Bundesamt
für Sicherheit in der
Informationstechnik

# FAQ und Checkliste zur Erbringung von Nachweisen gemäß § 8a Absatz 3 BSIG

Diese Checkliste dient lediglich der internen Planung der Nachweiserbringung beim Betreiber der Kritischen Infrastruktur; die Checkliste bitte nicht an das BSI zurücksenden.

Gemäß § 8a Absatz 1a BSIG müssen Betreiber Kritischer Infrastrukturen ab dem 01.05.2023 mit dem nächsten fälligen Nachweis gemäß § 8a Absatz 3 BSIG auch Systeme zur Angriffserkennung (SzA) nachweisen. Alle notwendigen Informationen hierzu finden sich in der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung.

Hauptverantwortliche Person:

Frist zur Nachweiserbringung:

- [ ] Alle technischen und organisatorischen Maßnahmen sind umgesetzt.
- [ ] Die Anforderungen gemäß § 8a Absatz 5 BSIG sind berücksichtigt worden.

**Was sind die Anforderungen gemäß § 8a Absatz 5 BSIG?**

Betreiber einer Kritischen Infrastruktur müssen über die allgemeinen Anforderungen an einen Nachweis gemäß § 8a Absatz 3 BSIG hinaus beachten, dass das BSI gemäß § 8a Absatz 5 BSIG „[...] 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 kann."

Die Anforderungen gemäß § 8a Absatz 5 BSIG – Grundsätzliche Anforderungen im Nachweisverfahren (GAiN) sind auf der Website des BSI veröffentlicht.

Betreiber Kritischer Infrastrukturen der Anlagenkategorie 2.1.1 Rechenzentrum gemäß Anhang 4 Teil 3 BSI-KritisV müssen zudem weitere Anforderungen berücksichtigen. Diese sind ebenfalls auf der Website veröffentlicht.

- [ ] Eine prüfende Stelle wurde beauftragt.

**Wer kann ein Sicherheitsaudit, eine Prüfung oder Zertifizierung nach § 8a Absatz 3 BSIG durchführen?**

Grundsätzlich können Nachweise gemäß § 8a Absatz 3 BSIG von allen prüfenden Stellen erbracht werden, die zur Erbringung geeigneter Nachweise fähig sind. Letztendlich liegt die Verantwortung für die Erbringung eines geeigneten Nachweises und damit auch die Auswahl einer geeigneten prüfenden Stelle beim Betreiber der Kritischen Infrastruktur.

In der Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG beschreibt das BSI Kriterien, um die Eignung einer prüfenden Stelle (Kapitel 3) und des Prüfteams (Kapitel 4) bewerten zu können. Die Einhaltung dieser Kriterien bietet den Betreibern Sicherheit in der korrekten Umsetzung von § 8a Absatz 3 BSIG.

☐ Eine geeignete Prüfgrundlage wurde festgelegt.

**Können ISO 27001-Zertifikate für Nachweise gemäß § 8a Absatz 3 BSIG genutzt werden?**

Auf der Website des BSI sind FAQ zur Nutzung eines bestehenden ISO 27001-Zertifikats als Bestandteil für Nachweise gemäß § 8a Absatz 3 BSIG veröffentlicht.

☐ Der Geltungsbereich wurde in geeigneter Weise sowohl textuell als auch grafisch festgelegt und dokumentiert.

**Wie beschreibt man den Geltungsbereich und wie stellt man den Geltungsbereich grafisch dar?**

Der textuelle Geltungsbereich beschreibt die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur maßgeblich sind und erklärt die Details der betroffenen kritischen Prozesse.

Zentrales Element der grafischen Darstellung des Geltungsbereichs ist ein Netzstrukturplan. Die Grafik soll eine schnell zu erfassende Übersicht der zur kritischen Dienstleistung gehörenden Systeme, Komponenten und ggf. Applikationen abbilden.

Eine Zuordnung zwischen Prozessen und zugehörigen, notwendigen IT-Systemen muss möglich sein. Schnittstellen oder Abhängigkeiten zu außerhalb des Geltungsbereichs liegenden Bereichen müssen sichtbar werden. Die textuelle Beschreibung ergänzt diese Übersicht mit der nötigen Tiefe an Informationen. Ausführliche Informationen und Anforderungen zum Geltungsbereich finden sich in den Anforderungen gemäß § 8a Absatz 5 BSIG – Grundsätzliche Anforderungen im Nachweisverfahren (GAiN), der Orientierungshilfe zu Nachweisen (Kapitel 5) und in der BSI-Publikation „Zur Dokumentation des Geltungsbereiches bei KRITIS-Betreibern“.

☐ Die Prüfstelle hat zugesichert, die Prüfung nach dem Vier-Augen-Prinzip durchzuführen sowie die Anforderungen gemäß § 8a Absatz 5 BSIG hierzu einzuhalten.

**Was bedeutet Prüfung nach dem Vier-Augen-Prinzip?**

Prüfung nach dem Vier-Augen-Prinzip bedeutet, dass die Prüfung durch mindestens zwei Prüfer gemeinsam durchzuführen sind, um Unabhängigkeit und Objektivität zu gewährleisten. Die beteiligten Prüfer müssen dabei hinreichend qualifiziert sein, um unabhängig voneinander zu einer Bewertung der Sachlage gelangen zu können. Zu ausgewählten Prüfungssachverhalten existieren zudem verbindliche Anforderungen nach § 8a Absatz 5 BSIG, wie das Vier-Augen-Prinzip dort umzusetzen und zu dokumentieren ist.

☐ Mit der Prüfstelle wurde der geeignete Prüfaufwand festgestellt.

**Wie stelle ich den geeigneten Prüfaufwand fest?**

Die konkrete Prüfdauer ist schwer abzuschätzen, da sich die Anlagen der KRITIS-Betreiber stark unterscheiden. Hinweise zur Ermittlung der geeigneten Prüfdauer finden Sie in Abschnitt 5.4 der Orientierungshilfe zu Nachweisen.

☐ Der Termin zur Nachweiseinreichung wurde der prüfenden Stelle mitgeteilt.

☐ Der Prüfungszeitraum wurde festgelegt.

☐ Die Erstellung der Prüfdokumentation bis zur gesetzlichen Frist wurde von der prüfenden Stelle zugesichert.

☐ Aktuelle Formulare und Vorlagen des BSI werden verwendet.

☐ Der Umsetzungsplan zur Mängelliste wurde vollständig ausgefüllt.

**Was ist beim Ausfüllen des zur Mängelliste gehörenden Umsetzungsplans zu beachten?**

Alle vier Spalten im Umsetzungsplan sind vollständig auszufüllen. In der Spalte „Verantwortliche“ sind die Funktionen bzw. Fachbereiche der Verantwortlichen zu benennen. In der Spalte „Status“ ist der prozentuale Status der Umsetzung einzutragen. Wurde mit der Umsetzung der Mängelbeseitigung noch nicht begonnen, wird „0 %“ eingetragen. Bei Nachweiserbringung nach dem 01.01.2024 wurde die Bewertung der Prüfenden zum Umsetzungsplan eingeholt.

☐ Das Nachweisdokument KI wurde vollständig ausgefüllt und von einer verantwortlichen Person beim Betreiber der Kritischen Infrastruktur unterschrieben sowie mit Stempel versehen oder mit einer Digitalen Signatur versehen. Die dort aufgeführten Dokumente/Anlagen zum Nachweis liegen vollständig vor.

**Wo findet man die Nachweisformulare?**

Das BSI stellt die für einen Nachweis gemäß § 8a Absatz 3 BSIG notwendigen Formulare auf seiner Internetseite zum Download bereit:
www.bsi.bund.de/kritis-downloads

Der Nachweis soll am ☐ an das KRITIS-Büro des BSI übermittelt werden.