NICE Framework®
The GRC Management Platform

NIS-2 · § 30 BSIG

Die zehn Maßnahmenbereiche – und die Frage, die im Ernstfall gestellt wird.

§ 30 Abs. 2 BSIG nennt zehn Bereiche, die Risikomanagementmaßnahmen mindestens umfassen müssen. Nach § 30 Abs. 1 Satz 3 ist ihre Einhaltung zu dokumentieren. Die Prüfung fragt selten, ob ein Konzept existiert – sondern wer wann geprüft hat, dass es noch gilt.

NR.	WAS DAS GESETZ VERLANGT	DIE NACHWEISFRAGE
01	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	*Wann wurde die Risikoanalyse zuletzt aktualisiert, und wer hat das entschieden?*
02	Bewältigung von Sicherheitsvorfällen	*Wer war bei welchem Vorfall zuständig, und wann wurde eskaliert?*
03	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	*Wann wurde die Wiederherstellung zuletzt getestet — und mit welchem Ergebnis?*
04	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern	*Welche Anbieter sind bewertet, von wem, und wann ist die nächste Prüfung fällig?*
05	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen	*Welche Schwachstelle wurde wann gemeldet, und wer hat sie geschlossen?*
06	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik	*Woran wird Wirksamkeit gemessen, und wer hat sie zuletzt beurteilt?*
07	Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik	*Wer hat wann teilgenommen — und wer noch nicht?*
08	Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren	*Welches Verfahren gilt wo, und wann wurde die Vorgabe zuletzt überprüft?*
09	Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen	*Wer hat Zugriff, seit wann, und wann wurde das zuletzt rezertifiziert?*
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	*Für welche Zugänge gilt MFA — und für welche nachweislich nicht?*

Was „überwachen“ konkret heißt

§ 38 Abs. 1 BSIG verpflichtet die Geschäftsleitung, die Maßnahmen nach § 30 umzusetzen **und ihre Umsetzung zu überwachen**. Umsetzen ist ein Projekt. Überwachen ist ein Dauerzustand – und der lässt sich nicht durch ein Dokument belegen, nur durch eine Spur. Drei Angaben machen aus einer Maßnahme einen Nachweis:

Verantwortlicher

Eine benannte Person, nicht eine Abteilung. Ohne Namen gibt es im Streitfall keinen Adressaten.

Prüfrhythmus

Ein hinterlegtes Intervall mit Fälligkeit. Ein Konzept ohne Wiedervorlage altert unbemerkt.

Statushistorie

Wer wann was geändert hat – mit Zeitstempel. Was sich nicht rekonstruieren lässt, gilt als nicht geschehen.

Die Fristen, die dabei laufen

Meldepflichten nach § 32 Abs. 1 BSIG. Beachten Sie den Anknüpfungspunkt der letzten Frist – sie läuft ab der 72-Stunden-Meldung, nicht ab Kenntniserlangung.

24 h
Erstmeldung, unverzüglich, spätestens 24 Stunden nach Kenntniserlangung

72 h
Meldung, spätestens 72 Stunden nach Kenntniserlangung

auf Ersuchen
Zwischenmeldungen, wenn das BSI sie anfordert

1 Monat
Abschlussmeldung, spätestens einen Monat nach der 72-Stunden-Meldung

Wer wann prüft – und wer nicht

Ein verbreitetes Missverständnis: Die Nachweispflicht im Dreijahresturnus nach § 39 BSIG gilt **ausschließlich für Betreiber kritischer Anlagen**. Für besonders wichtige und wichtige Einrichtungen ohne kritische Anlage gibt es keine turnusmäßige Nachweis- oder Zertifizierungspflicht.

Kein Turnus heißt nicht keine Prüfung

Bei **besonders wichtigen Einrichtungen** kann das BSI nach § 61 BSIG Audits, Prüfungen und die Vorlage von Nachweisen anordnen; ein fester Turnus ist dafür nicht vorgesehen. Bei **wichtigen Einrichtungen** – im Mittelstand der Regelfall – genügt nach § 62 BSIG, dass Tatsachen die Annahme der Nichteinhaltung rechtfertigen; dann gelten dieselben Befugnisse. Einen Turnus kann man vorbereiten. Einen Anlass nicht.

Was die Geschäftsleitung persönlich betrifft

§ 38 Abs. 1: Maßnahmen umsetzen und ihre Umsetzung überwachen. Delegierbar ist die Ausführung, nicht die Verantwortung. · **Abs. 2:** Haftung gegenüber der eigenen Einrichtung nach dem Gesellschaftsrecht der Rechtsform (§ 43 GmbHG, § 93 AktG); eine eigenständige BSIG-Haftung greift nur subsidiär. · **Abs. 3:** regelmäßige Teilnahme an Schulungen.

Quellen: §§ 30, 32, 38, 39, 61, 62 BSIG in der Fassung des Gesetzes zur Umsetzung der NIS-2-Richtlinie, BGBl. 2025 I Nr. 301 vom 5. Dezember 2025, in Kraft seit dem 6. Dezember 2025. Der Wortlaut der zehn Maßnahmenbereiche ist § 30 Abs. 2 Nr. 1–10 BSIG entnommen. Stand dieser Übersicht: 8. September 2026. Diese Übersicht ersetzt keine Rechtsberatung.