen (Prüfverfahren usw.),
- das Prüfteam zusammenzustellen und die Abdeckung aller Kompetenz-bereiche sicherzustellen
- die Eignung der Prüfer zu bestätigen sowie
- die Kommunikation mit dem 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 Betreiber.

3.2 Eignung

Grundsätzlich können interne Revisoren, Auditoren, Wirtschaftsprüfer oder andere geeignete Stellen Prüfungen gemäß § 8a (3) BSIG vornehmen, sofern die Einhaltung der Anforderungen an die prüfenden Stellen gewährleistet ist (siehe auch Abschnitt 6.2 im Anhang).

Dies sind vor allem:

- Die Prüfung wird unabhängig, unparteilich, neutral und weisungsfrei durchgeführt. Die Einhaltung der ethischen Grundsätze (siehe Abschnitt 6.1 im Anhang) ist sichergestellt.
- Die erforderlichen Prozesse (z. B. Qualitätssicherungsverfahren, Prüfprozess) müssen eingeführt, umgesetzt und in Konzepten dokumentiert 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.

Damit die Qualität der Prüfergebnisse vergleichbar ist, sollten die Prüfungen 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.

Eine prüfende Stelle kann als geeignet angesehen werden, wenn sie gegenüber dieser unabhängigen Instanz ihre Neutralität und Eignung nachgewiesen hat.

3.3 Übersicht über 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)[11] bzw. DIIR-Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ (DIIR)[12] (Abschnitt 3.3.3) oder
- eine Zulassung als Wirtschaftsprüfer bei der IDW, verbunden mit einer Erklärung, dass die Anforderungen aus Abschnitt 3.3 und Abschnitt 6.1 im Anhang erfüllt sind (Abschnitt 3.3.4).

Sofern keine prüfende Stelle zur Verfügung steht, die unter die zuvor genannten oder vergleichbare Akkreditierungsregime fällt, ist im Ausnahmefall und nach Rücksprache mit dem BSI auch ein individueller Nachweis der Eignung einer prüfenden Stelle durch Selbsterklärung gegenüber dem BSI möglich (Abschnitt 3.3.5).

Zusätzlich sollte nachgewiesen werden, dass das Prüfteam über alle Kompetenzen (siehe Kapitel 4) verfügt.

In den folgenden Unterabschnitten werden die Qualifikationen genauer beschrieben.

3.3.1 Akkreditierte Zertifizierungsstellen der DAkkS

Im Rahmen eines ISO/IEC 27001-Zertifizierungsverfahrens übernimmt die DAkkS 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 Internetseite der Deutschen Akkreditierungsstelle (DAkkS) abgerufen werden.

3.3.2 Zertifizierte IT-Sicherheitsdienstleister oder anerkannte Prüfstellen des BSI

Darüber hinaus bietet das BSI eine Zertifizierung von IT-Sicherheitsdienstleistern an. Grundvoraussetzung für die Anerkennung als Prüfstelle oder Zertifizierung als IT-Sicherheitsdienstleister ist die Erfüllung der Anforderungen der DIN EN ISO/IEC 17025:2005.

11 http://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2015_Standards_V3.pdf
12 http://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr_3.pdf

Das Verfahren der Zertifizierung bzw. Anerkennung von Stellen ist in einer veröffentlichten Verfahrensbeschreibung festgelegt, die ein Begutachtungskatalog ergänzt [13].

Dabei kann eine Stelle für folgende Geltungsbereiche einen Antrag stellen:

- CC-Prüfstellen,
- TR-Prüfstellen,
- IT-Sicherheitsdienstleister: IS-Revision und IS-Beratung,
- IT-Sicherheitsdienstleister: Penetrationstester,
- Digitalfunk BOS oder
- Lauschabwehr im Bereich Wirtschaft.

Diese Stellen erfüllen damit geeignete Qualitätsansprüche. Auf der Website des BSI findet sich eine Liste von Prüfstellen bzw. IT-Sicherheitsdienstleistern, die durch das BSI anerkannt bzw. zertifiziert sind und damit die Voraussetzung einer ordnungsgemäßen Prüfung erfüllen.

3.3.3 Interne Revisoren

Interne Revisoren 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[14]-Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ und die IIA-Standards 1300ff zu Grunde[15].

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

- 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 sind sichergestellt.
- 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.

13 https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html
14 DIIR: Deutsches Institut für Interne Revision
15 http://www.diir.de/zertifizierung/quality-assessment/

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.[16]

3.3.4 Wirtschaftsprüfungsinstitutionen

Aufgrund der hohen Verantwortung, die ein Wirtschaftsprüfer übernimmt, erfüllt er die besonderen Berufspflichten, die in der Wirtschaftsprüferordnung (WPO)[17] zusammengefasst sind. Dies sind u. a. Unabhängigkeit, Verschwiegenheit und berufswürdiges Verhalten. Die meisten Wirtschaftsprüfungen in Deutschland werden von den „Big Four Wirtschaftsprüfungsgesellschaften“ durchgeführt. Wirtschaftsprüfungsunternehmen, die bei der IDW registriert sind, können gegenüber dem BSI eine Selbsterklärung[18] abgeben, dass die Aufforderungen aus Abschnitt 6.1 im Anhang erfüllt sind.

3.3.5 Selbsterklärung gegenüber dem BSI

Ein Betreiber kann die Neutralität und Eignung einer prüfenden Stelle, d. h. die Erfüllung der Anforderung gemäß Anhang 6.2, direkt beim BSI nachweisen. Die Qualität der Prüfung muss vergleichbar mit Zertifizierungsstellen nach ISO/IEC 17021 und ISO/IEC 27006 oder anderen einschlägigen Standards sein. Hierzu ist mit dem BSI Kontakt aufzunehmen. Das BSI überprüft anhand einer formellen Selbsterklärung der prüfenden Stelle, ob diese aus Sicht des BSI geeignet ist.

Das BSI bestätigt nach positiver Sichtung der Selbsterklärungsunterlagen die Eignung der prüfende Stelle für die beabsichtigte Prüfung, behält sich aber vor, Stichproben bei der Umsetzung der Anforderungen durchzuführen.

4 Das Prüfteam

Seitens der prüfenden Stelle wird ein Prüfteam mit der konkreten Prüfung bei einem KRITIS-Betreiber beauftragt.

Das Prüfteam sollte alle zur Erbringung geeigneter Nachweise erforderlichen Anforderungen erfüllen und über die hierfür erforderliche Kompetenz verfügen. Insbesondere sollte ein Prüfteam in der Regel aus mindestens zwei qualifizierten Mitarbeitern bestehen (Teamleiter und Prüfer). 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 sollten die im Abschnitt 6.1 „ethische Grundsätze“ des Anhangs aufgeführten Grundsätze befolgen.

16 siehe http://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2015_Standards_V3.pdf
17 siehe www.wpk.de/pdf/wpo.pdf
18 siehe Abschnitt 3.3.5

4.1 Aufgaben

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

Dabei kann diese Prüfung

- als eine Einzelprüfung einer geeigneten (internen oder externen) prüfenden Stelle

oder als Zusatzprüfung z. B. im Rahmen

- eines internen ISMS-Audits durch interne, unabhängige IS-Revisoren (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 (Third-Party-Audit)

durchgeführt werden.

4.2 Eignung

Damit die Prüfer geeignete Prüfungen und damit geeignete Nachweise zur Erfüllung der gesetzlichen Anforderungen erbringen können, sollten sie über Kompetenzen in den folgenden Bereichen verfügen:

- Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG,
- Audit-Kompetenz,
- IT-Sicherheits-Kompetenz bzw. Informationssicherheits-Kompetenz,
- Branchen-Kompetenz.

Abbildung 2 zeigt, welche Themengebiete in den einzelnen Kompetenzbereichen mindestens vorhanden sein sollten.

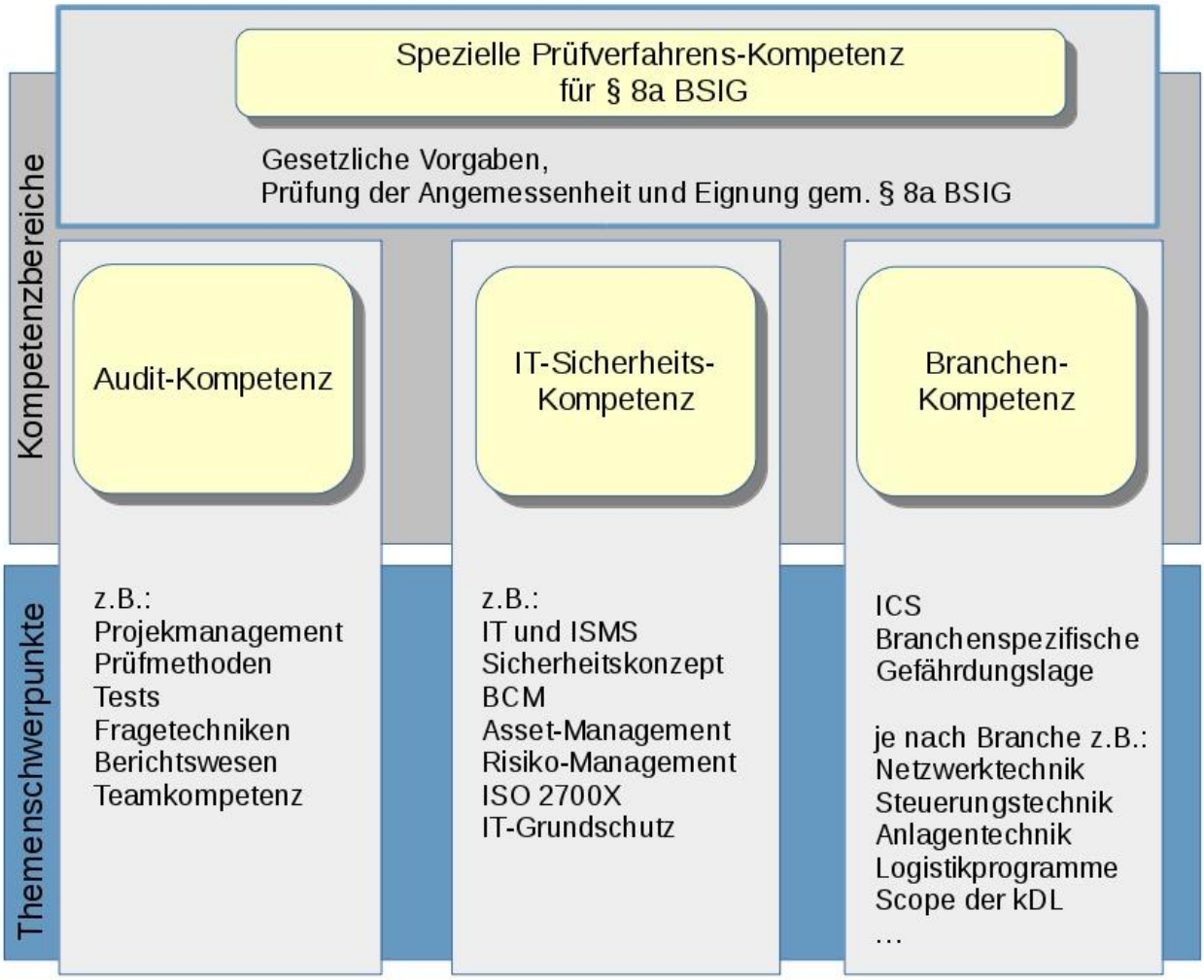

Abbildung 2: Themen der Kompetenzbereiche , Quelle: BSI

Tabelle 1 gibt eine Übersicht über typische Qualifikationen, über die geeignete Prüfer verfügen sollten.

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

4.3 Nachweis der Eignung

Sofern die erforderlichen Kompetenzen, nicht bei den Prüfern selbst vorliegen, sollte in das Prüfteam ein Fachexperte mit den entsprechenden Kenntnissen aufgenommen werden.

Anforderungen	Erläuterung	Nachweis
Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG		
Spezielle Prüfverfahrenskompetenz	Teilnahme an 2-3-tägiger Zusatzqualifikation „spezielle Prüfverfahrens-Kompetenz für § 8a BSIG“ sowie bestandene Prüfung[19] oder *gleichwertiger Kompetenznachweis*	Bestätigung der erfolgreichen Teilnahme und Prüfungszeugnis / Zertifikat über die bestandene Prüfung *oder* *Erklärung mit nachvollziehbarem Nachweis der gleichwertigen Prüfverfarenskompetenz*
Audit-Kompetenz		
Alternative 1	Innerhalb der letzten 3 Jahre verantwortliche Beteiligung an mindestens 4 Erstparteien-Audits oder Zweitparteien-Audits inkl. IT-Anteil im Gesamtaufwand von insgesamt 30 PT	Vom Auftraggeber / Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate
Alternative 2	Innerhalb der letzten 3 Jahre Beteiligung an Zertifizierungen im Umfang von insgesamt mindestens 30 PT davon können max. 10 PT auch durch zwei Beteiligungen an Prüfungen als Fachexperte abgedeckt werden.	Vom Auftraggeber / Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate
IT-Sicherheits-Kompetenz		
IT-Sicherheit / Informationssicherheit	In den letzten 8 Jahren mindestens 5 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich IT-/Informationssicherheit.	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten
Branchen-Kompetenz		
Branchenkenntnisse	In den letzten 5 Jahren mindestens 3 Jahre Branchenerfahrung im zu prüfenden Scope (kann durch Aufnahme eines Fachexperten in das Prüfteam erfüllt werden)	Zeugnis / Bescheinigungen eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten

Tabelle 1: Empfohlene Kompetenzen der Prüfer

19 Das BSI hat zusammen mit Schulungsanbietern ein ein Schulungskonzept erarbeitet, das Schulungen gemäß der „speziellen Prüfverfahrens-Kompetenz für § 8a BSIG“ ermöglicht.

4.4 Aufrechterhaltung der Kompetenz

Die Prüfer und die prüfende Stelle sollten ihre Fachkompetenz kontinuierlich durch den Austausch mit anderen Fachexperten aufrechterhalten.

Regelmäßig stattfindende „Erfahrungsaustausch-Tage“ der Branchenverbände oder des BSI sollen den prüfenden Stellen und den Prüfern die Möglichkeit geben, sich über aktuelle Entwicklungen zu informieren und Erkenntnisse auszutauschen und zu diskutieren. Zur Aufrechterhaltung der„Speziellen Prüfverfahrenskompetenz zu § 8a BSIG“ wird eine Teilnahme an mindestens einer eintägigen Veranstaltung jährlich empfohlen.

5 Durchführung der Prüfung

Das folgende Kapitel beschreibt, was bei der Durchführung der Prüfung beachtet werden sollte. Hieran sind 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 5.7)

5.1 Prüfgrundlage

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

5.1.1 Prüfgrundlage bei Umsetzung eines B3S nach § 8a (2) BSIG

Wenn ein branchenspezifischer Sicherheitsstandard (B3S)[20] mit Eignungsfeststellung des BSI für den jeweiligen Geltungsbereich vorliegt und dieser vom Betreiber bei der Umsetzung von Maßnahmen angewendet wurde, sollte dieser als Prüfgrundlage herangezogen werden. Ein B3S beinhaltet sowohl den Geltungsbereich (Scope) als auch die Mindestanforderungen der umzusetzenden Maßnahmen und i. Allg. auch Vorgaben an die prüfende Stelle. Der Betreiber muss die Vorgaben des B3S sinngemäß auf seine Anlagen anpassen und einen Umsetzungsplan festlegen.

20 Siehe auch: https://www.bsi.bund.de/Stand-der-Technik

Eine Liste aller B3S, deren Eignung vom BSI festgestellt wurde, findet sich auf der Website des BSI[21]. Die Ersteller der B3S sind nicht verpflichtet, den B3S ganz oder in Teilen zu veröffentlichen, da dieser Eigentum des Erstellers ist. Das Ergebnis der Eignungsfeststellung eines B3S und zugehörige Metadaten werden vom BSI veröffentlicht. Mit Zustimmung der Ersteller veröffentlicht das BSI auch Angaben zu in der Erstellung befindlichen B3S und wirkt bei der Verbreitung mit[22].

5.1.2 Prüfung ohne Umsetzung eines B3S

Liegt kein B3S vor oder soll die Prüfung unabhängig von einem B3S erfolgen, muss sichergestellt werden, dass die Anforderungen nach § 8a (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 dokumentierten. Dieses Prüfverfahren dient dann als Prüfgrundlage.

Anhaltspunkte für ein geeignetes Prüfverfahren können sein:

- die Orientierungshilfe zu branchenspezifischen Sicherheitsstandards (B3S) nach § 8a (2) BSIG
- andere B3S gemäß § 8a (2) BSIG, deren Eignung vom BSI festgestellt wurde (der Scope ist zu beachten!)
- 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 Prüfungen bei der Erbringung des Nachweises berücksichtigt werden, d. h. es besteht die Möglichkeit, für § 8a (3) BSIG erforderliche Prüfaspekte im Rahmen anderer Prüfungen abzudecken. Dabei müssen die Prüfungen aktuell sein, d. h. sie dürfen zum Zeitpunkt der Einreichung beim BSI nicht älter als ein Jahr sein. Ältere Nachweise 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 Scope 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“, wobei gleichwertige Ansätze denkbar sind.

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

21 ebd.
22 ebd.

Hinweis zu ISO/IEC 27001-Zertifizierungen [23]:

Bei einer reinen ISO/IEC 27001-Zertifizierung ist nicht von vornherein klar, dass Scope und Maßnahmen geeignet sind. Deswegen reicht diese alleine nicht aus; wichtige Schutzziele für kritische Dienstleistungen könnten dabei theoretisch unberücksichtigt bleiben.

Wer eine ISO/IEC 27001-Zertifizierung nachweist, im Rahmen der Umsetzung Risiken nur im Ausnahmefall akzeptiert hat und zusätzlich nachweist, dass Scope und Maßnahmen geeignet sind seine kritischen Dienstleistungen ausreichend zu schützen (inkl. ggü. ISO/IEC 27001 zusätzlicher Anforderungen zum Schutz der Kritischen Infrastruktur), hat damit die Voraussetzungen zur Erfüllung der Anforderungen gemäß § 8a (1) und (3) BSIG geschaffen.

Ein möglicher Weg ist, einen B3S zu erstellen, der in Ergänzung zu einem ISO-Standard die notwendigen zusätzlichen Regelungen gemäß der Orientierungshilfe B3S vornimmt und dokumentiert. Nach einer Eignungsprüfung durch das BSI liefert dieser dem Betreiber ein verlässliches Regelwerk für die Umsetzung und Prüfung des Stands der Technik.

5.2 Prüfthemen und Prüfung des Scopes

Die Prüfthemen sind im B3S i. Allg. konkret beschrieben, insbesondere sind dort branchenspezifische Anforderungen und/oder Maßnahmen aufgeführt, deren Umsetzung sichergestellt werden müssen.

Liegt kein B3S vor bzw. wird zur Prüfung kein B3S verwendet, lassen sich die Prüfthemen aus der Orientierungshilfe zur Erstellung eines B3S ableiten. Der Anhang A3 liefert Prüfthemen, die zu berücksichtigen sind.

Insbesondere die Überprüfung, ob der Scope richtig gewählt wurde, ist für die Eignung des Nachweises sehr wichtig. Der Prüfer muss sich hierzu die Prüffrage stellen: „Wie ist sichergestellt, dass die Wahl des Scopes korrekt ist? Umfasst er vollständig die informationstechnischen Systeme, Komponenten und Prozesse, die zur Kritischen Infrastruktur gehören, sowie diejenigen, die auf die Kritische Infrastruktur Einfluss haben?“

Dabei ist der Scope unter dem Prüfaspekt

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

zu bewerten und zu überprüfen.

Die Prüfung der Eignung des Scopes im Sinne von § 8a (3) BSIG ist Teil des Prüfergebnisses und wird von der prüfenden Stelle immer geprüft und ausdrücklich bestätigt.

Anmerkung:

Grundsätzlich ist es sinnvoll, dass die prüfende Stelle gemeinsam mit dem zu prüfenden Betreiber bereits vor Beauftragung den Scope der Prüfung klärt und dass die prüfende Stelle die Aufwandsabschätzung und das Angebot für die Prüfung auf dieser Grundlage erstellt.

23 Siehe auch „Häufige Fragen und Antworten (FAQ) zu § 8a BSIG im Rahmen der Orientierungshilfe B3S: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/B3S_FAQ.pdf

5.3 Mögliche Prüfmethoden

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

- 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
- Einbeziehung bestehender Nachweise (z. B. Prüfung des Prüfberichts einer in anderem Kontext vorgenommenen Prüfung; vorhergehende ISO 27001-Zertifikate. 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 Prüfaufwandes bei der Erstprüfung fließen z. B. ein:

- die Größe des zu prüfenden Scopes, gemessen an der Anzahl der Mitarbeiter der Organisation,
- die Kritikalität bzw. der Versorgungsgrad gemäß BSI-KritisV,
- die Komplexität des zu prüfenden Scopes,
- die IT-Abhängigkeit bzw. die IT-Durchdringung der kritischen Dienstleistung sowie
- die Frage, ob im Rahmen der Prüfung ein Penetrationstest durchgeführt werden muss – dies wird i. d. R. dann der Fall sein, wenn der Betreiber solche Tests nicht ohnehin 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 (Scope)?
- 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 Betreiber Kritischer Infrastrukturen stark unterscheiden.

Anmerkung:

Jede Branche kann in einem B3S einen angemessenen Prüfaufwand festlegen.

Jede Prüfung sollte die in Tabelle 2 folgenden sechs Prüfschritte abdecken. Der Zeitanteil ist eine Empfehlung und dient als Beispiel, das eine Orientierung für die Prüftiefe der einzelnen Prüfschritte geben soll.

Phase	Tätigkeit	Zeitanteile
Schritt 1	Vorbereitung der Prüfung sowie Prüfung der Eignung des Scopes	5 %
Schritt 2	Erstellung des Prüfplans	5 %
Schritt 3	Dokumentenprüfung	25 %
Schritt 4	Vor-Ort-Prüfung	55 %
Schritt 5	Nachbereitung der Vor-Ort-Prüfung	5 %
Schritt 6	Erstellung des Prüfberichtes	5 %

Tabelle 2: Orientierung zum relativen Zeitaufwand bei der Durchführung einer Prüfung als Nachweis der Umsetzung der Anforderungen § 8a (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 werden die Rollen im Prüfteam und die benötigten Ansprechpartner beim Betreiber sowie die zeitlichen Abläufe festgeschrieben.

Eine komplette Prüfung des gesamten Scopes 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 Kritischen Infrastruktur, aber auch netztopologische Abdeckung erzielt wird. Bereiche mit höheren Risiken sollen stärker berücksichtigt werden. In die Risikobetrachtung sollte insbesondere auch die Auswirkung auf die Versorgung durch die kritische Dienstleistung (Wie viele Menschen wären von einem Ausfall betroffen? Wie gravierend wäre eine Störung/ein Ausfall?) entsprechend der Größe des Betreibers einbezogen werden. 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 zulässig. 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 als Nachweis gemäß § 8a (3) BSIG über die Umsetzung der Anforderungen nach § 8a (1) BSIG soll

- ein eigenständiges Dokument sein.
- in deutscher Sprache[24] verfasst werden, alle Inhalte müssen nachvollziehbar sein.
- eine eindeutige Bezeichnung , Versionsverwaltung und Änderungshistorie haben.
- alle für die Bewertung relevanten Metainformationen enthalten (z. B. Scope 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.

24 Die Prüfberichte können auch in englischer Sprache verfasst werden. Die Nachweisdokumente müssen dem BSI jedoch in deutscher Sprache vorgelegt werden.

5.7 Sicherheitsmängel, Nicht-Konformitäten und Mängelkategorien

Die festgestellten Sachverhalte zu jeder geprüften Maßnahme sind im Prüfbericht aufzunehmen und hinsichtlich des Umsetzungsstatuses zu bewerten. Wird eine Abweichung zu den Anforderungen gemäß § 8a (1) BSIG festgestellt, handelt es sich um einen Mangel, der zu dokumentieren und 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 aufzunehmen.

Die geplante Nachverfolgung, zu ergreifende Maßnahmen und die Frist zur Beseitigung der Sicherheitsmängel sollen festgelegt und überwacht werden. Hierfür sollten Mängelkategorien definiert und im gesamten Prüfbericht einheitlich verwendet werden. 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 3 festgelegten Kategorien abbilden.

Kategorie	Definition	Prüfbericht / Mängelliste
Schwerwiegende oder erhebliche Abweichung bzw. 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 oder die Verfügbarkeit der kDL stark gefährdet ist und erheblicher Schaden zu erwarten ist.	Aufnahme in den Prüfbericht und Aufnahme in das Nachweisdokument
Geringfügige Abweichung bzw. Sicherheitsmangel	Eine „ geringfügige Abweichung“ stellt eine Gefährdung bzw. ein Risiko dar. Es besteht kein akuter Handlungsbedarf. Die zugrunde liegende Abweichung muss mittelfristig beseitigt werden. Die Vertraulichkeit, Integrität oder Verfügbarkeit der kDL kann beeinträchtigt werden.	Aufnahme in den Prüfbericht und Aufnahme in das Nachweisdokument
Empfehlung	Eine „Empfehlung“ stellt einen Verbesserungshinweis dar. Durch die Umsetzung der Empfehlung kann die Sicherheit erhöht werden.[25] Empfehlungen können -Verbesserungsvorschläge für die Umsetzung von Maßnahmen sein, - ergänzende Maßnahmen sein, die sich in der Praxis bewährt haben, oder - Kommentare hinsichtlich der Angemessenheit und Wirksamkeit von Maßnahmen sein.	Aufnahme in den Prüfbericht empfohlen keine Aufnahme in das Nachweisdokument notwendig
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.	keine Aufnahme in das Nachweisdokument notwendig

Tabelle 3: Mängelkategorien

Neben dem Gesamtvotum ist das einheitliche Verständnis von einzelnen Abweichungen für die Bewertung der Mängel zwingend erforderlich. Wird ein Sicherheitsmangel als schwerwiegende Abweichung bewertet, so sind die Ursachen zu analysieren und nachvollziehbar zu dokumentieren.

25 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 Daten zu rechnen ist.

6 Anhang

6.1 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 Vertraulichkeit:** 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 und die Prüfungsergebnisse dokumentieren können. Jedes Prüfteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei Prüfern bestehen („4-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.

6.2 Anforderungen an prüfende Stellen

Sofern eine prüfende Stelle nicht einem anerkannten Akkreditierungsregime unterliegt und deren Eignung im Ausnahmefall[26] über eine Selbsterklärung erfolgen soll, muss diese prüfende Stelle im Rahmen einer Selbsterklärung zumindest nachweisen, dass sie

- unabhängig und unparteilich, neutral und weisungsfrei die Prüfung nach einem dokumentierten Prüfverfahren bzw. Prüfprozess durchführt. Das einheitliche Verständnis von Abweichungen ist für die Bewertung der Mängel zwingend erforderlich. Wird ein Sicherheitsmangel als schwerwiegende Abweichung bewertet, so sind die Ursachen zu analysieren und nachvollziehbar zu dokumentieren.
- erforderliche Prozesse eingeführt, umgesetzt und in Konzepten dokumentiert hat:
  - Qualitätssicherungsverfahren,
  - Informationssicherheitsmanagementsystem (ISMS),
  - Archivierungs- und Backupkonzept,
  - Dokumentations- und Aufzeichnungsverfahren,
  - definierter Prüfprozess,
- ausreichende Ressourcen und geeignete Infrastruktur zur Verfügung stellt:
  - mindestens über einen hauptamtlich tätigen Leiter der prüfenden Stelle und einen Stellvertreter verfügt,
  - Prüfungsverfahren in einer vertretbaren Zeit (höchstens sechs Monate) durchführt,
  - sichere Infrastruktur, Systeme, Anwendungen und eine sichere Netzwerkstruktur nachweisen kann,
- über einen festgelegten Prozess zur Ermittlung der Kompetenz der an der Durchführung von Prüfungen beteiligten Personen bzw. Prüfteams verfügen, hierfür sind folgende Kompetenzen mindestens erforderlich:
  - belastbares Wissen im Bereich der Informationssicherheit,
  - technisches Wissen im Bereich der Erbringung der kritischen Dienstleistungen der geprüften Betreiber,
  - belastbares Wissen im Bereich Managementsysteme und insbesondere Informationssicherheitsmanagementsysteme (ISMS),
  - notwendige Kenntnisse und Erfahrungen in der Durchführung von Prüfungen im Sinne § 8a (3) BSIG,

26 Die Abgabe einer Selbsterklärung einer prüfenden Stelle ist nur auf Antrag eines Betreibers und nach Absprache mit dem BSI möglich.

- detaillierte Kenntnisse der Anforderungen an Prüfungen nach § 8a (3) BSIG (vgl. u. a. diese Orientierungshilfe),
- vertrauliche Informationen („Kenntnis, nur wenn nötig“, Verschwiegenheit (NDA), Betriebsgeheimnisse, Aufbewahrung vertraulicher Dokumente) angemessen schützt und die „ethischen Grundsätze“ einhält (siehe Abschnitt 6.1: „Ethische Grundsätze“),
- bei einer Unterbeauftragung durch Verifikation sicherstellt, dass externe Dienstleister die gleichen Anforderungen erfüllen (Unabhängigkeit, Ressourcen, Fachkunde, „ethische Grundsätze“ etc.).

6.3 Nachweisdokument (Formulare)

Die als Nachweisdokument zur Verwendung vorgesehenen Formulare sind auf der Website des BSI unter www.bsi.bund.de/Nachweise veröffentlicht.

7 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-Kritisverordnung
Betreiber	Ein Unternehmen, das eine Kritische Infrastruktur gemäß Rechtsverordnung nach § 10 (1) BSIG (BSI-KritisV) betreibt.
Branchenspezifischer Sicherheitsstandard (B3S)	Sicherheitsstandard, dessen Eignung nach § 8a (2) BSIG festgestellt wurde (siehe Anerkennungsverfahren).
Drittparteien-Audits	Audits, die von externen unabhängigen Organisationen durchgeführt weden. Solche Organisationen bieten die Zertifizierung oder Überprüfung der Konformität mit Anforderungen.
Erstparteien-Audit	Manchmal auch Interne Audits, genannt, werden von oder im Namen der Organisation selbst für interne Zwecke durchgeführt und können die Grundlage für die eigene Konformitätserklärung der Organisation bilden.
Gefundene Sicherheitsmängel	Im Rahmen der Prüfung gefundene, nicht oder nur teilweise umgesetzte notwendige Maßnahmen. Gefundene Sicherheitsmängel sind entsprechend mit „Schweregraden“ zu versehen (siehe Bewertungsschema).
Geltungsbereich / Scope	Bereich, den ein Branchenspezifischer Sicherheitsstandard abdeckt (siehe auch unter „Prüfgegenstand / Scope“).
Kompetenz	Angelernte Fähigkeit, die die Ausübung einer bestimmten Tätigkeit ermöglicht.
Kritische Infrastruktur	s. Definition im BSIG bzw. Konkretisierung in der BSI-Kritisverordnung
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 (1) BSIG. Zu diesen Vorkehrungen gehören auch infrastrukturelle und personelle Maßnahmen. Besonders kritische Prozesse bedürfen besonderer Sicherheitsmaßnahmen.
Nachweis	Bescheinigung eines unabhängigen Dritten über die Einhaltung eines angemessenen Sicherheitsniveaus durch den Betreiber. Die Umsetzung der angemessenen und wirksamen Maßnahmen kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Begriff	Definition
Nachweisdokument	Eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie der zur Bearbeitung erforderlichen Informationen.
Prüfbericht	Dokument der prüfenden Stelle, das die gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse enthält.
Prüfende Stelle	Institution, die den Nachweis erbringt, dass der Betreiber die Maßnahmen gemäß § 8a (1) BSIG umgesetzt hat.
Prüfgegenstand / Scope	Der Prüfgegenstand / Scope umfasst die informationstechnischen Systeme, Komponenten und Prozesse, Rollen bzw. Personen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind bzw. auf diesen Einfluss haben. (siehe auch unter „Geltungsbereich / Scope“)
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.
Prüfung	Geeigneter Nachweis der Umsetzung der Maßnahmen beim Betreiber. Sie wird durch unabhängige und qualifizierte Prüfer einer prüfenden Stelle durchgeführt. Unter Prüfungen versteht man Audits, Prüfungen und Zertifizierungen gemäß § 8a (3) BSIG.
Prüfverfahren	Methode, nach der die prüfende Stelle die Nachweise erbringt.
Überwachende Stelle	Organisation, die die Aufsichtsfunktion über eine prüfende Stelle ausübt.
Zweitparteien-Audits	Audits, die von Parteien, die ein Interesse an der Organisation haben, wie z. B. Kunden, oder von Personen im Namen dieser Parteien durchgeführt werden.