Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anforderungen nach § 8a Absatz 5 BSIG

Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)

Änderungshistorie

Version	*Datum*	*Verfasser*	*Beschreibung*
1.0	08.05.2023	BSI	Finale Version nach Anhörung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6166
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: www.bsi.bund.de/datenschutz
© Bundesamt für Sicherheit in der Informationstechnik 2023

Inhalt

1 Grundlage

Das Bundesamt kann gemäß § 8a Absatz 5 des BSI-Gesetzes (BSIG) zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach § 8a Absatz 3 BSIG Anforderungen

- an die Art und Weise der Durchführung (D)
- an die hierüber auszustellenden Nachweise (N)
- sowie weitere fachliche und organisatorische Anforderungen an die prüfende Stelle (P)

nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

In diesem Dokument nimmt das BSI die Festlegung solcher Anforderungen vor. Die Anforderungen sind zur besseren Orientierung mit Kennungen versehen, die eine erste Zuordnung nach Durchführung (D), Nachweise (N), Prüfende Stelle (P) ermöglichen. Die Anforderungen sind in allgemeine praktische Themenbereiche gegliedert. Die Themenbereiche sind in der Kennung der einzelnen Anforderungen festgehalten (z. B. „DG“ für Dokumentation des Geltungsbereichs, dann N.DG.01).

Die in diesem Dokument aufgeführten Anforderungen sind verpflichtend für die ordnungsgemäße Umsetzung der §§ 8a ff. BSIG. Für eine geeignete Nachweiserbringung hat der Betreiber ihre Erfüllung sicherzustellen. Soweit sie Regelungsbereiche betreffen, zu denen das BSI weitere Vorgaben in anderen Dokumenten veröffentlicht hat, ergänzen sich die bestehenden Regelungen. Im Falle einer inhaltlichen Überschneidung gilt die speziellere Regel (üblicherweise die sektorspezifische Vorschrift). Bei Feststellung einer inhaltlichen Überschneidung oder einer möglichen Unanwendbarkeit einer Regelung ist das BSI unverzüglich zu informieren und der Einzelfall zur Entscheidung vorzulegen, um eine rechtssichere Auslegung herbeizuführen. Eine spätere Berufung auf die Unsicherheit ist nicht möglich.

2 Prüfende Stelle und Prüfer

2.1 Unabhängigkeit der prüfenden Stelle und Prüfer

P.UP.01 Die prüfende Stelle muss gegenüber dem Betreiber der zu prüfenden KRITIS-Anlage bzw. des zu prüfenden KRITIS-Anlagenteils unternehmensfremd sowie rechtlich und wirtschaftlich unabhängig sein. Insbesondere sind damit Stellen untauglich, die über geteilte Unternehmens- oder Konzernstrukturen mit dem Betreiber verbunden sind.

P.UP.02 Die Mitglieder des Prüfteams müssen gegenüber dem Betreiber der zu prüfenden KRITIS-Anlage bzw. des zu prüfenden KRITIS-Anlagenteils unternehmensfremd sowie rechtlich und wirtschaftlich unabhängig sein. Sie müssen in ihrer Prüfung gleichermaßen unabhängig von Weisungen und anderen Umständen sein, die einen Einfluss auf die Objektivität der Prüfung haben können. Die prüfende Stelle stellt sicher, dass kein Grund vorliegt, der geeignet ist, die Unabhängigkeit der einzelnen Mitglieder des Prüfteams in Frage zu stellen.

N.UP.01 Die Unabhängigkeit aller Mitglieder des Prüfteams ist durch die vom BSI zur Verfügung gestellten Formulare zu bestätigen.

2.2 Anforderungen an die Interne Revision als prüfende Stelle

P.IR.01 Abweichend zu den Anforderungen aus P.UP.01 und P.UP.02 können Interne Revisionen und ihre Mitarbeitenden trotz fehlender grundsätzlicher rechtlicher und wirtschaftlicher Unabhängigkeit gemäß P.UP.01 und P.UP.02 gegenüber ihrem Unternehmen als prüfende Stelle oder Prüfer handeln, wenn sie

a) das Vorliegen eines angemessenen und wirksamen Revisionssystems und

b) die Wirksamkeit der Internen Revision durch die Einhaltung der internationalen Standards für die berufliche Praxis des Institute of Internal Auditors (IIA)

sicherstellen und nachweisen.

N.IR.01 Die Erfüllung der Anforderungen ist durch ein Quality Assessment (QA) nach IDW PS 983 oder DIIR Revisionsstandard Nr. 3 zu bestätigen. Der Nachweis des Betreibers nach §8a Absatz 3 BSIG muss einen Auszug daraus enthalten, welcher mindestens erkennbar

1) eine positive Gesamtaussage zur Wirksamkeit beinhaltet,

2) der Internen Revision bzw. prüfenden Stelle zugeordnet werden kann,

3) belegt, dass das zugrundeliegende Quality Assessment (QA) nicht mehr als fünf Jahre gegenüber dem Abschluss der Prüfung der KRITIS-Anlage oder des KRITIS-Anlagenteils zurückliegt.

3 Prüfung und Nachweis

3.1 Prüfung nach dem 4-Augen-Prinzip

D.4A.01 Mindestens die Prüfungen in den folgenden Prüfungssachverhalten müssen im 4-Augen-Prinzip entsprechend D.4A.02 vorgenommen werden:

1) die Prüfung der korrekten Festlegung des Geltungsbereiches,
2) die Prüfung gültiger, referenzierter Zertifikate (bspw. ISO/IEC 27001-Zertifikat), insb. deren Geltungsbereich, Geeignetheit und Relevanz für den Nachweis,
3) die Prüfung des Vorgehens des Betreibers zu Risikoanalyse und Risikobehandlung,
4) die Prüfung der vorangegangenen Mängelliste gemäß den geltenden Anforderungen sowie
5) die Vor-Ort-Prüfung über die Erfüllung der gesetzlichen Anforderungen (im Sinne der Prüfmethoden der „Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten und Gegenständen“ und der „technischen Vor-Ort-Prüfung bzw. gezielten Beobachtung“).

D.4A.02 Die Prüfung eines Prüfungssachverhaltes, der innerhalb der Gesamtprüfung im 4-Augen-Prinzip durchgeführt wird, muss mindestens folgende Anforderungen erfüllen:

1) Die Prüfung des betroffenen Prüfungssachverhaltes wird durch zwei oder mehr beteiligte Prüfer vorgenommen, die unabhängig voneinander hinreichend qualifiziert sind, den zu prüfenden Prüfungssachverhalt bzw. relevante Teilaspekte zu beurteilen.
2) Die beteiligten Prüfer tragen eigenständig durch ihre Einschätzungen zur Gesamtbeurteilung des betroffenen Prüfungssachverhaltes bei. Die Einschätzungen sind innerhalb des Prüfteams angemessen zu berücksichtigen und zu einer Gesamtbewertung zu konsolidieren.
3) Die beteiligten Prüfer prüfen den Prüfungssachverhalt unmittelbar. Hierbei ist zulässig, dass die beteiligten Prüfer den Prüfungssachverhalt gemeinsam unmittelbar prüfen. Ebenso ist zulässig, dass der Prüfungssachverhalt auf verschiedene beteiligte Prüfer aufgeteilt wird, die ihren jeweiligen Anteil unmittelbar prüfen. Wird der Prüfungssachverhalt auf verschiedene beteiligte Prüfer aufgeteilt, sind die Ergebnisse der einzelnen Prüfer einer Qualitätskontrolle zu unterziehen. Unzulässig ist, dass nur ein Prüfer den gesamten Prüfungssachverhalt unmittelbar prüft, auch wenn im Anschluss eine Qualitätskontrolle erfolgt.
4) Die beteiligten Prüfer sollen über in etwa gleiche zeitliche Ressourcen für den im 4-Augen-Prinzip zu prüfenden Prüfungssachverhalt verfügen. Für keinen Prüfer darf der prozentuale zeitliche Prüfanteil dabei zwei Drittel der gesamten aufsummierten zeitlichen Prüfanteile zur Prüfung des Prüfungssachverhaltes überschreiten.

N.4A.01 Die Prüfungssachverhalte, in denen die Prüfungen im 4-Augen-Prinzip nach D.4A.02 durchgeführt werden, werden im Prüfplan einzeln als solche gekennzeichnet. Die Prüfer, die an der jeweiligen Prüfung im 4-Augen-Prinzip beteiligt sind, sind namentlich mit ihrem jeweiligen prozentualen zeitlichen Prüfanteil festzuhalten.

3.2 Dokumentation des Prüfergebnisses

N.PE.01 Soweit das BSI einen Prüfbericht anfordert, muss der Betreiber dem BSI den Prüfbericht inklusive der zugehörigen Unterlagen und Dateien zur Verfügung stellen.

D.PE.01 Die Ergebnisse einer Prüfung sind durch Prüfer und prüfende Stelle im „Prüfbericht über die Umsetzung der Anforderungen nach § 8a Absatz 1 BSIG“ zu dokumentieren.

D.PE.02 Der Prüfbericht muss ein eigenständiges Dokument sein.

D.PE.03 Der Prüfbericht muss in deutscher oder englischer Sprache verfasst sein.

D.PE.04 Der Prüfbericht muss strukturiert und inhaltlich frei von Widersprüchen sein. Er muss ein schlüssiges und nachvollziehbares Ergebnis beinhalten.

D.PE.05 Der Prüfbericht muss eine eindeutige Bezeichnung und Versionskennung enthalten.

D.PE.06 Der Prüfbericht muss alle für die Bewertung relevanten Metainformationen enthalten. Diese sind mindestens:

1) der Geltungsbereich der Prüfung,
2) das Prüfziel,
3) Zeitpunkt, Ort und Dauer der Prüfung,
4) die prüfende Stelle sowie
5) das Prüfteam (unter namentlicher Benennung der einzelnen Mitglieder des Prüfteams).

D.PE.07 Im Prüfbericht müssen alle Prüfschritte nachvollziehbar dokumentiert sein. In Inhalt und Form soll diese Dokumentation an der Darstellung des Prüfablaufs im Prüfplan ausgerichtet werden und muss insbesondere Informationen zu den Prüfobjekten und den jeweils genutzten Prüfmethoden beinhalten.

D.PE.08 Der Prüfbericht muss eine Erklärung durch einen Prüfer enthalten, wie die Stichprobenauswahl für die Vor-Ort-Prüfung getroffen wurde. Sofern es sich nicht um eine Erstprüfung handelt, muss diese Erklärung die Aussage enthalten, dass sich die Stichprobenauswahl von der Stichprobenauswahl der vorangegangenen Prüfung unterscheidet.

D.PE.09 Auf Anfrage eines Prüfers muss der Betreiber dem Prüfteam notwendige Informationen zur Stichprobenauswahl der vorangegangenen Prüfung zur Verfügung stellen. Dies beinhaltet in der Regel mindestens den entsprechenden Abschnitt nach D.PE.08 aus dem Prüfbericht der vorangegangenen Prüfung.

D.PE.10 Falls Sicherheitsmängel bestehen, muss der Prüfbericht die Liste der Sicherheitsmängel enthalten.

D.PE.11 Der Prüfbericht ist dem Betreiber zur Verfügung zu stellen.

D.PE.12 Nachdem der Betreiber die Liste der Sicherheitsmängel von der prüfenden Stelle erhalten hat, ergänzt der Betreiber diese Liste um einen Umsetzungsplan zur schnellstmöglichen Behebung dieser Mängel. Die Liste inklusive des Umsetzungsplans muss er der prüfenden Stelle vorlegen. Abschließend beurteilt ein Prüfer unter Berücksichtigung der Ergebnisse der Prüfung, ob die geplanten Maßnahmen geeignet sind, die identifizierten Mängel zu beseitigen. Der Prüfer hält diese Beurteilung abschließend am Ende der Liste der Sicherheitsmängel fest. Hält er eine oder mehrere Maßnahmen in der Beurteilung für ungeeignet, muss der Prüfer zudem eine kurze Begründung in der Liste hinzufügen.

3.3 Dokumentation des Geltungsbereiches

N.DG.01 Die Dokumentation des Geltungsbereiches in Anlage PD.A zu Nachweisdokument P muss folgende Kriterien erfüllen:

- G01: Die Anlage ist erkennbar und nachvollziehbar beschrieben.
- G02: Die vom Betreiber erbrachten Teile der kritischen Dienstleistung (kDL) sind erkennbar und nachvollziehbar beschrieben.
- G03: Die Darstellung enthält alle wesentlichen Merkmale der Anlagenkategorie.
- G04: Alle für die kritische Dienstleistung (kDL) maßgeblichen Prozesse sind erfasst.
- G05: Alle für die kritische Dienstleistung (kDL) maßgeblichen Systeme, Komponenten und ggf. Applikationen sind erfasst.
- G06: Alle Bereiche der KRITIS-Anlage 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-Anlage 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.

N.DG.02 Für den Netzstrukturplan muss die Dokumentation des Geltungsbereiches in Anlage PD.A zu Nachweisdokument P folgende Kriterien erfüllen:

- 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 kritische Dienstleistung (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.

3.4 Berücksichtigung alter Mängelliste in Prüfung und Nachweis

D.AM.01 Handelt es sich um eine Erstprüfung der Anlage, für die noch keine Nachweiseinreichung stattgefunden hat, muss der KRITIS-Betreiber die Prüfer darüber informieren.

D.AM.02 Handelt es sich um eine Folgeprüfung der Anlage, für die bereits eine Nachweiseinreichung stattgefunden hat, muss der KRITIS-Betreiber den Prüfern das Datum der letzten Einreichung benennen. Falls eine solche bestand, hat er den Prüfern die Mängelliste des letzten abschließend erbrachten und vom BSI akzeptierten Nachweises über die Anlage oder Anlagenteile vollständig und änderungsfrei zur Verfügung zu stellen. Er muss die Liste um ein aktuelles Datum und den Stand der Behebung der aufgeführten Mängel zu diesem Datum ergänzen. Der Stand der Behebung der einzelnen Mängel muss dabei durch eine von drei Bewertungen angegeben werden, die aufeinander folgende Phasen der Behebung eines Mangels kategorisieren:

- „In Planung“,
- „In Umsetzung“,
- „Abgeschlossen“.

D.AM.03 Die Mängelliste des vorangegangenen Nachweises muss, falls vorhanden, durch die Prüfer in die Prüfung einbezogen werden. Für alle dort aufgeführten Mängel ist der aktuelle Stand der Behebung, wie vom Betreiber angegeben, im Rahmen einer Plausibilitätskontrolle zu beurteilen. Für nicht vollständig behobene Mängel ist der aktuelle Stand, wie vom Betreiber angegeben, und die Plausibilitätsbeurteilung im Prüfbericht festzuhalten.

N.AM.01 In die Nachweisdokumente ist aufzunehmen, ob für die Anlage bereits ein Nachweis eingereicht wurde, es sich also um eine Erstprüfung oder um eine Folgeprüfung handelt.

N.AM.02 Falls eine Mängelliste für den zeitlich vorangegangenen Nachweis bestand, ist die Erklärung der prüfenden Stelle aufzunehmen, dass eine Prüfung dieser erfolgt ist.

N.AM.03 Nicht vollständig behobene Mängel aus der vorangegangenen Mängelliste sind in die aktuelle Mängelliste aufzunehmen. In der Beschreibung des Mangels (Mangelbeschreibung) sind der Stand der Behebung und die Plausibilitätsbeurteilung durch den Prüfer aufzuführen. Die neue ID dieser Mängel in der Mängelliste ist stets durch die ID aus der alten Mängelliste unter Voranstellung des Präfixes „ALT-[JAHR]-“ zu bilden, wobei „[JAHR]“ durch die Jahreszahl der Einreichung des vorangegangenen Nachweises ersetzt werden soll. Das Präfix „ALT-“ darf in der Mängelliste nur für diesen Kontext genutzt werden. Wird ein Mangel, der in der vorangegangenen Mängelliste bereits mit dem Präfix „Alt-[JAHR]-“ gekennzeichnet war, in eine neue Mängelliste überführt, ist weiterhin seine alte ID (unter Beibehaltung der alten Jahreszahl) zu verwenden.

3.5 Vorlagen für Bestandteile eines Nachweises nach § 8a Absatz 3 BSIG

N.BN.01 Soweit vorhanden, sind zur Nachweiserbringung für alle Dokumente und Unterlagen vom Betreiber verpflichtend die aktuellen vom BSI zur Verfügung gestellten Formulare und Vorlagen im vorgegebenen Dateiformat zu verwenden. Das BSI veröffentlicht diese in jeweils aktueller Version und gibt gegebenenfalls Übergangsfristen an. Eine abweichende Einreichung kann nur in begründeten Ausnahmefällen mit schriftlicher Zustimmung des BSI erfolgen.

N.BN.02 Ausschließlich der vom BSI festgelegten Ausnahmen müssen alle Bestandteile eines Nachweises in deutscher Sprache vorgelegt werden. Eine abweichende Einreichung kann nur in begründeten Ausnahmefällen mit schriftlicher Zustimmung des BSI erfolgen.

N.BN.03 **Nachweisdokument KI**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss das „Nachweisdokument KI“ beinhalten, inklusive Unterschrift und Stempel des Betreibers und Datum. Alternativ sind bei einer digitalen Einreichung auch Digitale Signaturen zulässig.

N.BN.04 **Nachweisdokument P**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Nachweisdokument P“ beinhalten, inklusive Unterschrift und Stempel der prüfenden Stelle und Datum. Alternativ sind bei einer digitalen Einreichung auch Digitale Signaturen zulässig.

N.BN.05 **Anlage PD.A**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Anlage PD.A: Beschreibung und grafische Darstellung des Geltungsbereichs der Prüfung in einem Netz-/ Anlagenplan“ beinhalten.

N.BN.06 **Anlage PD.B**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Anlage PD.B: Prüfplan“ beinhalten.

N.BN.07 **Anlage PE.A**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Anlage PE.A: Liste der Sicherheitsmängel inklusive Umsetzungsplan zur Behebung der Mängel“ beinhalten. Falls Mängel vorhanden sind, müssen die Liste der Sicherheitsmängel, der Umsetzungsplan und die abschließende Beurteilung des Umsetzungsplans durch den Prüfer ordnungsgemäß und ohne nachträgliche Änderungen enthalten sein. Falls keine Mängel vorhanden sind, ist das in der Anlage anzugeben.

N.BN.08 **Anlage PS.A**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Anlage PS.A: Nachweis über die zusätzliche Prüfverfahrenskompetenz für § 8a BSIG“ beinhalten. Anlage PS.A muss hierbei für einen Prüfer des Prüfteams vorgelegt werden. Sofern dieser Prüfer kein Mitarbeiter der prüfenden Stelle ist, muss die Anlage PS.A zusätzlich für einen Mitarbeiter der prüfenden Stelle vorgelegt werden.

N.BN.09 **Anlage PD.C**: Der vollständige Nachweis gemäß § 8a Absatz 3 BSIG muss „Anlage PD.C: Beschreibung der Prüfgrundlage“ beinhalten.

N.BN.10 Prüfplan PD.B bei Zusatzprüfung: Wurde eine Prüfung zur Erbringung des Nachweises nach § 8a Absatz 3 BSIG als Zusatzprüfung zu einer anderen Prüfung durchgeführt, sind im Prüfplan Prüfthemen, die durch die andere Prüfung abgedeckt wurden, unter Anbringung eines entsprechenden Hinweises aufzunehmen. Der Hinweis soll in der Angabe zur Prüfmethode vermerkt sein. Der Hinweis muss vollständige und geeignete Verweise auf die relevanten Stellen (zum Beispiel auf Seitenzahlen oder auf Abschnitte in Kapiteln) im zugehörigen Auditbericht beinhalten.

4 Inkrafttreten

Die Anforderungen treten grundsätzlich zum 01.06.2023 in Kraft.

Abweichend hierzu treten die Anforderungen

- N.IR.01,
- D.4A.01, D.4A.02, N.4A.01,
- D.PE.07, D.PE.12,
- D.AM.02, D.AM.03

zum 01.01.2024 in Kraft.