BSIG & NIS2: Praxistipps für Sofortmaßnahmen

Das neue BSI-Gesetz (BSIG) zur Umsetzung der NIS2-Richtlinie ist am 6. Dezember 2025 offiziell in Kraft getreten.

Für circa 30.000 betroffene Unternehmen in Deutschland besteht nun sofortiger Handlungsbedarf.

Wir zeigen die wichtigsten Anforderungen, Sofortmaßnahmen und strategische Umsetzung.

Business sichern, Risiken minimieren, Chancen nutzen.

Was bedeutet das konkret für Ihr Unternehmen?

1

Erweiterter Anwendungsbereich

Circa 30.000 Unternehmen fallen nun unter die neuen Pflichten als „besonders wichtige oder wichtige Einrichtungen"

2

Unverzügliche Registrierung

Betroffene Unternehmen müssen bis spätestens März 2026 beim BSI registrieren

3

10-Punkte-Mindestkatalog

Zwingender Katalog an Risikomanagement-Maßnahmen ist zu implementieren

4

Persönliche Haftung der Geschäftsführung

Management ist direkt für Implementierung und Überwachung der IT-Sicherheitsmaßnahmen verantwortlich

Management-Haftung, verschärfte Meldepflichten, Sanktionen

Persönliche Verantwortung

Die Geschäftsführung ist direkt für Implementierung und Überwachung der IT-Sicherheitsmaßnahmen verantwortlich, muss an Schulungen teilnehmen und haftet bei Verstößen persönlich.

Meldepflichten

Betroffene Unternehmen müssen erhebliche Sicherheitsvorfälle innerhalb strenger Fristen (24 / 72 Std) über einen zentralen Eingangskanal an das BSI melden.

Sanktionen

- Bußgelder bis zu 10 Mio. € oder 2% des weltweiten Jahresumsatzes
- Behördliche Weisungen bis zur Untersagung von Leitungsfunktionen
- Öffentliche Warnungen

⚠ **Wichtig:** Für betroffene Unternehmen besteht nun dringender Handlungsbedarf. Wir zeigen die wichtigsten Sofortmaßnahmen.

PHASE 1

Rechtliche Betroffenheitsprüfung & Registrierung

Frist: 05. März 2026

⚠ **Achtung:** Betroffene Unternehmen müssen sich eigenständig prüfen und bis spätestens März 2026 beim BSI registrieren. Eine unterlassene Registrierung im Betroffenheitsfall kann mit Bußgeldern bis zu 500.000 € geahndet werden.

⚠ **Sofortige Aktion erforderlich:**

Falls noch nicht geschehen: Prüfen Sie jetzt Ihre NIS2-Betroffenheit und registrieren Sie sich beim BSI.

Schritt 1: Sofortige Betroffenheitsprüfung

01

Einordnung als BWIE oder WIE

Prüfen Sie, ob Ihr Unternehmen als besonders wichtige Einrichtung (BWIE) oder wichtige Einrichtung (WIE) einzuordnen ist

02

Sektoren und Anlagen

Identifizieren Sie, welche Sektoren und Anlagen (Anlagen 1 und/oder 2) betroffen sind

03

Größenschwellen & KRITIS Status

Prüfen Sie, ob die Größenschwellen erfüllt sind und ob ein KRITIS-Status vorliegt

04

Sonderfälle und Ausnahmen

Prüfen Sie, ob Sonderfälle (z.B. Vertrauensdienste, DNS, Telekommunikation) einschlägig sind oder Ausnahmen greifen

05

Dokumentation

Dokumentieren Sie das Ergebnis und die Gründe revisionssicher

Praxistipp: Nutzen Sie zunächst das anonyme Tool des BSI zur unverbindlichen Betroffenheitsprüfung unter https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html e

Zum BSI-Tool

Wichtige Hinweise zur Betroffenheitsprüfung

Keine Rechtssicherheit durch BSI-Tool

Das BSI-Tool liefert nur eine unverbindliche Ersteinschätzung – keine Rechtssicherheit. Bei Zweifeln an der Betroffenheit gilt: Im Zweifel betroffen. Gehen Sie zunächst davon aus, dass die BSIG-Pflichten greifen.

Rechtlich verbindliche Detailanalyse erforderlich

Bei unklarer Betroffenheit ist eine rechtlich verbindliche Detailanalyse zwingend erforderlich.

Eine unterlassene Registrierung im Betroffenheitsfall kann mit Bußgeldern bis zu 500.000 € geahndet werden.

Unser Service: Wir unterstützen bei der verbindlichen Betroffenheitsprüfung mit unseren ISO Experten und Lead Auditoren.

Jetzt Betroffenheitsprüfung anfragen

Schritt 2: Prüfung der Ausnahmen

Prüfen Sie ob für bestimmte Tätigkeiten oder Teile ihres Unternehmens Ausnahmen von den NIS2-/BSIG-Anforderungen gelten, um den Compliance-Aufwand zu reduzieren. Eine erfolgreiche Ausnahmen erfordert jedoch eine gründliche Dokumentation und Nachweisführung.

Unwesentliche Nebentätigkeit und IT-Unabhängigkeit (§ 28 Abs. 3 & 4)

Unwesentlichkeit der Tätigkeit

Prüfkriterien:

1. Relevanz-Check: Liegt der Umsatzanteil der kritischen Tätigkeit stabil unter der Geringfügigkeitsschwelle?
2. Abhängigkeits-Check: Würde das Kerngeschäft weiterlaufen, wenn der kritische Unternehmensteil sofort isoliert würde?
3. Markt-Check: Gibt es genügend Wettbewerber, die Ihren Ausfall kompensieren könnten?

Erforderliche Nachweise:

- Wirtschaftlicher Nachweis (Umsatz/Deckungsbeitrag)
- Prozess-Isolation dokumentieren
- Marktanalyse zur Versorgungssicherheit

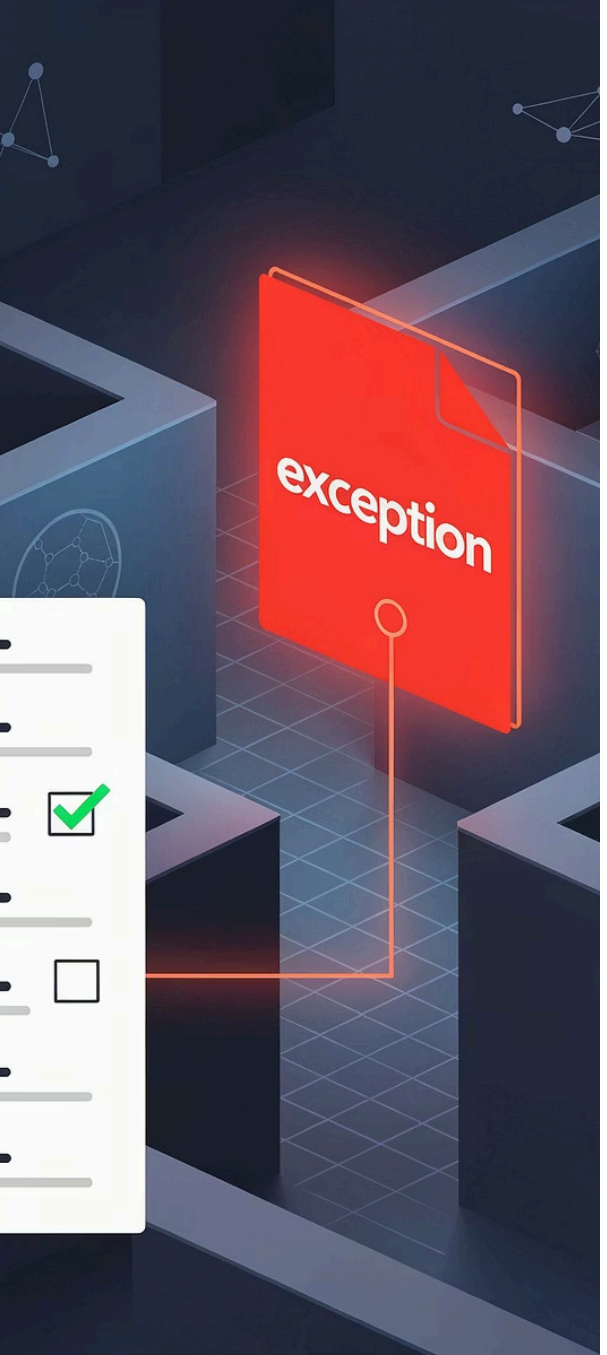
IT-Unabhängigkeit

Prüfkriterien:

1. Netztrennungs-Check: Logische und physische Trennung der IT-Systeme
2. Governance-Inventur: Eigene IT-Sicherheitsrichtlinien
3. Budget & Personal: Eigenes IT-Budget und Personal
4. IT-Autarkie: Vollständig autarker Betrieb möglich

Erforderliche Nachweise:

- Technisches Netzwerkdiagramm
- Governance-Nachweis
- Bestätigung der IT-Leitung



Wichtige Hinweise zu Ausnahmen

Diese Ausnahmen sind rechtlich eng auszulegen. Insbesondere bei der IT-Unabhängigkeit scheitern viele Konzerne an „geteilten Diensten" (Shared Services wie zentrales SAP oder HR-Tools).

Selbst wenn einzelne Tätigkeiten die Betroffenheits-Schwellenwerte unterschreiten, ist eine Herabstufung von „besonders wichtiger Einrichtung" zu „wichtiger Einrichtung" nicht möglich.

NIS-2 und BSIG erfassen die gesamte juristische Person. Das Risikomanagement muss daher unternehmensweite gelten. Für vernachlässigbare Tätigkeiten können risikobasiert geringere Schutzmaßnahmen implementiert werden.

Achtung: Angreifer nutzen gezielt schwach geschützte Unternehmensteile als Einfallstor. Auch wenn „unwesentliche" Tätigkeiten von den gesetzlichen Mindestmaßnahmen ausgenommen sind, haftet die Geschäftsführung bei Sicherheitsvorfällen. Die Ausnahmen entbinden nicht von der allgemeinen Sorgfaltspflicht – das Schutzniveau muss durchgängig angemessen sein.

Schritt 3: Validierung und Argumentation

1

Sektoreinordnung validieren

Prüfen Sie, ob nach Abzug der „unwesentlichen" Bereiche überhaupt noch eine Schwellenwertüberschreitung (Mitarbeiter/Umsatz) vorliegt

2

Rechtsfolgen-Simulation

Simulieren Sie, welche Unternehmensteile im Falle einer erfolgreichen Inanspruchnahme dieser Ausnahmen von den Meldepflichten und Umsetzungsmaßnahmen (§ 30 BSIG) befreit wären

3

BSI-Kommunikation vorbereiten

Bereiten Sie eine Argumentationslinie vor, falls das BSI die Stammdatenmeldung oder die Registrierung aufgrund der Konzernzugehörigkeit hinterfragt

Schritt 4: Registrierung beim BSI

MUK-Konto anlegen

Erstellen Sie ein ELSTER-basiertes „Mein Unternehmenskonto" (MUK) – Voraussetzung für das BSI-Portal

BSI-Registrierung

Schließen Sie die Registrierung im neuen BSI-Portal **bis 05. März 2026** ab

Kontaktstelle benennen

Legen Sie mindestens zwei befähigte Personen als dauerhafte Ansprechpartner für das BSI fest und hinterlegen Sie diese im Portal

Praxistipp: Ändern Sie diese Personen später entsprechend der aufgebauten Cyber- & IT-Sicherheit-Governance, des ISMS und den darin festgelegten RACI-Verantwortlichkeiten.

PHASE 2

Strategische Cyber- & IT-Sicherheit Governance etablieren

Management-Verantwortung & Haftung

Die Geschäftsführung verantwortet und haftet persönlich für die Umsetzung und Kontrolle von ausreichenden IT-Sicherheitsmaßnahmen.

Die Geschäftsführung muss dringend strategische Cyber- & IT-Sicherheit Governance-Strukturen etablieren.

- Implementieren Sie strategische Governance-Strukturen mit klaren Verantwortlichkeiten, Überwachungsprozessen und Management-Accountability

Praxistipp: Erstellen Sie eine Mehrjahres-Roadmap mit 1-3-Jahres-Plan und Budget für den Aufbau eines kompletten ISMS inklusive der 10 Mindest-IT-Sicherheitsmaßnahmen mit konkreten Meilensteinen und Budgetplanung. Passen Sie diese kontinuierlich an.

1. Management-Verantwortung: Kernpflichten

⚠ IT-Sicherheit und BSIG Compliance ist Chefsache. Das Management muss insbesondere die folgenden Maßnahmen implementieren:

Grundlegende Verantwortung & Governance Struktur

- Cyber- und Informationssicherheit formell als Unternehmensrisiko einstufen
- Gesamtverantwortung für Cyber-Risiken auf Geschäftsführungsebene festlegen und dokumentieren
- Verbindliche Cyber-Governance-Struktur (Management-Gremium) etablieren
- CISO/IT-Sicherheitsverantwortlichen mit direkter Berichtslinie an die Geschäftsführung benennen

Strategie & Risikomanagement

- IT-Sicherheitsstrategie und Risikomanagement-Konzept formell per Beschluss billigen
- Risikotoleranz, Risikoappetit und Kriterien zur Risikoakzeptanz verbindlich festlegen
- Formellen Prozess zur dokumentierten Risikoakzeptanz durch das Management etablieren
- Verbindliches RACI-Modell mit Eskalations- und Entscheidungsmatrix für Cyber- und Informationssicherheit beschließen
- Cyber-Risiken verbindlich in Unternehmenssteuerung und ERM integrieren

Monitoring & Kontrolle

- Monatliches Cyber-Dashboard mit Management-KPIs zur IT-Sicherheitslage (Incident-Rate, Patch-Status, kritische Risiken) verbindlich einführen
- Feste Überwachungs-Routine mit mindestens vierteljährlichen Cyber-Governance-Meetings und KPIs definieren
- IT-Sicherheitsbudget explizit ausweisen und risikobasiert genehmigen

Schulung & Versicherung

- Gesetzlich geforderte Geschäftsführungsschulungen durchlaufen (§ 38 BSIG)
- Die bestehende D&O-Versicherung im Hinblick auf Cyber- und NIS2-Haftungsrisiken prüfen

Review & Wirksamkeit

- Einen jährlichen Management-Review zur Wirksamkeit der Cyber- & NIS2-Governance durchführen
- Wirksamkeitsprüfungen der Cyber-Governance durchführen

Geschäftsführerschulungen (§ 38 Abs. 3 BSIG)

Wichtig: § 38 Abs. 3 BSIG schreibt vor, dass sich die Geschäftsführung regelmäßig zu IT-Sicherheitsrisiken schulen lassen muss!

Geschäftsführer-Schulung durchführen

3-4 Stunden Schulung nach BSI Empfehlung für alle Geschäftsführer zu IT-Risiken, Sicherheitsmaßnahmen und persönlicher Haftung

Teilnahme dokumentieren

Teilnahmebestätigungen mit Datum, Inhalten und Unterschrift revisionssicher archivieren (BSI-Prüfung!)

Jährlich wiederholen

Auffrischungsschulung fest einplanen

Achtung – Versicherungsschutz: Fehlende Schulungen gelten als grobe Fahrlässigkeit der Geschäftsführung und führen ggf. zum Deckungsausfall bei D&O- und Cyber-Versicherungen. Im Schadensfall zahlt die Versicherung vielleicht nicht!

Unser Service: Ab Ende Januar bieten wir spezialisierte **onlinebasierte Videoschulungen, Webinare und Workshops für Geschäftsführer** – erstellt von zertifizierten ISO-Officern & Auditoren sowie Rechtsanwälten. Kontaktieren Sie uns für Termine und Buchung.

Jetzt Geschäftsführerschulung anfragen

Organisationsstruktur & CISO-Bestellung

1 **CISO bestellen**

Benennen Sie einen IT-Sicherheitsbeauftragten (CISO), der operativ responsible für die Maßnahmen ist

2 **Ressourcen bereitstellen**

Mindestbudget und Personalstärke des IT-Sicherheitsteams festlegen

3 **Unabhängigkeit sichern**

Direkten Meldeweg vom CISO an die Geschäftsführung etablieren – unter Umgehung der Hierarchieebenen

4 **Kontaktstellen benennen**

Zwei Personen als Kontaktstellen für das BSI offiziell benennen und im BSI-Portal hinterlegen

Praxistipp: Der CISO sollte organisatorisch unabhängig von der IT-Leitung sein und direkt an die Geschäftsführung berichten. Definieren Sie in der RACI-Matrix und/oder der Stellenbeschreibung im Arbeitsvertrag klare Befugnisse, Weisungsfreiheit gegenüber der operativen IT sowie ein Veto-Recht bei allen Sicherheitsfragen.

Meldeprozess bei Sicherheitsvorfällen

24h / 72h / 1 Monat

⚠ **24 Stunden Meldepflicht:** Betroffene Einrichtungen müssen erhebliche Sicherheitsvorfälle unverzüglich an das BSI melden. Verstöße gegen die Meldepflicht sind bußgeldbewehrt (bis 500.000 €).

Was ist ein „erheblicher Sicherheitsvorfall"?

Ein Vorfall ist erheblich, wenn er tatsächlich oder wahrscheinlich:

- Die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten beeinträchtigt
- Die Sicherheit von Netz- und Informationssystemen erheblich stört
- Erhebliche Auswirkungen auf die Erbringung Ihrer Dienstleistungen hat

Beispiele: Ransomware-Angriff, Datendiebstahl, DDoS-Attacke, erfolgreiche Phishing-Angriffe mit Systemzugriff, großflächiger Systemausfall durch Cyberangriff

Meldefristen

24 Stunden

Erstmeldung (Frühwarnung) an das BSI

72 Stunden

Update/Vollmeldung mit Details zum Vorfall

1 Monat

Abschlussbericht mit Lessons Learned

✓ **Praxistipp:** Orientieren Sie sich an dem Prozess zur Bewertung und Meldung von Datenschutzverletzungen und bauen Sie diesen zu einem konsolidierten Melde-Prozess aus.

Meldeprozess: Interne Umsetzung

1 Erkennung sicherstellen

Sicherstellung, dass erhebliche Vorfälle identifiziert werden können (z.B. durch SIEM "Security Information and Event Management")

2 Meldekriterien definieren

Erstellen Sie eine klare Checkliste, wann ein Vorfall als „erheblich" gilt und meldepflichtig ist

3 Meldekette etablieren

Legen Sie fest, wer intern innerhalb von 24 Stunden entscheidet, ob gemeldet wird und wer die Meldung ans BSI übermittelt (Management-Einbindung zwingend)

4 Verantwortlichkeiten klären

Benennen Sie einen Incident Response Manager, der für die Koordination und fristgerechte Meldung verantwortlich ist

5 Template vorbereiten

Erstellen Sie Meldevorlagen, um im Ernstfall Zeit zu sparen

6 Meldeprozess testen

Testen Sie in einer Simulation (z.B. Tabletop-Übung mit Ransomware-Szenario), dass „erhebliche Sicherheitsvorfälle" innerhalb der neuen Fristen gemeldet werden können

Incident Response Prozess: Überlebenswichtig für Ihr Unternehmen

Die Meldepflicht ist nur der erste Schritt. Ein funktionierender Incident-Response-Prozess ist überlebensnotwendig für das Unternehmen.

Ohne strukturierte Reaktion auf Sicherheitsvorfälle drohen:

- **Existenzbedrohende Folgen**
- **Produktions- & Betriebsausfall**
- **Verlust von wichtigen Daten und Geschäftsgeheimnissen**
- **Folgeschäden wie Reputationsschäden, Vertragsstrafen, Schadensersatz, Bußgelder**

⚠ **Achtung:** Ein Ransomware-Angriff ohne vorbereiteten Incident-Response-Prozess kann ein Unternehmen innerhalb von Stunden für lange Zeit lahmlegen. Die Vorbereitung ist keine Option – sie ist überlebenswichtig.

Incident-Response-Prozess einrichten und testen

Wichtig: Die schnelle und professionelle Reaktion auf einen Cyberangriff entscheidet über das Überleben des Unternehmens. Ein Incident-Response-Plan muss VOR dem Ernstfall stehen. Der Prozess muss im Ernstfall innerhalb von Stunden funktionieren (im schlimmsten Fall auch ohne funktionsfähige IT-Systeme).

Krisenstab-Struktur

Dokumentieren Sie die Rollen für einen IT-Krisenstab, inklusive Vertretungsregelung und Befugnissen zur Systemabschaltung

Erheblichkeits-Kriterien

Klare Schwellenwerte für BSI-Meldepflicht definieren (z.B. >X Kunden betroffen, >Y Stunden Ausfall)

Krisenraum einrichten

Physischer/virtueller Raum mit allen notwendigen Kontakten und Zugriffsmöglichkeiten inkl. funktionierender Notfallkommunikation

Externe Dienstleister und Budget (bei Hausbank)

Liste qualifizierter Incident-Response-Dienstleister und Rechtsberatung vorhalten, die Sie sofort beauftragen können

Externe Kommunikation

Definieren, wer im Krisenfall mit Medien, Kunden und Partnern kommuniziert

Jährliche Krisenübung

Simulation z.B. eines Ransomware-Angriffs mit Management-Beteiligung durchführen

Wichtig: Dokumentieren Sie jeden Schritt des Incident Response (Zeitstempel, Maßnahmen, Entscheidungen) – diese Dokumentation ist entscheidend für den Abschlussbericht und schützt vor Bussgeldern, Haftung und Schadensersatzforderungen.

PHASE 3

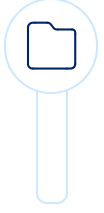
Asset-Identifizierung und Klassifizierung

Vorbereitung des ISMS

Ein Asset (Wertegegenstand) ist alles, was für die Erbringung Ihres Dienstes kritisch ist.

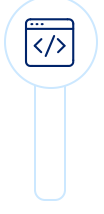
Die systematische Erfassung und Klassifizierung aller Assets ist die Grundlage für wirksame IT-Sicherheitsmaßnahmen und den Aufbau eines funktionierenden ISMS (Information Security Management System).

Asset-Identifizierung und Klassifizierung: Was muss wie geschützt werden?



Kategorisierung

Unterteilen Sie Ihre Assets in Primär-Assets (Geschäftsprozesse und Informationen wie Kundendaten, Produktionssteuerung) und Sekundär-Assets (IT-Systeme, Server, Cloud, Netzwerkkomponenten, Software, Personal, physische Standorte)



Software-Inventarisierung

Erstellen Sie eine Liste aller genutzten Softwareprodukte inklusive Versionen, um Schwachstellen (Vulnerabilities) schneller zuordnen zu können

Klassifizierung (C-I-A)

Bewerten Sie jedes Asset nach Vertraulichkeit (Confidentiality: Wer darf die Daten sehen?), Integrität (Integrity: Wie schlimm ist eine unbemerkte Manipulation?) und Verfügbarkeit (Availability: Wie lange darf das System ausfallen?)

Abhängigkeits-Mapping

Dokumentieren Sie, welche IT-Systeme welche Geschäftsprozesse stützen (z.B. „Ohne Active Directory steht die Logistik")

Bedrohungsrisiko festlegen (Risikoanalyse)

Führen Sie eine Risikoanalyse durch und ermitteln Sie "Eintrittswahrscheinlichkeit" und "Auswirkungen". Orientieren Sie sich an der ISO 27001 oder BSI-Standard 200-3. Die folgenden Schritte beschreiben den Prozess zur Risikobewertung.

1

Gefährdungskatalog durchgehen

Überprüfen Sie die „Elementaren Gefährdungen", dazu gehören:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen/Cyberangriffe

2

Risikomatrix erstellen

Bewerten Sie jedes Szenario nach zwei Kriterien:

- **Eintrittswahrscheinlichkeit:** (von Selten bis Sehr häufig)
- **Schadensauswirkung:** (von Gering bis Existenzbedrohend)

3

Risiko-Appetit definieren

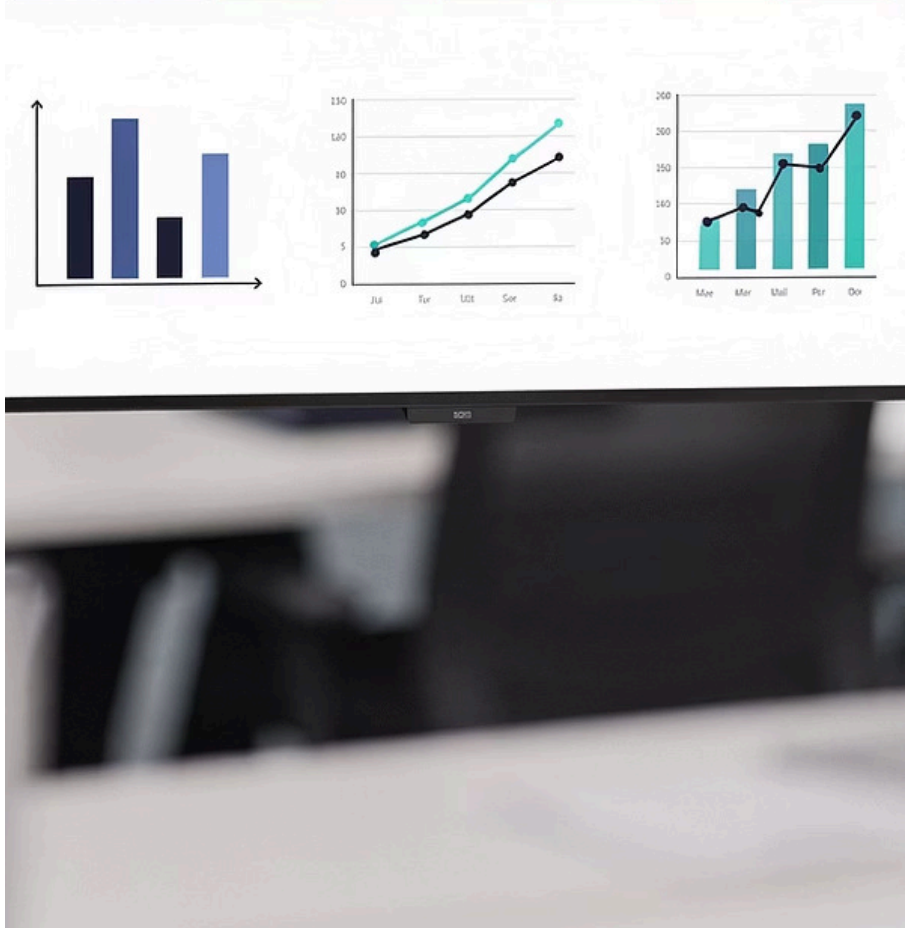
Legen Sie klare Schwellenwerte fest (z.B. „Hohes Risiko"), ab denen zwingend sofortige technische oder organisatorische Maßnahmen ergriffen werden müssen.

4

Risikobehandlung entscheiden

Dokumentieren Sie für jedes identifizierte Risiko die entsprechende Behandlungsstrategie:

- **Vermeiden:** Prozess abschalten oder ändern
- **Reduzieren:** Maßnahmen zur Risikominderung ergreifen
- **Übertragen:** Risiko auf Dritte verlagern (z.B. Versicherung)
- **Akzeptieren:** Das Restrisiko bewusst hinnehmen (Management-Entscheidung)



Die 10 wesentlichen Mindestmaßnahmen nach § 30 BSIG

Wichtig: § 30 BSIG verpflichtet betroffene Einrichtungen zur Umsetzung und Dokumentation von 10 wesentlichen Mindestmaßnahmen. Die jeweils nötigen Maßnahmen und deren Tiefe müssen auf einem gefahrenübergreifenden Ansatz beruhen.

1. Risikoanalyse & ISMS

ISMS-Rahmenwerk nach ISO 27001 oder BSI 200-3

2. Incident Management

Prozesse zur Erkennung, Meldung und Behebung (24h/72h/1 Monat)

3. Business Continuity

Notfallpläne, Backup-Strategien (3-2-1-Regel!), Disaster Recovery

4. Supply Chain Security

Lieferantenrisikomanagement mit Sicherheitsnachweisen

5. Cyberhygiene mit Patch- und Schwachstellenmanagement & Secure Development

Security by Design, Patch-Management, SBOM-Verwaltung

6. Wirksamkeitsprüfung

Regelmäßige Audits, Penetrationstests (mindestens jährlich)

7. Awareness & Schulungen

Mitarbeitersensibilisierung durch Phishing-Simulationen

8. Kryptografie

Verschlüsselung ruhender Daten und Daten im Transit

9. IAM

Least-Privilege-Prinzip, Zugriffskontrolle, Asset-Management

10. MFA

Multi-Faktor-Authentifizierung für alle kritischen Systeme

Gap-Analyse und Roadmap

Praktische Umsetzung der Gap-Analyse

01

IST-Aufnahme

Erfassen Sie für jede der 10 Mindestmaßnahmen den aktuellen Stand (Nicht vorhanden / Teilweise / Vollständig umgesetzt)

02

Gap-Identifikation

Dokumentieren Sie konkrete Lücken (z.B. "MFA nur für VPN, nicht für Admin-Accounts")

03

Risikobewertung

Bewerten Sie jede Lücke nach Kritikalität (Kritisch = direkter Gesetzesverstoß / Mittel / Gering)

04

Maßnahmenplanung

Leiten Sie konkrete Umsetzungsprojekte ab mit Verantwortlichen, Budget und Zeitplan

05

Quick Wins identifizieren

Markieren Sie Maßnahmen, die schnell und kostengünstig umgesetzt werden können

06

Roadmap erstellen

Priorisieren Sie: Erst kritische Gaps, dann Quick Wins, dann mittelfristige Projekte

Praxistipp: Erstellen Sie eine Tabelle mit den Spalten: Anforderung | IST-Zustand | GAP | Kritikalität | Maßnahme | Verantwortlich | Termin | Budget.

So behalten Sie den Überblick und können der Geschäftsführung den Fortschritt transparent berichten.

Business Continuity & Disaster Recovery implementieren

RTO definieren

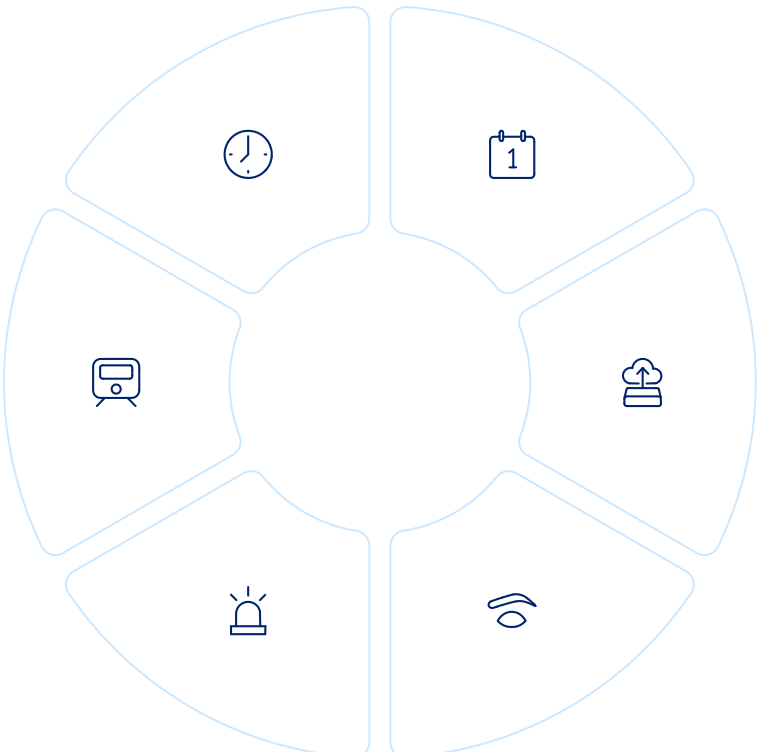
Recovery Time Objective: Wie lange darf ein System maximal ausfallen? (z.B. E-Mail: 4h, Produktion: 2h)

DR-Tests

Halbjährlich vollständige Systemwiederherstellung in isolierter Testumgebung durchführen

Notfallpläne

Schritt-für-Schritt-Anleitung für verschiedene Szenarien – auch offline verfügbar!



RPO festlegen

Recovery Point Objective: Wie viel Datenverlust ist tolerierbar? (z.B. Finanzdaten: max. 15 Min.)

3-2-1-Regel

3 Kopien der Daten, auf 2 verschiedenen Medien, 1 Kopie offline/offsite (Ransomware-Schutz!)

Backup-Tests

Regelmäßige Wiederherstellungstests (mindestens quartalsweise) – ein ungetestetes Backup ist wertlos!

Achtung: Viele Unternehmen scheitern nicht am technischen Recovery, sondern an fehlender Kommunikation und unklaren Entscheidungswegen. Definieren Sie, wer im Krisenfall welche Entscheidungen treffen darf und sorgen Sie dafür dass sie umgehend getroffen werden!

PHASE 4

Lieferkettensicherheit (Supply Chain) sicherstellen

⚠ **Wichtig:** BSIG macht Sie für die IT-Sicherheit Ihrer direkten Zulieferer und Dienstleister verantwortlich. Sicherheitslücken bei Partnern können zu Ihrer eigenen Haftung führen.

1 Risikoprofil erstellen

Kategorisieren Sie alle IT-Dienstleister, Cloud-Provider, Software-Anbieter und kritische Zulieferer nach Risiko (Hochrisiko: direkter Systemzugriff, Datenverarbeitung; Mittelrisiko: indirekte Abhängigkeit; Niedrigrisiko: unkritische Services)

2 Sicherheitsnachweise einfordern

Verlangen Sie von kritischen Partnern Nachweise wie SOC 2-Berichte, ISO 27001-Zertifikate, BSIG-Compliance-Bestätigungen oder vergleichbare Sicherheitsdokumentationen

3 Verträge anpassen

Nehmen Sie IT-Sicherheitsklauseln in alle Verträge auf – inkl. Meldepflicht bei Sicherheitsvorfällen, Audit-Rechte, SLAs für Verfügbarkeit und Incident Response, sowie Kündigungsrecht bei schweren Sicherheitsverstößen

4 Cyber-Audits durchführen

Prüfen Sie kritische Lieferanten regelmäßig (mindestens jährlich) durch Fragebögen, Vor-Ort-Audits oder externe Auditoren

5 Notfallplanung

Entwickeln Sie für kritische Abhängigkeiten Alternativszenarien (Second Source, Exit-Strategie) für den Fall, dass ein Lieferant ausfällt oder kompromittiert wird

6 Kontinuierliches Monitoring

Etablieren Sie einen Prozess zur laufenden Überwachung der Sicherheitslage bei Schlüssellieferanten (z.B. News-Monitoring, automatische Zertifikats-Checks)

✓ **Praxistipp:** Beginnen Sie mit den Top 10 kritischsten Lieferanten. Erstellen Sie ein Lieferantenregister mit Risikobewertung, Vertragsstatus und Fristen für Maßnahmen.

Von der Strategie bis zur Umsetzung:
Wir unterstützen Sie bei der Umsetzung.

Unsere Leistungen:

- Betroffenheitsprüfung NIS2 & BSIG
- ISMS-Aufbau, -Implementierung & Dokumentation
- Audit und Zertifizierung
- Externer ISB / CISO

Unsere Experten:

- Rechtsanwälte & Wirtschaftsjuristen,
- Zertifizierte ISO/IEC 27001 Officer & Compliance Officer
- Zertifizierte ISO/IEC 27001 Lead-Auditoren

PRICOM kontaktieren **Forbsec kontaktieren**