GREENSOCKS
r.evolutionary consulting

NIS2 ISMS-GUIDE

Strukturiertes ISMS-Vorgehen

GREENSOCKS
BEFÄHIGEN
STATT NUR
BERATEN
r.evolutionary consulting

1. Management Summary

Die aktuelle Bedrohungslage im Bereich der Informationssicherheit ist dynamisch und komplex. Cyberangriffe, Ransomware und gezielte Attacken auf kritische Infrastrukturen nehmen stetig zu. Unternehmen jeder Größe stehen vor der Herausforderung, ihre sensiblen Daten und Systeme wirksam zu schützen, ohne unverhältnismäßige Ressourcen zu binden.

Mit der Umsetzung der EU-NIS2-Richtlinie in deutsches Recht durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsCG wurde vom Bundestag am 13. November 2025 angenommen, am 21.11.2026 vom Bundesrat zugestimmt, bedeutet nun die endgültige Freigabe des überarbeiteten IT-Sicherheitsgesetz = das neue BSI-Gesetz) ergeben sich für Unternehmen neue, verbindliche Anforderungen an die Informationssicherheit. Ziel ist es, ein hohes und einheitliches Cybersicherheitsniveau in der EU zu etablieren und die Widerstandsfähigkeit kritischer sowie wichtiger Infrastrukturen nachhaltig zu stärken. Die Verantwortung für die Cybersicherheit liegt ausdrücklich bei der Geschäftsleitung, die für die Umsetzung und Überwachung aller erforderlichen Maßnahmen verantwortlich ist.

Konkret bedeutet dies für Unternehmen

- Technische und organisatorische Maßnahmen (TOMs): Angemessene Maßnahmen zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme müssen umgesetzt, dokumentiert und regelmäßig überprüft werden.
- Risikomanagement: Ein risikobasierter Ansatz ist verpflichtend, der die individuelle Risikoexposition, Unternehmensgröße, Umsetzungskosten sowie die Wahrscheinlichkeit und Schwere möglicher Sicherheitsvorfälle berücksichtigt.

- Schulungspflicht: Die Geschäftsleitung ist verpflichtet, regelmäßig (mindestens alle drei Jahre) an Schulungen teilzunehmen, um ausreichende Kenntnisse im Bereich Cybersicherheit und Risikomanagement sicherzustellen.
- Nachweisführung: Die Einhaltung aller Maßnahmen muss dokumentiert und auf Anfrage gegenüber Behörden nachgewiesen werden können.
- Sanktionen: Bei Verstößen drohen empfindliche Sanktionen, darunter Bußgelder, die Offenlegung von Verantwortlichen oder temporäre Führungsverbote.

Um all diese Aspekte der Informationssicherheit zuverlässig zu gewährleisten, dient dieser Guide als strukturierter Leitfaden, um die eigene Informationssicherheit nach NIS2 entweder von Grund auf zu etablieren oder bestehende Strukturen gezielt zu optimieren – und das ohne unnötige Komplexität.

Die GreenSocks Consulting GmbH bringt über 15 Jahre Erfahrung in der Begleitung von Unternehmen auf dem Weg zur ISO/IEC 27001-Zertifizierungsreife mit. In dieser Zeit haben wir dutzende Organisationen – vom Mittelstand bis zum Konzern – mit einem praxisbewährten, pragmatischen Vorgehen von Null auf ein belastbares Informationssicherheitsmanagementsystem (ISMS) geführt.
Unser Ansatz ist klar strukturiert, realistisch und umsetzbar, weil er sich an den tatsächlichen Herausforderungen im Unternehmensalltag orientiert – nicht an theoretischen Idealbildern. Genau diese Erfahrung haben wir in diesem Guide komprimiert: konkrete Schritte, klare Prioritäten, sofort anwendbar.

Es funktioniert. Es spart Zeit.

Es schützt Ihr Unternehmen.

Biker Ehrenwort!

Inhaltsverzeichnis

NIS 2-GUIDE

GREENSOCKS
r.evolutionary consulting

2. NIS2 Relevanz beachten und umsetzen

2.1. Branchen- und Schwellenwertprüfung

Die erste und wichtigste Frage jeder NIS2-Betrachtung lautet:

Fällt das Unternehmen überhaupt unter die NIS2-Richtlinie und wenn ja, in welcher Kategorie?

Die NIS2-Richtlinie unterscheidet zwischen zwei Kategorien:

- Wesentliche Einrichtungen („essential entities"): sie unterliegen einer strengeren Aufsicht und intensiveren Prüfungen.
- Wichtige Einrichtungen („important entities"): sie werden reaktiv überwacht, müssen aber dennoch umfangreiche Pflichten erfüllen.

Diese Einstufung ist entscheidend, denn sie bestimmt die Intensität der behördlichen Aufsicht, den Bußgeldrahmen, die Prüfpflichten und den Umfang der regulatorischen Anforderungen. Damit eine Organisation rechtssicher agieren kann, muss die Einstufung systematisch geprüft, dokumentiert und begründet werden.

Warum ist das wichtig?

Eine falsche oder fehlende Einstufung führt unmittelbar zu Compliance-Risiken:

- verspätete oder unterlassene Registrierung,
- unzureichende Sicherheitsmaßnahmen,
- falsche oder fehlende Meldungen erheblicher Sicherheitsvorfälle,
- aufsichtsrechtliche Maßnahmen und Bußgelder,
- sowie persönliche Haftungsrisiken der Geschäftsleitung nach § 38 BSIG-E.

Behörden erwarten eine strukturierte, nachvollziehbare und risikobasierte Entscheidung, keine Bauchentscheidung.

Die drei Kernbausteine der Einstufung

1. Branchenprüfung

Die NIS2-Richtlinie gilt nicht für alle Unternehmen gleichermaßen. Sie definiert insgesamt 18 Sektoren, davon 11 als „wesentlich" und 7 als „wichtig".

2. Schwellenwertprüfung

Neben der Branche sind EU-weit einheitliche Mindestschwellen (z. B. Unternehmensgröße) sowie nationale Konkretisierungen nach BSIG-E relevant.

3. Dokumentation und Begründung

Die Entscheidung, ob und in welcher Kategorie NIS2 gilt, muss prüffähig dokumentiert und von der Geschäftsleitung freigegeben werden.

✅ Schritt 1: Branchenprüfung – Zuordnung zu „wesentlich" oder „wichtig"

Wesentliche Einrichtungen (höchste Regulierung) sind u. a.:

- Energie (Strom, Gas, Öl, Fernwärme)
- Verkehr (Luft, Bahn/Schiene, Wasser)
- Gesundheitswesen (Krankenhäuser, Hersteller kritischer Medizinprodukte)
- Trinkwasser/Abwasser
- Digitale Infrastruktur (IXPs, TLD-Registry, DNS)

- Öffentliche Verwaltung
- Raumfahrt

Diese Sektoren unterliegen einer proaktiven Aufsicht mit Audits, Prüfungen und Vor-Ort-Kontrollen.

Wichtige Einrichtungen (hohe Regulierung) sind u. a.:

- Post- und Kurierdienste
- Abfallwirtschaft
- Lebensmittelproduktion und -verarbeitung
- Chemischer Sektor
- Pharmazeutische Produktion
- Digitale Dienste (Cloud, Hosting, MSSP, Suchmaschinen)
- Maschinen- und Fahrzeugtechnik

Hier erfolgt die Aufsicht reaktiv, also anlassbezogen bei Auffälligkeiten oder Vorfällen.

Besonderheit „Digitale Dienste“:

Für Cloud-Provider, MSP/MSSP, Hosting-Anbieter, Rechenzentren und Domain-Registrare gelten NIS2-Pflichten unabhängig von der Unternehmensgröße, da diese Dienste als besonders kritisch eingestuft werden.

Praxisbeispiel: Ein IT-Dienstleister, der Remote-Administrationszugänge für Kunden verwaltet, fällt in der Regel als wichtige Einrichtung unter NIS2 – selbst ohne große Mitarbeiterzahl.

✅ Schritt 2: Schwellenwertprüfung – Größe und Bedeutung

Unternehmen fallen unter NIS2, wenn sie in einem relevanten Sektor tätig sind und mindestens eines der folgenden Kriterien erfüllt:

- ≥ 50 Mitarbeitende
- ≥ 10 Mio. € Jahresumsatz
- ≥ 10 Mio. € Jahresbilanzsumme

Sind Sektor + Schwelle erfüllt, ist das Unternehmen NIS2-pflichtig.

Ausnahmen / Sonderfälle (unabhängig von der Größe):

- Betreiber kritischer digitaler Infrastrukturen
- Cloud-Anbieter
- Domain-Registrare
- MSP/MSSP
- bestimmte Energie- oder Gesundheitsdienstleister
- Unternehmen mit systemrelevanter Bedeutung

Nationale Zusatzkriterien (Deutschland, BSIG-E / NIS2UmsuCG):

Die Einstufung kann strenger sein, z. B. wegen:

- besonderer Relevanz eines Dienstes
- Auswirkungen auf öffentliche Sicherheit
- grenzüberschreitender Risiken
- Abhängigkeiten anderer Unternehmen

Diese Aspekte müssen risikobasiert bewertet und dokumentiert werden.

✅ Schritt 3: Einstufung und Dokumentation

Die Einstufung muss schriftlich und prüffähig erfolgen. Enthalten sein müssen:

- **Branchenidentifikation**: Sektor, Begründung, Beschreibung der relevanten Dienste
- **Schwellenwertnachweise**: Mitarbeitenden-Zahl, Umsatz, Bilanzsumme, Ausnahmen
- **Risikobasierte Begründung**: Kritikalität, Abhängigkeiten, Auswirkungen bei Störung
- **Einstufungsentscheidung**: Kategorie (wesentlich/wichtig), Datum, beteiligte Rollen
- **Freigabe durch die Geschäftsleitung**: Protokoll oder Signatur, Ablage im DMS/GRC-System

Die BSI-Handreichung betont die Nachweispflicht gegenüber Aufsichts-behörden und „unabhängigen Stellen".

Pflichtartefakte für die Nachweisführung

Folgende Dokumente müssen jederzeit vorzeigbar sein:

- NIS2-Scope-Assessment (Einstufungsdokument)
- Branchen- und Schwellenwertanalyse
- Risiko- und Schweregradbewertung (inkl. Business-Impact)
- Management-Freigabe / Vorstandsbeschluss
- Liste relevanter Dienste mit Kritikalität
- Legal/Compliance-Prüfvermerk
- Review-Nachweise (mindestens jährlich oder bei Änderungen)

So gehst Du vor – Schritt für Schritt

✅ **1. Ziel klären**: Feststellen, ob und wie NIS2 greift (inklusive Kategorie).

✅ **2. Branchenzuordnung**: Leistungen auf NIS2-Sektoren mappen, Digital-Dienst-Kriterien prüfen.

✅ **3. Schwellenwerte prüfen**: Mitarbeitende, Umsatz, Bilanzsumme, Sonderfälle dokumentieren.

✅ **4. Risiko- und Impact-Analyse**: Abhängigkeiten, Dominoeffekte, Business-Impact ergänzen.

✅ **5. Einstufung entscheiden**: Kategorie festlegen, Begründung dokumentieren, Freigabe einholen.

✅ **6. Registrierung vorbereiten**: Verantwortlichkeiten für Registrierung und Änderungen definieren.

✅ **7. Review etablieren**: Jährliche Überprüfung oder bei Struktur-/Serviceänderungen.

✅ Selbstcheck – sind wir korrekt eingestuft?

1. Haben wir formal geprüft, ob wir in einem NIS2-Sektor liegen?
2. Ist klar dokumentiert, ob wir „wesentlich“ oder „wichtig“ sind?
3. Haben wir Größe, Umsatz und kritische Dienstleistungen bewertet?
4. Liegt eine schriftliche Begründung vor, die Behörden nachvollziehen können?
5. Gibt es einen jährlichen Einstufungs-Review?
6. Ist Legal/Compliance in die Entscheidung eingebunden?
7. Ist geregelt, wer Änderungen neu bewertet?

2.2. Registrierung beim BSI und Pflege der Unternehmensdaten

Die NIS2-Umsetzung in Deutschland verpflichtet alle betroffenen Einrichtungen zur **Registrierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Diese Registrierung ist die formale Grundlage für die Kommunikation mit den Behörden, die Erfüllung von Meldepflichten und die Teilnahme an Unterstützungsmaßnahmen.

Wichtig: Die Registrierung ist **kein einmaliger Schritt**. Unternehmen müssen ihre Angaben **fortlaufend aktuell halten** und Änderungen unverzüglich nachpflegen.

Warum ist das wichtig?

Das BSI muss jederzeit wissen:

- **Wer** im Unternehmen zuständig ist,
- **wie** die Organisation erreichbar ist,
- und **welche Systeme und Dienste** unter die Regulierung fallen.

Nur so können Behörden im Ernstfall:

- schnell warnen,
- Rückfragen stellen,
- verpflichtende Informationen übermitteln,
- oder Unterstützungsmaßnahmen einleiten.

Fehlende oder falsche Registrierungsdaten gelten als **Verstoß gegen NIS2**, können Bußgelder auslösen und im Ereignisfall zu Verzögerungen führen.

✅ Schritt-für-Schritt-Anleitung zur Registrierung

1. Registrierungspflicht prüfen

2. Registrierungsdaten vorbereiten

3. Registrierung im BSI-Portal durchführen

4. Interne Freigabe und Nachweisführung sicherstellen

5. Fristen einhalten und Änderungen unverzüglich melden

6. Regelmäßige Überprüfung der Daten etablieren

1. Feststellen der Registrierungspflicht

- **Verantwortlich:** Legal/Compliance gemeinsam mit ISB oder CISO
- **Kriterien:**
    - Sektor (z. B. Gesundheit, Verkehr, Energie, digitale Dienste, Verwaltung)
    - Schwellenwerte (Unternehmensgröße, kritische Dienstleistung)
    - Kritikalität einzelner Services

Tipp: Viele Organisationen sind NIS2-pflichtig, ohne es zu wissen. Frühzeitige juristische Prüfung spart später Aufwand und Bußgeldrisiken.

2. Vorbereitung der Registrierungsdaten

Erforderliche Angaben beinhalten:

- Offizielle Unternehmensdaten
- Gesellschaftsform und Anschrift(en)
- Verantwortliche Kontaktpersonen (24/7 erreichbar)
- Interne Rollen (ISB, NIS2-Kontaktstelle)
- Beschreibung der wesentlichen Dienste und Prozesse
- Technische Kontaktpunkte (CERT/SOC, Notfallnummern)

Praxisbeispiel:
Viele Unternehmen benennen einen generischen Verteiler („security@...“) als 24/7-Kontakt. Das erfüllt die Form – aber ohne klare Rufbereitschaft bleibt die Erreichbarkeit lückenhaft.

3. Registrierung im BSI-Portal

- **Verantwortlich:** ISB/CISO oder benannte Kontaktstelle
- **Schrittfolge:**
    1. Benutzerkonto anlegen
    2. Unternehmen registrieren
    3. Kontaktstelle eintragen
    4. Verantwortlichkeiten hinterlegen
    5. Dienste/Services beschreiben
    6. Nachweise hochladen (je nach Sektor)

Die Registrierung muss dokumentiert und intern freigegeben werden.

Registrierungsportal

Melde- und Informationsportal des BSI – verfügbar über https://mip2.bsi.bund.de/authentifizierung/registrieren/ [mip2.bsi.bund.de]

4. Interne Freigabe und Nachweisführung

- Dokumentation der Registrierung im internen DMS
- Ablage der Bestätigungsmail und Registrierungs-ID
- Checkliste für Vollständigkeit
- Eintrag in das NIS2-Compliance-Register (falls vorhanden)

5. Fristen und Wiederholung

- **Registrierung:** sofort mit Eintritt der NIS2-Pflicht
- **Anpassungen:** unverzüglich, spätestens innerhalb von 14 Tagen
- **Überprüfung:** mindestens jährlich (z. B. im ISMS- oder BCM-Review)

6. Pflege der Unternehmensdaten im BSI-Portal

Die Daten müssen aktuell sein. Typische Änderungen, die sofort eingepflegt werden müssen:

- Wechsel der Geschäftsführung oder Rechtsform
- neue IT-Infrastrukturstandorte
- neue kritische Dienste
- Änderung der 24/7-Erreichbarkeit
- Übernahme oder Fusion
- Änderung der internen Kontaktstelle
- Outsourcing oder neuer Dienstleister

Verantwortlichkeiten:

- Datenpflege: ISB/CISO
- Organisatorische Änderungen: Compliance/Legal
- Technische Kontaktpunkte: SOC/IT-Security
- Freigabe: Management oder Risikoausschuss

Pflichtartefakte / Nachweise

- Registrierungsunterlagen (Export aus BSI-Portal)
- Interne Verfahrensanweisung zur Registrierungspflicht
- Aktuelle Kontaktstellenliste
- DMS-Ablage der Änderungen
- Audit-Trail oder Änderungsprotokoll aus dem Portal
- Jahresreview-Protokoll (z. B. ISMS/BCM Management Review)

✅ Selbstcheck: Erfüllen wir die Registrierungspflicht?

1. Wissen wir zweifelsfrei, ob wir unter NIS2 fallen?
2. Haben wir einen definierten Prozess zur Registrierung?
3. Sind 24/7-Kontakte benannt und erreichbar?
4. Ist klar geregelt, wer Änderungen meldet und wer sie freigibt?
5. Prüfen wir unsere Registrierungsdaten mindestens einmal pro Jahr?
6. Können wir Nachweise für Audits oder Behörden innerhalb von 24 Stunden bereitstellen?

2.3. Governance & Haftung

Die NIS2-Richtlinie macht unmissverständlich klar: **Die Verantwortung für Cybersicherheit und Resilienz liegt nicht bei der IT-Abteilung, sondern explizit bei der Geschäftsleitung.**
Leitungspersonen müssen sicherstellen, dass Sicherheitsmaßnahmen umgesetzt, überwacht und regelmäßig bewertet werden. Diese Pflichten sind **nicht delegierbar**. Governance ist damit nicht nur ein Organisationskonzept, sondern ein **rechtlich relevanter Pflichtenkatalog**.

Warum ist das wichtig?

Anders als frühere Regelungen verpflichtet NIS2 die Geschäftsleitung **persönlich**. Verstöße können führen zu:

- **persönlicher Haftung**,
- **Bußgeldern**,
- **aufsichtsrechtlichen Maßnahmen**,
- und in Extremfällen sogar **berufsrechtlichen Konsequenzen**.

Ohne klare Governance – also definierte Zuständigkeiten, Nachweise und regelmäßige Kontrolle – ist NIS2-Compliance nicht erreichbar.

Kernbausteine der Governance

✅ 1. Pflichten der Geschäftsleitung

Die Leitung muss nachweislich:

- regelmäßig an **Schulungen zu Cybersicherheit** teilnehmen,
- das Sicherheitsniveau des Unternehmens aktiv überwachen,
- Risiken und kritische Vorfälle bewerten und Entscheidungen treffen,
- sicherstellen, dass alle organisatorischen und technischen Maßnahmen umgesetzt werden,

- ausreichende Ressourcen bereitstellen,
- ein wirksames Managementsystem unterstützen (ISMS, BCMS, Risikomanagement).

Wichtig: Governance-Pflichten können delegiert werden – die **Verantwortung bleibt bei der Geschäftsleitung**.

✅ 2. Schulungsnachweis der Geschäftsleitung

NIS2 schreibt verpflichtende Schulungen für Leitungspersonen vor.

Inhalte:

- Überblick NIS2 und nationales Umsetzungsgesetz,
- Verantwortlichkeiten und Haftung,
- Meldepflichten (24h / 72h / 30 Tage),
- Risikobewertung und Sicherheitsmaßnahmen,
- Grundprinzipien sicherer IT- und Organisationsführung.

Nachweisformen:

- Teilnahmezertifikat,
- Schulungsprotokoll,
- Dokumentation im Learning-System,
- Eintrag im Management-Review.

Praxisfehler:
Nur „informiert" zu sein reicht nicht – die Schulung muss **dokumentiert** sein.

✅ 3. Regelmäßige Reviews (Pflichtkontrollen)

Mindestens einmal jährlich (besser halbjährlich) muss die Geschäftsleitung ein strukturiertes Review durchführen:

- Zielerreichung der Sicherheitsmaßnahmen,
- aktuelle Risikolage und Trends,
- Ergebnisse von Audits, Tests und Vorfällen,
- strukturelle Schwachstellen,
- Status aller Umsetzungsmaßnahmen,
- Ressourcenbedarf,
- offene oder akzeptierte Risiken,
- Status der NIS2-Compliance.

Ergebnis:

- Beschlüsse der Geschäftsleitung,
- priorisierte Maßnahmenliste,
- Nachweis der Ressourcenfreigabe,
- dokumentierte Risikoakzeptanzen.

✅ 4. Haftungsrisiken für Leitungspersonen

NIS2 definiert eine **verschärfte Sorgfaltspflicht**. Verstöße können zu:

- persönlichen Sanktionen,
- Bußgeldern gegen das Unternehmen,
- aufsichtsrechtlichen Einschränkungen,
- Abberufung leitender Personen führen.

Klartext: Nicht die IT haftet – die Geschäftsleitung haftet für fehlende Governance.

Fehlende Reviews, Schulungsnachweise oder unklare Rollen sind unmittelbare Haftungsrisiken.

✅ 5. Dokumentation der Management-Entscheidungen

Governance muss **prüfbar** sein. Dokumentation zeigt, dass die Geschäftsleitung ihrer Sorgfaltspflicht nachkommt.

Notwendige Inhalte:

- Beschlüsse der Geschäftsleitung (Datum, Inhalt, Verantwortlicher),
- Risikoakzeptanzen inkl. Begründung,
- Ressourcenfreigaben (Budget, Personal),
- Ernennung von ISB / CISO / Kontaktstelle,
- Freigabe des NIS2-Konzepts oder Sicherheitsmaßnahmen,
- Ergebnisse der Management-Reviews,
- Nachweise über Schulungen der Leitungsebene.

Typische Ablageorte:

- DMS / SharePoint,
- ISMS-Tool,
- Governance-Register,
- Protokollordner der Geschäftsleitung.

Tipp: Behörden bewerten nicht die Menge an Dokumenten, sondern die **Entscheidungsfähigkeit**. Entscheiden, begründen, dokumentieren.

✅ Typische Rollen in der Governance

Rolle	Verantwortung
Geschäftsleitung	Gesamtverantwortung, Freigaben, Schulungspflicht, Haftung
ISB / CISO	Fachliche Steuerung der Sicherheitsmaßnahmen
Compliance / Legal	Bewertung rechtlicher Pflichten, Dokumentation
Risk Manager	Risikoanalyse, Registerpflege
IT-Leitung	technische Umsetzung
Krisenstab / BCM	Management von Großvorfällen
Kontaktstelle nach NIS2	24/7-Erreichbarkeit, Behördenkommunikation

Pflichtartefakte / Nachweise

- Schulungsnachweise der Geschäftsleitung,
- Protokolle und Beschlüsse aus Management-Reviews,
- Governance- und Verantwortlichkeitsmatrix,
- Ernennungsdokumente (ISB, CISO, Kontaktstelle),
- Risiko- und Maßnahmenregister,
- Nachweis der Ressourcenfreigaben,
- Dokumentation der internen Kontrollen.

✅ Selbstcheck: Erfüllen wir die Governance-Pflichten?

1. Gibt es eine dokumentierte Verantwortlichkeitsmatrix?
2. Liegt ein gültiger Schulungsnachweis aller Leitungspersonen vor?
3. Wird jährlich ein strukturiertes Management-Review durchgeführt?
4. Sind Entscheidungen mit Datum, Verantwortlichem und Begründung dokumentiert?
5. Sind Ressourcen für Sicherheit nachweislich freigegeben?
6. Ist definiert, wer NIS2-relevante Entscheidungen vorbereitet?
7. Können wir Behörden oder Auditoren in 24 Stunden vollständige Nachweise liefern?

2.4. Bußgeld- und Sanktionsmechanismen – Compliance ist Pflicht

Die NIS2-Richtlinie setzt auf strengere Kontrollen und Sanktionen, um Cybersicherheit verbindlich durchzusetzen. Die Regeln gelten sowohl für Unternehmen als auch für Führungskräfte. Verstöße haben **organisatorische und persönliche Konsequenzen**.

Unter NIS2 ist es nicht mehr möglich, Sicherheitslücken oder fehlende Governance als „organisatorische Nachlässigkeit" abzutun. Die Richtlinie setzt klare Signale:

- **Sicherheitsmanagement ist Chefsache**
- **Sicherheitsmängel sind keine Bagatellen**
- Fehlende Maßnahmen oder unzureichende Umsetzung können **sanktionsbewehrt** sein

Für Organisationen bedeutet das: Compliance ist kein reines Audit-Thema mehr, sondern ein **strategisches Risiko für Unternehmensführung, Reputation und Geschäftsbetrieb**.

✅ 1. Bußgeld- und Sanktionsmechanismen nach NIS2

Die Richtlinie führt eine Kombination aus **finanziellen, organisatorischen und persönlichen Sanktionen** ein. Diese gelten abhängig von Einrichtungstyp (wesentlich vs. wichtig), Sektor und Schwere des Verstoßes.

Sanktionen gegen Unternehmen

Bußgelder:

- **Wesentliche Einrichtungen:** bis zu **10 Mio. EUR** oder **2 % des weltweiten Jahresumsatzes** (je nachdem, was höher ist)
- **Wichtige Einrichtungen:** bis zu **7 Mio. EUR** oder **1,4 % des weltweiten Jahresumsatzes**

Typische Gründe für Bußgelder:

- fehlende oder verspätete Meldung von Sicherheitsvorfällen
- unzureichende Sicherheitsmaßnahmen
- fehlende Registrierung
- wiederholte Pflichtverletzungen
- Nichterfüllung behördlicher Anordnungen

Hinweis: Behörden berücksichtigen Schwere, Dauer, Wiederholung, Vorsatz/Fahrlässigkeit und Kooperation.

Sanktionen gegen Leitungspersonen

NIS2 adressiert explizit die persönliche Verantwortung:

- **Führungsverbote** (temporär oder dauerhaft bei schweren Verstößen)
- **persönliche Haftung** bei Verletzung der Sorgfaltspflichten
- verpflichtende Schulungsauflagen
- behördliche Verwarnungen oder Anordnungen

Praxisbeispiel:
Fehlt ein dokumentiertes Management-Review oder Schulungsnachweis, gilt das als Verletzung der Sorgfaltspflicht.

Weitere Sanktionsmechanismen

- **Offenlegung („Naming & Shaming"):** öffentliche Bekanntmachung schwerer Verstöße
- **Behördliche Anordnungen:** Sofortmaßnahmen, Nachbesserungen, unabhängige Audits, Vorlage von Unterlagen
- **Vor-Ort-Prüfungen:** Gebäude betreten, Systemeinsicht, Logfiles prüfen, Interviews führen, technische Beweise sichern

✅ Compliance-Checkliste: Nachweis der Einhaltung

Die zentrale Frage: **Wie weist eine Organisation nach, dass sie NIS2-konform ist?**

Eine strukturierte Checkliste hilft, Auditfähigkeit sicherzustellen.

1. Governance & Verantwortlichkeiten

- Verantwortlichkeitsmatrix vorhanden (inkl. Geschäftsleitung)
- ISB/CISO formal ernannt
- Kontaktstelle gemäß NIS2 definiert (24/7 erreichbar)
- Schulungsnachweise für Leitungsebene dokumentiert
- jährliches NIS2-Management-Review durchgeführt

2. Registrierung & Meldung

- Registrierung beim BSI abgeschlossen
- Registrierungsdaten aktuell (Review mindestens jährlich)
- definierter Prozess für 24h/72h/30-Tage-Meldungen
- Vorlagen für Meldungen verfügbar
- Nachweispaket je Sicherheitsvorfall dokumentiert

3. Technische & organisatorische Sicherheitsmaßnahmen

- Risikoanalyse nach NIS2 umgesetzt
- Sicherheitsmaßnahmen gemäß Annex (ISO 27001-ähnlich) abgedeckt
- Patch- und Schwachstellenmanagement etabliert
- Backup-, Notfall- und Wiederanlaufstrategien dokumentiert
- Monitoring & Logging vorhanden
- Zugangskontrollen / IAM / MFA flächendeckend

4. Lieferketten & Dienstleister

- Risikoanalyse Lieferketten durchgeführt
- Sicherheitsanforderungen in SLAs/Verträgen verankert
- Notfall- und Cyber-Klauseln vorhanden
- regelmäßige Überwachung und Bewertung

5. Dokumentation & Nachweise

- alle relevanten Entscheidungen dokumentiert
- Risiko- und Maßnahmenregister gepflegt
- Auditberichte abgelegt
- Protokolle der Geschäftsleitung vorhanden
- technische Evidenzen (Tickets, Logs, Screenshots)
- Schulungslisten vollständig

6. Was prüft die Behörde konkret?

- Governance: Verantwortlichkeiten, Schulungsnachweise
- Meldeverhalten: Einhaltung der Fristen
- Sicherheitsniveau: Maßnahmen, Prozesse, Rollen
- Nachweise: Dokumentation, Logs, Auditfähigkeit
- Risikomanagement & BCM-Integration
- Lieferkettenmanagement
- Reaktion auf behördliche Anordnungen
- Umsetzung früherer Auflagen
- Fähigkeit zur 24/7-Erreichbarkeit

Wichtig: Behörden prüfen **Wirksamkeit**, nicht die Menge an Dokumenten. Ein dicker Ordner ersetzt keine funktionierenden Prozesse.

3. Vorgehen zur Etablierung/Optimierung Deines ISMS

3.1. Reifegrad-Assessment

Bevor Du ein Informationssicherheits-Managementsystem (ISMS) aufbaust, solltest Du wissen, wo Du stehst. Genau dafür gibt es die Reifegradanalyse. Sie ist der Ausgangspunkt, um Dein aktuelles Sicherheitsniveau zu bewerten und gezielt Verbesserungen anzugehen.

Warum ist das wichtig?

- Du erkennst, wie weit Deine Organisation in Sachen Informationssicherheit entwickelt ist.
- Du findest Lücken gegenüber den Anforderungen der NIS2.
- Du kannst Maßnahmen priorisieren und Ressourcen effizient einsetzen.

Die Bewertungsskala (Reifegrad)

Wir nutzen ein Modell, das sich am **Capability Maturity Model (CMM)** orientiert. Damit ordnest Du jeden Prozess oder jede Kontrolle auf einer Skala von **0 bis 5** ein:

Stufe	Beschreibung
0 – Nicht existent	Der Prozess oder die Kontrolle existiert nicht oder verfehlt das Ziel.
1 – Initial / Ad Hoc	Erste Ansätze sind erkennbar, aber alles läuft ungeordnet und ohne klare Verantwortlichkeiten.
2 – Wiederholbar, aber intuitiv	Prozesse sind implementiert, aber nicht dokumentiert. Viel hängt vom Wissen einzelner Personen ab.
3 – Definiert	Prozesse sind dokumentiert, standardisiert und grundsätzlich wirksam.
4 – Gemanaged & messbar	Prozesse werden überwacht, gemessen und regelmäßig bewertet.
5 – Optimiert	Kontinuierliche Verbesserung, Automatisierung und proaktive Beteiligung der Mitarbeiter.

So führst Du die Reifegradanalyse durch – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst herausfinden, wie gut Dein Unternehmen aktuell beim Thema Informationssicherheit aufgestellt ist.
Warum? Damit Du weißt, wo Du stehst – und was verbessert werden muss.

✅ 2. Vorbereitung

- Sammle alle relevanten Unterlagen: Richtlinien, Prozesse, Rollenbeschreibungen, technische Maßnahmen.
- Stelle ein kleines Team zusammen (IT, Organisation, ggf. Datenschutz).

✅ 3. Gap-Analyse starten

Vergleiche Deine aktuellen Maßnahmen mit den Anforderungen der NIS2.
Fragen, die Du stellen kannst:

- Gibt es eine Richtlinie zur Zugriffskontrolle?
- Wie gehst Du mit Sicherheitsvorfällen um?
  Nutze dafür eine Checkliste oder ein Tool, das die Normpunkte auflistet.

✅ 4. Prozesse bewerten

- Schau Dir Deine Abläufe an: Risiko Management, Change-Management, Incident-Handling, Schulungen, Umgang mit Lieferanten, etc.
- Dokumentiere, was funktioniert – und wo Lücken sind.

✅ 5. Reifegrad festlegen

Bewerte jeden Bereich auf der Skala von 0 bis 5.
Beispiele:

- Zugriffskontrolle: **3 – Definiert**

- Lieferantenmanagement: **1 – Ad Hoc**

  So entsteht ein klares Bild Deines IST-Zustands.

✅ 6. Ergebnisse zusammenfassen

Erstelle eine Übersicht mit:

- **Stärken**
- **Schwächen**
- **Empfehlungen für nächste Schritte**

✅ Nutzen und Vorteil

Die Analyse zeigt Dir:

- Wo Du bereits gut aufgestellt bist
- Wo dringender Handlungsbedarf besteht
- Wie Du gezielt und effizient ein ISMS aufbauen kannst

3.2. Stakeholder-Analyse

Bevor Du Dein ISMS einführst, musst Du wissen, **wer alles involviert ist, und welche Erwartungen bestehen**. Die Stakeholder-Analyse ist dafür der Schlüssel. Sie sorgt dafür, dass niemand vergessen wird und alle relevanten Personen oder Gruppen rechtzeitig eingebunden sind.

Identifiziere alle relevanten Stakeholder, die Einfluss auf die Informationssicherheit und die Umsetzung der NIS2-Anforderungen haben. Berücksichtige insbesondere die explizite Verantwortung der Geschäftsleitung und die Einbindung externer Partner, Lieferanten und Behörden.

Warum ist das wichtig?

- Du erkennst, wer Einfluss auf Dein ISMS hat und wie groß das Interesse ist.
- Du kannst Prioritäten setzen: Wer muss intensiv eingebunden werden? Wer nur informiert?
- Du schaffst Transparenz und vermeidest Widerstände.

Die drei Kernbausteine

1. **Stakeholder-Matrix**: Visualisiert Einfluss und Interesse.
2. **Rollen & Verantwortlichkeiten**: Klare Zuordnung von Zuständigkeiten.
3. **Kommunikationsbedarfe**: Definiert Informationsflüsse und Kanäle.

So führst Du die Stakeholder-Analyse durch – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst herausfinden, **wer vom Thema Informationssicherheit betroffen ist oder Anforderungen stellt**.
Warum? Damit Du alle relevanten Personen rechtzeitig einbindest.

✅ 2. Stakeholder identifizieren

Erstelle eine Liste aller Beteiligten:

- Geschäftsführung
- IT-Abteilung
- Datenschutzbeauftragte
- Mitarbeitende
- Kunden
- Lieferanten
- Externe Partner (z. B. Auditoren)

Notiere, welche Rolle diese Personen oder Gruppen im Unternehmen spielen.

✅ 3. Stakeholder-Matrix erstellen

Zeichne eine einfache Matrix:

- **Achse 1:** Einfluss (Wie stark können sie Entscheidungen beeinflussen?)
- **Achse 2:** Interesse (Wie wichtig ist ihnen das Thema Informationssicherheit?)

Ordne jeden Stakeholder ein:

- **Hoher Einfluss + hohes Interesse:** Eng einbinden
- **Hoher Einfluss + geringes Interesse:** Regelmäßig informieren
- **Geringer Einfluss + hohes Interesse:** Awareness schaffen
- **Geringer Einfluss + geringes Interesse:** Minimaler Aufwand

✅ 4. Rollen und Verantwortlichkeiten festlegen

Bestimme, wer welche Aufgaben übernimmt:

- Wer ist ISMS-Verantwortlicher?
- Wer trifft Entscheidungen?
- Wer muss informiert werden?

Dokumentiere diese Rollen klar und verständlich.

✅ 5. Kommunikationsbedarfe definieren

Überlege, wie Du mit den Stakeholdern kommunizierst:

- Wer bekommt regelmäßige Updates?
- Wer muss geschult werden?
- Welche Kanäle nutzt Du (E-Mail, Meetings, Intranet)?
- Wie oft wird kommuniziert?

✅ 6. Ergebnisse dokumentieren

Halte alles schriftlich fest:

- Stakeholder-Liste
- Matrix
- Rollenverteilung
- Kommunikationsplan

✅ Nutzen und Vorteil

- Du weißt genau, wer eingebunden werden muss.
- Du vermeidest Missverständnisse und Widerstände.
- Du schaffst Transparenz und Akzeptanz für Dein ISMS.

3.3. ISMS-Ziele definieren

Ein ISMS ist kein Selbstzweck. Es soll Dir helfen, **konkrete Sicherheitsziele zu erreichen**, die den Schutz Deiner Informationen systematisch verbessern. Ohne klare Ziele weiß niemand, worauf hingearbeitet wird – und ob Fortschritte erzielt werden.

Leite die Ziele deines ISMS direkt aus den NIS2-Anforderungen ab, z. B. Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit kritischer Systeme, Nachweisfähigkeit gegenüber Behörden, Sensibilisierung der Mitarbeitenden und kontinuierliche Verbesserung der Sicherheitsmaßnahmen

Warum ist das wichtig?

- Du schaffst Klarheit und Orientierung für alle Beteiligten.
- Du machst Fortschritte messbar.
- Du verankerst Informationssicherheit in der Unternehmensstrategie.

Die drei Kernprinzipien

1. **SMART-Ziele**: Spezifisch, Messbar, Attraktiv, Realistisch, Terminiert.
2. **Strategiebezug**: Ziele müssen die Unternehmensstrategie unterstützen.
3. **Regelmäßige Überprüfung**: Sicherstellen, dass Ziele aktuell und relevant bleiben.

So definierst Du ISMS-Ziele – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst festlegen, **was Dein Unternehmen im Bereich Informationssicherheit konkret erreichen soll**.
Warum? Damit Du Fortschritte sichtbar machen und gezielt steuern kannst.

✅ 2. Ziele nach dem SMART-Prinzip formulieren

Schreibe Deine Ziele so auf, dass sie:

- **Spezifisch** sind: Was genau soll erreicht werden?
- **Messbar** sind: Woran erkennst Du, ob das Ziel erreicht wurde?
- **Attraktiv** sind: Ist das Ziel sinnvoll und motivierend?
- **Realistisch** ist: Ist es mit den vorhandenen Mitteln erreichbar?
- **Terminiert** ist: Bis wann soll das Ziel erreicht sein?

Beispiel:
„Bis zum 30.06. sollen 90 % der Mitarbeitenden eine IT-Sicherheitsschulung abgeschlossen haben."

✅ 3. Ziele mit der Unternehmensstrategie verknüpfen

Überlege: **Wie unterstützen die Sicherheitsziele die Gesamtziele Deines Unternehmens?**
Beispiel:
Strategisches Ziel: „Vertrauen bei Kunden stärken"
ISMS-Ziel: „Einführung von Zwei-Faktor-Authentifizierung für alle Kundenkonten."

✅ 4. Ziele regelmäßig überprüfen

Lege fest, wann und wie oft Du die Ziele überprüfst – z. B. alle 3 Monate oder im Rahmen von Management-Reviews.
Prüfe:

- Sind die Ziele noch aktuell?
- Wurden sie erreicht?
- Müssen neue Ziele definiert werden?

✅ 5. Ziele dokumentieren

Halte alle Ziele schriftlich fest – am besten in einem zentralen ISMS-Dokument (das ISMS-Handbuch (folgt später noch)).
Notiere auch:

- Wer für die Umsetzung verantwortlich ist
- Wie der Fortschritt gemessen wird

✅ Nutzen und Vorteil

- Du schaffst Klarheit und Orientierung.
- Du kannst Fortschritte sichtbar machen und gezielt steuern.
- Du verankerst Informationssicherheit strategisch im Unternehmen – nicht nur als Pflicht, sondern als echten Mehrwert.

3.4. Scope des ISMS festlegen - Den Geltungsbereich klar definieren

Bevor Du Dein ISMS einführst, musst Du festlegen, **wo es gilt und wo nicht**. Der sogenannte „Scope" beschreibt den Geltungsbereich des ISMS – also die Standorte, Organisationseinheiten, IT-Systeme, Prozesse und Dienstleistungen, die einbezogen werden.

Definiere den Geltungsbereich deines ISMS mit Blick auf die NIS2-relevanten Systeme, Prozesse und Infrastrukturen. Dokumentiere, welche Bereiche, Standorte und IT-Systeme vom ISMS abgedeckt werden und warum

Warum ist das wichtig? Damit Du Ressourcen gezielt einsetzt und keine unnötige Arbeit in Bereichen machst, die nicht betroffen sind.

Warum ist ein klarer Scope entscheidend?

- Du schaffst Transparenz und Fokus.
- Du vermeidest unnötigen Aufwand.
- Du legst die Basis für eine spätere Erweiterung des ISMS.

So definierst Du den Scope – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst festlegen, **welche Teile Deines Unternehmens vom ISMS abgedeckt werden sollen**.
Warum? Damit klar ist, wo Sicherheitsmaßnahmen greifen – und wo nicht.

✅ 2. Überlege, was geschützt werden soll

Stelle Dir folgende Fragen:

- **Standorte:** Zentrale, Niederlassungen, Homeoffice?

- **IT-Systeme:** Server, Netzwerke, Anwendungen, Datenbanken?
- **Prozesse:** Kundenservice, Buchhaltung, Produktentwicklung?
- **Organisationseinheiten:** IT, HR, Vertrieb, Produktion?

✅ 3. Grenzen klar ziehen

Entscheide, **was nicht zum Scope gehört** – z. B.:

- Externe Partner
- Bestimmte Standorte oder Systeme mit geringer Relevanz
  Notiere auch die Gründe für den Ausschluss (z. B. separate Sicherheitsregelungen).

✅ 4. Scope schriftlich festhalten

Erstelle eine kurze Beschreibung:

- Was ist im Scope enthalten?
- Was ist ausgeschlossen?
- Warum wurde dieser Umfang gewählt?

Dokumentiere den Scope im **ISMS-Handbuch** oder einem zentralen Projekt-Dokument.

✅ 5. Scope mit Beteiligten abstimmen

Besprich den Scope mit:

- Geschäftsführung
- IT-Abteilung
- Weitere relevante Teams
  Hole eine **Freigabe** ein – damit alle wissen, worauf sich das ISMS bezieht.

✅ Nutzen und Vorteil

- Du schaffst Klarheit und Fokus.
- Du setzt Ressourcen effizient ein.
- Du legst eine skalierbare Basis für spätere Erweiterungen.

3.5. Lieferantenmanagement & Sicherheitsanforderungen für externe Dienstleister

Die NIS2-Richtlinie verschärft die Anforderungen an das Management von Lieferanten und externen Dienstleistern. Der Grund: Viele Sicherheitsvorfälle entstehen nicht in der eigenen IT-Infrastruktur, sondern durch Schwachstellen in der Lieferkette. Besonders betroffen sind Softwarehersteller, Cloud-Anbieter sowie Managed Service Provider (MSP/MSSP).

NIS2 verlangt deshalb, dass Unternehmen die Sicherheit externer Partner aktiv steuern, überwachen und regelmäßig bewerten.

IT-Sicherheit endet nicht an der Unternehmensgrenze. Lieferanten können erhebliche Risiken darstellen:

- unsichere Softwareupdates
- kompromittierte Identitäten oder Remote-Zugänge
- Cloud-Ausfälle
- fehlerhafte Wartungsarbeiten
- fehlende Verschlüsselung oder Logging
- unzureichende Notfall- und Wiederanlaufkonzepte

Ein unkontrollierter Drittanbieter kann die gesamte Organisation gefährden – und die Verantwortung liegt bei der Geschäftsleitung.

✅ 1. Erweiterte Anforderungen an das Lieferantenmanagement

NIS2 fordert einen **systematischen, dokumentierten Umgang mit Lieferkettenrisiken**:

- vertragliche Absicherung
- Risikoanalysen
- regelmäßige Kontrollen
- klare Sicherheitsvorgaben
- Nachweisführung

✅ 2. Sicherheitsanforderungen an externe Dienstleister

Je kritischer ein Dienst, desto höher die Sicherheitsanforderungen.
Besonders relevant:

- Cloud-Anbieter
- Softwarelieferanten
- MSP/MSSP
- Hosting-Provider
- Outsourcing-Partner

✅ Erweiterte Anforderungen an das Lieferantenmanagement

1. Vertragliche Pflichten

Verträge mit kritischen Lieferanten müssen Sicherheitsklauseln enthalten:

- Einhaltung relevanter Normen (z. B. ISO 27001)
- Pflicht zur Meldung sicherheitsrelevanter Vorfälle (SLO: 2–12 Stunden)
- Nachweis regelmäßiger Penetrationstests
- Regelung zur Nutzung von Unterauftragnehmern
- Zugriffsschutz (VPN, MFA, Zero Trust)
- Logging und Aufbewahrungsfristen
- Backup- und Wiederherstellungsverfahren
- Exit-Strategien (Datenrückgabe, Schattenbetrieb)
- Audit- und Prüfungsrechte

2. Risikoanalyse für Lieferanten

Lieferanten müssen nach Risikoprofil bewertet werden:

- Kritikalität des Dienstes
- Zugriff auf Systeme oder Daten
- geografische Risiken (z. B. Hosting außerhalb EU)
- Abhängigkeit (Single Point of Failure)
- bisherige Sicherheitsvorfälle
- Sicherheitsreife (ISO 27001, SOC2, TISAX)
- Notfall- und Wiederanlaufkonzepte

Die Analyse ist schriftlich zu dokumentieren und jährlich zu aktualisieren.

3. Regelmäßige Überprüfung und Monitoring

NIS2 fordert laufende Überwachung kritischer Lieferanten:

- jährliche Sicherheitsabfragen oder Audits
- Review von Zertifikaten und Prüfberichten
- Kontrolle der SLAs/SLOs
- Test der Meldewege bei Sicherheitsvorfällen
- Überprüfung der Notfallprozesse
- Bewertung von Änderungen (Standorte, Outsourcing, Softwareversionen)

✅ Sicherheitsanforderungen an externe Dienstleister

1. MSP/MSSP

Risiken: privilegierte Zugriffe, Konfiguration kritischer Systeme, operative Sicherheitsaufgaben.
Pflichten:

- durchgängige MFA
- Zero-Trust-Kontrollen
- rollenbasierte Zugriffsbeschränkungen
- Protokollierung aller Admin-Aktivitäten
- Pflicht zur Vorfallmeldung
- Nachweis sicherer Betriebsprozesse
- gemeinsame Notfallübungen

2. Cloud-Dienstleister

Pflichten:

- Transparenz über Speicherort und Zugriffe
- ISO 27001/27017/27018-konforme Maßnahmen
- Exit-Strategien
- Absicherung der API-Zugriffe
- Logging auf Tenant-Ebene
- regelmäßige Sicherheitsreports
- Nachweis von Notfallprozessen

3. Softwarelieferanten

Pflichten:

- Secure Development Lifecycle (SDLC)
- Patch-Management

- Signatur und Validierung von Updates
- SBOM (Software Bill of Materials)
- regelmäßige Sicherheitsbewertungen
- verpflichtende Incident-Meldungen

SBOM ist unter NIS2 ein zentraler Kontrollpunkt gegen Supply-Chain-Angriffe.

3.6. Kontext der Organisation analysieren – Rahmenbedingungen für Informationssicherheit verstehen

Bevor Du Dein ISMS planst, musst Du wissen, **in welchem Umfeld Dein Unternehmen agiert**. Informationssicherheit hängt stark von internen und externen Faktoren ab. Ziel ist es, diese Einflussfaktoren systematisch zu erfassen, um Dein ISMS passgenau auszurichten.

Analysiere interne und externe Einflussfaktoren, die für die Umsetzung der NIS2-Anforderungen relevant sind. Berücksichtige gesetzliche und regulatorische Vorgaben, branchenspezifische Besonderheiten und aktuelle Bedrohungslagen

Warum ist das wichtig?

- Du erkennst Risiken und Chancen frühzeitig.
- Du planst Dein ISMS passend zur Unternehmenssituation.
- Du erfüllst gesetzliche und regulatorische Anforderungen.

Die drei Kernbausteine

1. **SWOT-Analyse**: Stärken, Schwächen, Chancen, Risiken.
2. **PESTEL-Analyse**: Politische, wirtschaftliche, soziale, technologische, ökologische und rechtliche Faktoren.
3. **Regulatorische Anforderungen**: Gesetze und branchenspezifische Vorgaben.

So analysierst Du den Kontext – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst herausfinden, **welche internen und externen Faktoren Deine Informationssicherheit beeinflussen**.
Warum? Damit Du Dein ISMS nicht „blind" planst, sondern passend zu Deiner Unternehmensrealität.

✅ 2. SWOT-Analyse durchführen

Erstelle eine Tabelle mit vier Feldern:

- **Stärken:** Was läuft gut? (z. B. engagiertes IT-Team, gute Infrastruktur)
- **Schwächen:** Wo gibt es Lücken? (z. B. keine Schulungen, veraltete Systeme)
- **Chancen:** Was kannst Du nutzen? (z. B. neue Technologien, Förderprogramme)
- **Risiken:** Was gefährdet Deine Sicherheit? (z. B. Cyberangriffe, Fachkräftemangel)

✅ 3. PESTEL-Analyse erstellen

Notiere externe Einflüsse aus sechs Bereichen:

- **Politisch:** Neue Gesetze, staatliche Förderungen?
- **Wirtschaftlich:** Budgetgrenzen, Marktveränderungen?
- **Sozial:** Erwartungen von Kunden oder Mitarbeitenden?
- **Technologisch:** Neue IT-Trends, Sicherheitslücken?
- **Ökologisch:** Umweltauflagen, Nachhaltigkeitsanforderungen?
- **Rechtlich:** Datenschutzgesetze, branchenspezifische Normen?

✅ 4. Regulatorische Anforderungen prüfen

Sammle alle relevanten Vorgaben:

- DSGVO (Datenschutz)
- IT-Sicherheitsgesetz
- Branchenstandards (z. B. NIS2, KRITIS, PCI-DSS)
  Prüfe, welche davon für Dein Unternehmen gelten.

✅ 5. Ergebnisse dokumentieren

Halte Deine SWOT- und PESTEL-Analyse schriftlich fest.
Füge die Erkenntnisse in Dein **ISMS-Handbuch** oder ein zentrales Projekt-Dokument ein.

✅ Nutzen und Vorteil

- Du verstehst, welche Faktoren Deine Informationssicherheit beeinflussen.
- Du planst Dein ISMS gezielt und realistisch.
- Du vermeidest Überraschungen und erfüllst Compliance-Anforderungen frühzeitig.

3.7. Business-, Management- und Unterstützungs-prozesse identifizieren

Ein wirksames ISMS braucht ein klares Bild Deiner Abläufe. **Warum?** Weil Du nur Risiken analysieren kannst, wenn Du weißt, welche Prozesse kritisch sind. Ziel ist es, eine solide Grundlage für die spätere **Asset-Identifikation** und **Risikoanalyse** zu schaffen.

Warum ist das wichtig?

- Du erkennst, wo sensible Daten verarbeitet werden.
- Du kannst kritische Prozesse priorisieren.
- Du legst die Basis für ein risikoorientiertes ISMS.

Die zwei Kernbausteine

1. **Prozesslandkarte**: Visualisierung aller relevanten Prozesse.
2. **Priorisierung**: Identifikation kritischer Prozesse mit hohem Schutzbedarf.

So gehst Du vor – Schritt für Schritt 

✅ 1. Verstehe Dein Ziel

Du willst herausfinden, **welche Abläufe im Unternehmen wichtig sind**, damit Du später gezielt Risiken erkennen und Schutzmaßnahmen planen kannst.

✅ 2. Prozesse sammeln

Erstelle eine Liste aller Abläufe:

- **Geschäftsprozesse:** Kundenservice, Vertrieb, Produktion, Projektabwicklung
- **Managementprozesse:** Planung, Controlling, Qualitätsmanagement
- **Unterstützungsprozesse:** IT-Betrieb, Personalwesen, Einkauf, Facility Management

✅ 3. Prozesslandkarte erstellen

Visualisiere die Prozesse:

- Welche Prozesse gibt es?
- Wie hängen sie zusammen?
- Wer ist verantwortlich?

Darstellungsmöglichkeiten:

- Tabelle
- Diagramm
- Flussmodell

✅ 4. Kritische Prozesse priorisieren

Bewerte, welche Prozesse besonders wichtig sind:

- Verarbeiten sie sensible Daten?
- Sind sie stark von IT abhängig?
- Was passiert bei einem Ausfall?

Markiere diese Prozesse als **kritisch** – sie brauchen später besondere Aufmerksamkeit.

✅ 5. Ergebnisse dokumentieren

Halte Deine Prozessliste und Priorisierung schriftlich fest.

Füge die Informationen in Dein **ISMS-Handbuch** oder ein zentrales Projekt-Dokument ein.

✅ Nutzen und Vorteil

- Du bekommst einen klaren Überblick über Deine Abläufe.
- Du kannst später gezielt Risiken analysieren und wichtige Prozesse schützen.
- Du schaffst eine strukturierte Grundlage für Dein gesamtes ISMS.

3.8. Asset-Identifikation & Schutzbedarfsanalyse – Was muss geschützt werden und wie dringend?

Ein ISMS funktioniert nur, wenn Du weißt, **was geschützt werden muss**. Assets sind alle Werte, die für Dein Unternehmen wichtig sind – von Datenbanken über IT-Systeme bis hin zu Dokumenten und Personen mit sensiblen Zugriffsrechten. Ziel ist es, diese Assets zu erfassen, ihren Schutzbedarf zu bewerten und sie in Schutzklassen einzuordnen.

Warum ist das wichtig?

- Du erkennst, welche Assets besonders kritisch sind.
- Du kannst Sicherheitsmaßnahmen gezielt planen.
- Du erfüllst Anforderungen nachvollziehbar und auditfähig.

Die drei Kernbausteine

1. **Asset-Inventar**: Liste aller relevanten Informationswerte inkl. Eigentümer.
2. **Schutzbedarfsanalyse**: Bewertung nach dem CIA-Prinzip (Vertraulichkeit, Integrität, Verfügbarkeit).
3. **Klassifizierungssystem**: Einteilung in Schutzklassen.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst herausfinden, **welche Werte (Assets) geschützt werden müssen** und wie dringend.
Warum? Damit Du Risiken erkennst und Prioritäten setzen kannst.

✅ 2. Asset-Inventar erstellen

Im ISMS werden **Assets** nach ihrer Rolle und Abhängigkeit unterschieden:

- **Primäre Assets**
  Das sind die eigentlichen Informationswerte, die geschützt werden müssen – z. B. Kundendaten, Geschäftsgeheimnisse, Finanzinformationen.
  Frage: Was ist für das Unternehmen geschäftskritisch?
- **Sekundäre Assets**
  Unterstützende Ressourcen, die für die Verarbeitung oder Speicherung der primären Assets notwendig sind – z. B. IT-Systeme, Anwendungen, Datenbanken, Netzwerke.
  Frage: Welche Systeme ermöglichen den Zugriff auf die Informationen?
- **Tertiäre Assets**
  Physische und organisatorische Infrastruktur, die sekundäre Assets absichert – z. B. Gebäude, Serverräume, Stromversorgung, Personal, Prozesse.
  Frage: Was sorgt dafür, dass Systeme und Informationen verfügbar und geschützt bleiben?

Merke:
Primär = Information selbst
Sekundär = Technik zur Verarbeitung
Tertiär = Umgebung und Organisation

Erfasse alle wichtigen Assets:

- **Aufteilung** in primäre, sekundäre und tertiäre Assets
- **IT-Systeme:** Server, PCs, Netzwerke
- **Datenbanken:** Kundendaten, Verträge

- **Dokumente:** Rechnungen, interne Richtlinien
- **Personen:** Mitarbeitende mit Zugang zu sensiblen Daten

Notiere für jedes Asset den **Eigentümer**, der für Schutz und Pflege verantwortlich ist.

✅ 3. Schutzbedarf bewerten (CIA-Prinzip)

Für jedes Asset prüfe:

- **Vertraulichkeit:** Muss verhindert werden, dass Unbefugte Zugriff haben?
- **Integrität:** Müssen Daten korrekt und unverändert bleiben?
- **Verfügbarkeit:** Muss das Asset jederzeit nutzbar sein?

Bewerte jede Kategorie als **niedrig, mittel oder hoch**.

✅ 4. Klassifizierungssystem anwenden

Ordne jedes Asset einer Schutzklasse zu:

- **Öffentlich** – keine besonderen Schutzmaßnahmen
- **Intern** – nur für Mitarbeitende
- **Vertraulich** – eingeschränkter Zugriff
- **Streng vertraulich** – besonders geschützt

Dokumentiere, wie mit jeder Klasse umgegangen wird (Zugriff, Speicherung, Weitergabe).

✅ 5. Ergebnisse dokumentieren

Halte fest:

- Asset-Liste
- Schutzbedarfsbewertung
- Klassifizierung

Speichere alles im **ISMS-Handbuch** oder einem zentralen Dokument.

✅ Nutzen und Vorteil

- Du weißt genau, was besonders geschützt werden muss.
- Du kannst Sicherheitsmaßnahmen gezielt planen.
- Du erfüllst NIS2-Anforderungen – transparent und auditfähig.

3.9. Sicherheitsleitlinie erstellen und veröffentlichen

Die Sicherheitsleitlinie ist das Fundament Deines ISMS. Sie definiert die **Prinzipien, Ziele und Verpflichtungen** Deiner Organisation im Umgang mit Informationssicherheit. Ziel ist es, eine verbindliche Grundlage zu schaffen, die Orientierung bietet und das Sicherheitsbewusstsein im Unternehmen stärkt.

Warum ist das wichtig?

- Sie zeigt, dass Informationssicherheit Chefsache ist.
- Sie schafft Verbindlichkeit und Orientierung für alle Mitarbeitenden.
- Sie ist ein zentraler Nachweis für Audits und Zertifizierungen.

Die zwei Kernbausteine

1. **Management-Commitment**: Sichtbare Unterstützung durch die Unternehmensleitung.
2. **Kommunikation & Schulung**: Veröffentlichung und Erklärung der Leitlinie für alle Mitarbeitenden.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst eine Leitlinie erstellen, die klar beschreibt, **wie Dein Unternehmen mit Informationssicherheit umgeht**.
Warum? Damit alle wissen, was Sicherheit bedeutet und wer verantwortlich ist.

✅ 2. Management-Commitment einholen

- Sprich mit der Geschäftsleitung und erkläre:
  - Warum die Leitlinie wichtig ist
  - Was darin stehen soll
  - Wie sie das Unternehmen schützt
- Hole eine **offizielle Zustimmung** ein – z. B. durch Unterschrift oder interne Freigabe.

✅ 3. Leitlinie formulieren

Schreibe die Leitlinie **klar und verständlich**. Sie sollte enthalten:

- Warum Informationssicherheit wichtig ist
- Welche Ziele verfolgt werden
- Wer Verantwortung trägt
- Wie mit Risiken und Vorfällen umgegangen wird
- Wie die Sicherheit kontinuierlich verbessert wird

✅ 4. Leitlinie veröffentlichen

Mache die Leitlinie für alle zugänglich:

- Im Intranet
- Per E-Mail
- Als Aushang in zentralen Bereichen
  Speichere sie auch im **ISMS-Handbuch** oder Dokumentenmanagementsystem.

✅ 5. Mitarbeitende informieren und schulen

Organisiere kurze Schulungen oder Info-Sessions:

- Was steht in der Leitlinie?
- Was bedeutet das für den Arbeitsalltag?
- Was muss jede*r beachten?

Dokumentiere die Teilnahme – z. B. mit einer Unterschriftenliste oder digitalem Nachweis.

✅ Nutzen und Vorteil

- Alle wissen, was Informationssicherheit bedeutet.
- Die Geschäftsleitung zeigt, dass sie das Thema ernst nimmt.
- Die Leitlinie schafft Verbindlichkeit und Orientierung – für Mitarbeitende, Partner und Auditoren.

3.10. Erstellung spezifischer Richtlinien Sicherheitsprinzipien in konkrete Vorgaben übersetzen

Nachdem die Sicherheitsleitlinie die Grundsätze festgelegt hat, musst Du diese nun in **konkrete Regeln für den Alltag** überführen. Ziel ist es, klare Vorgaben zu schaffen, die Mitarbeitenden helfen, sich sicher zu verhalten – und die technische sowie organisatorische Maßnahmen einheitlich umsetzen.

Warum ist das wichtig?

- Du schaffst klare Regeln für den sicheren Umgang mit Informationen und IT.
- Du reduzierst Risiken und Fehler.
- Du erfüllst NIS2-Anforderungen nachvollziehbar und auditfähig.

Typische Richtlinien

- **Zugriffskontrolle**
- **Mobile Geräte**
- **Kryptografie**
- **Backup & Recovery**

⚠️ **Wichtiger Hinweis:**
Diese Richtlinien sind **nur Beispiele**. Die NIS2 fordert eine Vielzahl weiterer Richtlinien, die je nach Unternehmenskontext relevant sind – z. B. für **Cloud-Nutzung**, **KI-Systeme**, **Lieferantenmanagement**, **Netzwerksicherheit** oder **Incident-Management**.
Stelle sicher, dass Du alle relevanten Themen für Dein Unternehmen abdeckst.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst aus der allgemeinen Leitlinie **konkrete Regeln ableiten**, damit klar ist, was erlaubt ist und was nicht.

✅ 2. Zugriffskontrolle regeln

Definiere:

- Wer darf auf welche Daten und Systeme zugreifen?
- Wie werden Zugriffsrechte vergeben, geändert und gelöscht?
- Wie werden Passwörter und Benutzerkonten verwaltet?

Dokumentiere alles in einer **Zugriffsrichtlinie**.

✅ 3. Umgang mit mobilen Geräten festlegen

Bestimme:

- Welche Geräte dürfen genutzt werden?
- Welche Sicherheitsmaßnahmen sind Pflicht (z. B. PIN, Verschlüsselung)?
- Was passiert bei Verlust oder Diebstahl?

Erstelle eine **Mobile-Device-Richtlinie**.

✅ 4. Kryptografie-Richtlinie erstellen

Lege fest:

- Wann müssen Daten verschlüsselt werden?
- Welche Verfahren sind erlaubt?
- Wie werden Schlüssel sicher verwaltet?

Dokumentiere in einer **Kryptografie-Richtlinie**.

✅ 5. Backup & Recovery regeln

Definiere:

- Welche Daten müssen gesichert werden?
- Wo werden Backups gespeichert?
- Wie oft werden Wiederherstellungen getestet?

Erstelle eine **Backup- und Recovery-Richtlinie**.

✅ 6. Weitere Richtlinien ergänzen

Prüfe, ob zusätzliche Themen relevant sind:

- **Cloud-Nutzung** (z. B. Zugriff, Verschlüsselung, Provider-Risiken)
- **KI-Systeme** (z. B. Datenschutz, Bias, Modell-Updates)
- **Lieferantenmanagement**
- **Netzwerksicherheit**
- **Security-Incident-Management**

✅ 7. Richtlinien veröffentlichen und schulen

- Stelle die Richtlinien im Intranet oder per E-Mail bereit.
- Führe kurze Schulungen durch:
    - Was bedeuten die Richtlinien?
    - Was muss im Alltag beachtet werden?

Dokumentiere die Teilnahme.

✅ Nutzen und Vorteil

- Du schaffst klare Regeln für den sicheren Umgang mit Informationen und IT.
- Mitarbeitende wissen, was erlaubt ist und was nicht.
- Du erfüllst NIS2-Anforderungen – transparent und auditfähig.

3.11. Risiko-Management – Risiken erkennen, bewerten und steuern

Ein ISMS basiert auf einem risikoorientierten Ansatz. Das bedeutet: Du musst wissen, **welche Risiken für Deine Informationssicherheit bestehen**, wie groß ihre Auswirkungen sind und wie Du sie behandeln willst. Ziel ist es, Risiken systematisch zu identifizieren, zu bewerten und geeignete Maßnahmen festzulegen.

Setze ein risikobasiertes Managementsystem auf, das alle NIS2-Anforderungen erfüllt: Identifikation, Bewertung und Behandlung von Risiken, regelmäßige Überprüfung und Dokumentation

Warum ist das wichtig?

- Du erkennst Bedrohungen und Schwachstellen frühzeitig.
- Du kannst Sicherheitsmaßnahmen gezielt und effizient planen.
- Du erfüllst zentrale Normanforderungen – transparent und auditfähig.

Die drei Kernbausteine

1. **Risiko-Identifikation**: Welche Bedrohungen und Schwachstellen gibt es?
2. **Risiko-Bewertung**: Wie wahrscheinlich ist der Eintritt, wie groß die Auswirkung?
3. **Risiko-Behandlung**: Welche Maßnahmen reduzieren das Risiko auf ein akzeptables Niveau?

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst Risiken erkennen, bewerten und steuern – nicht nur dokumentieren, sondern aktiv managen.

✅ 2. Risiken identifizieren

- Sammle alle potenziellen Risiken für Deine Informationssicherheit:
  - Technische Risiken (z. B. Systemausfall, Malware)
  - Organisatorische Risiken (z. B. fehlende Rollen, unklare Prozesse)
  - Menschliche Risiken (z. B. Social Engineering, Fehlbedienung)
  - Externe Risiken (z. B. Lieferantenausfall, regulatorische Änderungen)

✅ 3. Risiken bewerten

- Nutze eine einfache Skala für **Eintrittswahrscheinlichkeit** und **Auswirkung** (z. B. niedrig, mittel, hoch).
- Berechne den **Risikowert** (z. B. Wahrscheinlichkeit × Auswirkung).
- Priorisiere die Risiken: Hohe Werte zuerst behandeln.

✅ 4. Maßnahmen festlegen

Für jedes Risiko:

- Definiere eine **Behandlungsstrategie**:
  - Vermeiden
  - Reduzieren
  - Übertragen (z. B. Versicherung)
  - Akzeptieren
- Lege konkrete Maßnahmen fest (z. B. Firewall-Update, Schulung, Backup-Konzept).
- Bestimme Verantwortliche und Fristen.

✅ 5. Risiko-Register führen

Das Risiko-Register ist das zentrale Dokument für Dein Risikomanagement. Es sollte folgende Spalten enthalten:

Spalte	Inhalt
Risiko-ID	Eindeutige Kennung
Risiko-Beschreibung	Kurze Beschreibung des Risikos
Kategorie	Technisch, organisatorisch, menschlich, extern
Eintrittswahrscheinlichkeit	Niedrig / Mittel / Hoch
Auswirkung	Niedrig / Mittel / Hoch
Risikowert	Berechneter Wert (z. B. Skala 1–9)
Maßnahmen	Geplante oder umgesetzte Maßnahmen
Verantwortlich	Wer ist zuständig?
Status	Offen / In Umsetzung / Erledigt
Rest-Risiko	Bewertung nach Umsetzung der Maßnahmen

✅ 6. Ergebnisse dokumentieren und überwachen

- Speichere das Risiko-Register im ISMS-Handbuch oder einem zentralen Tool.
- Überprüfe regelmäßig:
  - Sind neue Risiken hinzugekommen?
  - Wurden Maßnahmen umgesetzt?
  - Muss die Bewertung angepasst werden?

✅ Nutzen und Vorteil

- Du erkennst Risiken frühzeitig und steuerst sie aktiv.
- Du kannst Ressourcen gezielt einsetzen – dort, wo das größte Risiko besteht.
- Du erfüllst NIS2-Anforderungen – transparent und auditfähig.

3.12. Definition der ISMS-Prozesse – Sicherheitsrelevante Abläufe systematisch steuern

Ein ISMS lebt nicht nur von Dokumenten und Richtlinien, sondern vor allem von **klar definierten Prozessen**. Diese Prozesse sorgen dafür, dass Sicherheitsmaßnahmen im Alltag wirksam umgesetzt, überwacht und verbessert werden. Ziel ist es, sicherheitsrelevante Abläufe zu identifizieren, zu strukturieren und verbindlich zu regeln.

Definiere und dokumentiere alle sicherheitsrelevanten Abläufe (z. B. Incident Management, IT-Change-Management, Supplier Management, Awareness-Management) und stelle sicher, dass sie den NIS2-Vorgaben entsprechen.

Warum ist das wichtig?

- Du schaffst Struktur und Verlässlichkeit.
- Du stellst sicher, dass Informationssicherheit nicht dem Zufall überlassen wird.
- Du erfüllst zentrale Anforderungen nachvollziehbar und auditfähig.

Typische ISMS-Prozesse

- **Incident Management**
- **IT Change Management**
- **Supplier Management**
- **Risiko Management**

⚠️ **Wichtiger Hinweis:**
Diese Prozesse sind **nur Beispiele**. NIS2 und die Praxis erfordern weitere Abläufe, die je nach Unternehmenskontext relevant sind – z. B. für **Cloud-Services**, **KI-Systeme**, **Notfallmanagement**, **Compliance-Überwachung** oder

Awareness-Kampagnen.

Stelle sicher, dass Du alle relevanten Prozesse für Dein Unternehmen definierst.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst festlegen, **wie sicherheitsrelevante Abläufe im Unternehmen ablaufen sollen** – z. B. bei Vorfällen, Änderungen oder Risiken.

✅ 2. Incident Management-Prozess definieren

Regle:

- Was ist ein Sicherheitsvorfall? Und was ist ein Sicherheits-Event?
- Wer muss informiert werden?
- Wie wird dokumentiert und nachverfolgt?
- Was passiert danach (Analyse, Maßnahmen)?

Erstelle eine **einfache Anleitung für Mitarbeitende**: „Was tun im Ernstfall?“

✅ 3. IT Change Management-Prozess festlegen

Definiere:

- Welche Änderungen müssen geprüft werden?
- Wer darf Änderungen freigeben?
- Wie wird dokumentiert, was geändert wurde?

Ziel: **Sicherstellen, dass Änderungen keine neuen Risiken verursachen.**

✅ 4. Supplier Management-Prozess einführen

Regle:

- Wie werden Dienstleister ausgewählt?
- Welche Sicherheitsanforderungen müssen sie erfüllen?
- Wie wird ihre Leistung regelmäßig überprüft?

Dokumentiere alle relevanten Verträge und Vereinbarungen.

✅ 5. Risk Management-Prozess aufsetzen

Lege fest:

- Wie werden Risiken erkannt und bewertet?
- Welche Maßnahmen werden ergriffen?
- Wie oft wird alles überprüft?

Nutze **Tabellen oder Tools zur Risikobewertung**.

✅ 6. Weitere Prozesse ergänzen

Prüfe zusätzliche Themen:

Prozessname	Beschreibung
Incident Management	Erkennung, Meldung, Analyse und Behandlung von Sicherheitsvorfällen.
IT Change Management	Sichere Durchführung und Dokumentation von Änderungen an IT-Systemen und Prozessen.
Supplier Management	Auswahl, Bewertung und Überwachung von Lieferanten im Hinblick auf Sicherheitsanforderungen.
Risk Management	Identifikation, Bewertung, Behandlung und Überwachung von Risiken.
Cloud Security Management	Regelung der sicheren Nutzung von Cloud-Diensten, inkl. Zugriff, Verschlüsselung und Compliance.
KI-Governance	Festlegung von Richtlinien und Prozessen für den sicheren Einsatz von KI-Systemen.
Notfallmanagement	Planung und Durchführung von Maßnahmen zur Aufrechterhaltung des Betriebs bei Störungen.
Compliance-Überwachung	Überprüfung der Einhaltung gesetzlicher, regulatorischer und interner Anforderungen.
Awareness-Management	Schulung und Sensibilisierung der Mitarbeitenden für Informationssicherheit.
Patch-Management	Regelmäßige Aktualisierung von Systemen und Anwendungen zur Schließung von Sicherheitslücken.
Asset-Management	Erfassung und Verwaltung aller relevanten Informationswerte und deren Eigentümer.
Backup & Recovery	Regelmäßige Datensicherung und Wiederherstellung im Notfall.
Zugriffskontrolle	Regelung von Benutzerzugriffen, Rollen und Berechtigungen.
Datenschutz-Management	Sicherstellung der Einhaltung von Datenschutzgesetzen und -richtlinien.

✅ 7. Prozesse dokumentieren und schulen

- Schreibe die Prozesse klar und verständlich auf.
- Schulen:
  - Was ist die Rolle der Mitarbeitenden?
  - Was müssen sie beachten?

✅ Nutzen und Vorteil

- Du schaffst klare Abläufe für den Umgang mit sicherheitsrelevanten Themen.
- Mitarbeitende wissen, was zu tun ist – schnell und sicher.
- Du erfüllst zentrale Anforderungen der ISO/IEC 27001 – transparent und auditfähig.

3.13. Meldepflichten von Cyberangriffen

Die NIS2-Richtlinie verschärft die Anforderungen an die Meldung sicherheitsrelevanter Vorfälle erheblich. Ziel ist, dass Behörden frühzeitig informiert werden, um sektorübergreifend reagieren zu können. Für Unternehmen bedeutet das: **ein klar definierter Meldeprozess, feste Fristen und eine konsistente interne Eskalation**.

Warum ist das wichtig?

Meldepflichten sind nicht optional. Verstöße führen zu Bußgeldern und gefährden das Vertrauen von Kunden, Partnern und Aufsichtsbehörden.
Ein funktionierendes Meldesystem sorgt dafür, dass kritische Informationen schnell zusammenfließen und korrekt kommuniziert werden – intern wie extern.
Frühe Meldung ist Pflicht – auch bei Verdacht. NIS2 erwartet keine perfekte Meldung, sondern eine schnelle.

✅ 1. Dreistufiges Meldeverfahren (Pflicht nach NIS2)

Erstmeldung (≤ 24 Stunden)

- erfolgt auch bei begründetem Verdacht
- Ziel: Behörden frühzeitig informieren
- Inhalt:
  - Art des Vorfalls
  - vermutete Ursache
  - erste Einschätzung der Auswirkungen
  - eingeleitete Sofortmaßnahmen
  - Kontaktperson

Hauptmeldung (≤ 72 Stunden)

- detaillierte technische Informationen
- Inhalt:
    - bestätigte Fakten
    - Auswirkungen
    - betroffene Systeme
    - Indikatoren für Kompromittierung (IOCs)
    - Angriffsvektor
    - Risikoentwicklung
    - Kommunikationsstatus

Abschlussmeldung (≤ 30 Tage)

- finaler Bericht nach Analyse
- Inhalt:
    - Ursache / Root Cause
    - Impact-Analyse
    - nachhaltige Maßnahmen
    - Lessons Learned
    - Präventionsmaßnahmen

Tipp: Ein Ransomware-Verdacht reicht für die Erstmeldung. Warten ist ein Compliance-Risiko.

✅ 2. Prozessbeschreibung: Wer meldet? Wie läuft die Eskalation?

Rollen:

- ISB / CISO – fachlich verantwortlich
- Incident Manager – operative Steuerung
- BCM-/Krisenstab – bei Betriebsrelevanz
- Compliance / Legal – regulatorische Prüfung
- Management – finale Freigabe

Eskalationskette:

1. Erkennung / Verdacht (Monitoring, SOC, Meldung durch Mitarbeitende)
2. Erste Bewertung (0–2 Stunden) – Kritikalität, NIS2-Relevanz
3. Eskalationsentscheidung (≤ 4 Stunden) – sofortige Info an ISB + Management
4. Interne Lagebewertung (≤ 12 Stunden) – technische Analyse, Risikoabschätzung
5. Erstmeldung (≤ 24 Stunden) – Meldung an BSI
6. Hauptmeldung (≤ 72 Stunden)
7. Abschlussbericht (≤ 30 Tage)

✅ 3. Schnittstellen zum BSI

- Meldung über BSI-Portale
- Rückfragen zu technischen Details
- Austausch von IOCs
- Teilnahme an Lagebildgesprächen
- Anordnung weiterer Maßnahmen

Wichtig: Organisationen müssen **24/7 erreichbar** sein.

Pflichtartefakte / Nachweise

- dokumentierter Meldeprozess (Flowchart + Rollenbeschreibung)
- Checkliste für NIS2-Relevanzbewertung
- Vorlagen für 24h-, 72h- und 30-Tage-Meldungen
- Nachweispaket je Vorfall (Screenshots, Logs, Tickets)
- Kommunikationsplan für regulatorische Meldungen
- Schulungsnachweise der beteiligten Rollen
- Incident- und Root-Cause-Reports

Vorlage für Meldeformulare

Erstmeldung (24h):

- Datum/Uhrzeit
- Beschreibung des Vorfalls
- betroffene Services
- erste Auswirkungen
- vermutete Ursache
- Sofortmaßnahmen
- Kontaktperson

Hauptmeldung (72h):

- technische Beschreibung
- IOCs (Hashes, IPs, Domains)
- Angriffsvektor
- zeitlicher Ablauf
- Auswirkungen
- Maßnahmen
- Risikoentwicklung

Abschlussmeldung (30 Tage):

- Ursache / Root Cause
- Impact-Analyse
- Maßnahmen
- Lessons Learned
- Prävention

3.14. Interne Audits – Die Wirksamkeit des ISMS regelmäßig überprüfen

Ein funktionierendes ISMS muss nicht nur geplant und umgesetzt, sondern auch **regelmäßig überprüft** werden. Genau hier kommen interne Audits ins Spiel. Sie sind ein zentrales Instrument zur Qualitätssicherung und helfen, **Schwachstellen frühzeitig zu erkennen**, Verbesserungen anzustoßen und die **Einhaltung** sicherzustellen.

Zusätzliche Norm: ISO 19011 – Leitfaden für Audits von Managementsystemen (empfohlen für die Durchführung interner Audits).

Warum ist das wichtig?

- Du stellst sicher, dass das ISMS nicht nur auf dem Papier existiert, sondern im Alltag gelebt wird.
- Du erkennst Risiken und Verbesserungspotenziale frühzeitig.
- Du erfüllst zentrale Normanforderungen – transparent und auditfähig.

So führst Du interne Audits durch – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst regelmäßig prüfen, **ob Dein ISMS funktioniert und eingehalten wird**. **Warum?** Damit Du Schwachstellen erkennst, bevor sie zu echten Problemen werden.

✅ 2. Auditplan erstellen

Definiere:

- **Was wird geprüft?** (z. B. Prozesse, Richtlinien, IT-Systeme)
- **Wie oft?** (z. B. jährlich oder halbjährlich)
- **Wer führt das Audit durch?** (unabhängig vom geprüften Bereich)

Dokumentiere den Plan – z. B. in einer Excel-Tabelle oder einem Auditkalender.

✅ 3. Audit vorbereiten

- Sammle relevante Unterlagen: Richtlinien, Protokolle, Nachweise (z. B. Schulungen, Zugriffslisten).
- Vereinbare Termine mit den Beteiligten.

✅ 4. Audit durchführen

Prüfe:

- Werden die ISMS-Vorgaben eingehalten?
- Gibt es Lücken oder unklare Zuständigkeiten?

Führe Interviews, prüfe Abläufe und Dokumente.
Notiere **alle Beobachtungen** – positive und kritische Punkte.

✅ 5. Auditbericht erstellen

Erstelle einen Bericht mit:

- Geprüften Bereichen
- Positiven Feststellungen
- Abweichungen und Verbesserungspotenzialen

Teile den Bericht mit der Geschäftsleitung und Verantwortlichen.

✅ 6. Maßnahmen ableiten und umsetzen

Für jede Abweichung:

- Definiere eine Maßnahme
- Bestimme Verantwortliche
- Setze eine Frist
- Verfolge die Umsetzung (z. B. mit einer Maßnahmenliste).

✅ Nutzen und Vorteil

- Du erkennst Schwachstellen frühzeitig.
- Du verbesserst Dein ISMS kontinuierlich.
- Du erfüllst ISO-Anforderungen – nachvollziehbar und auditfähig.

⚠️ **Hinweis:**

Nutze für die Planung und Durchführung von Audits die Empfehlungen der **ISO 19011**. Diese Norm bietet einen umfassenden Leitfaden für Auditprinzipien, Auditprogramme und die Kompetenz von Auditoren.

3.15. Technische und organisatorische Sicherheitsmaßnahmen – vier kritische Bereiche

NIS2 schreibt ein **nachweisbares, angemessenes Sicherheitsniveau** für alle betroffenen Unternehmen vor. Bestimmte Maßnahmen sind verpflichtend – unabhängig von Branche oder Geschäftsmodell. Die folgenden vier Bereiche gehören zu den häufigsten Prüf- und Schwachstellen:

✅ 1. Cloud-Sicherheit – Transparenz und Kontrolle sind Pflicht

Cloud-Dienste sind zentrale Bestandteile moderner IT und oft kritische Abhängigkeiten. NIS2 macht klar: Cloud-Nutzung ist ein Hochrisikothema. Unternehmen müssen Sicherheitsmaßnahmen für Cloud-Anbieter prüfen, dokumentieren und überwachen.

Kernanforderungen

- **Transparenz & Standort:** Dokumentation der Speicherorte (EU / Non-EU), Risikoanalyse für Drittstaatenzugriffe
- **Identitäts- und Berechtigungsmanagement:** MFA für alle Zugänge, RBAC, Least Privilege, Monitoring privilegierter Zugriffe
- **Technische Maßnahmen:** Verschlüsselung (Data in Transit & at Rest), Logging & Monitoring, Härtung nach CIS Benchmarks, Absicherung von APIs
- **Betriebsprozesse:** regelmäßige Compliance-Berichte (SOC2, ISO 27017/27018), Notfall- und Wiederanlaufkonzepte, Patch-Management des Providers
- **Lieferantenmanagement:** Sicherheitsklauseln in Verträgen, Incident-Meldewege, Exit-Strategien

Pflichtartefakte

- Cloud-Risikoanalyse
- Sicherheitsnachweise (SOC2, ISO 27017/27018)
- Dokumentation der Speicherorte
- Policy für Cloud-Nutzung
- Protokolle zu MFA, Logging, Hardening

✅ 2. KI-Systeme – Governance und Risikokontrolle

KI-Systeme beeinflussen zunehmend sicherheitskritische Prozesse. Fehler, Bias oder Manipulation können gravierende Folgen haben.

Kernanforderungen

- **Governance:** klare Rollen (AI Owner, Risk Manager), Management-Freigabe, Register aller produktiven KI-Systeme
- **Risikoanalyse:** Dokumentation möglicher Fehlwirkungen, Analyse von Angriffsflächen (Prompt Injection, Poisoning)
- **Monitoring:** Logging, menschliche Aufsicht (Human-in-the-loop), Mechanismen zur Fehlererkennung
- **Fairness & Bias:** Tests auf diskriminierende Muster, Transparenz der Modelle, dokumentierte Trainingsdaten

Pflichtartefakte

- KI-Risikobewertung
- Einsatzdokumentation
- Entscheidungsprotokolle
- Bias-Tests
- Betriebskonzept (Monitoring, Updates, Re-Training)

✅ 3. Notfallmanagement – Business Continuity und Disaster Recovery

NIS2 verlangt, dass Unternehmen **unterbrechungsfähige Geschäftsprozesse planen, üben und sicherstellen**.

Kernanforderungen

- **BCM:** Identifikation kritischer Prozesse (BIA), Festlegung von RTO/RPO, Notfallhandbücher
- **Disaster Recovery:** definierte Szenarien (Ransomware, Cloud-Ausfall), getestete Wiederherstellungsverfahren, Fallback-Systeme
- **Krisenmanagement:** Aktivierungsmechanismen, Kommunikationskonzepte, Rollen und Eskalationswege
- **Rückführung:** Qualitätskontrollen, Lessons Learned

Pflichtartefakte

- BCM-Policy
- BIA-Dokumentation
- Wiederanlaufpläne
- Krisenstabsordnung
- Protokolle von Tests und Übungen
- Restore-Nachweise

✅ 4. Patch- und Schwachstellenmanagement

Ungepatchte Systeme sind Hauptangriffsvektoren. NIS2 fordert ein systematisches, dokumentiertes Patch-Management.

Kernanforderungen

- **Asset-Überblick:** vollständige Systemliste, Kritikalitätsklassifizierung

- **Schwachstellenbewertung:** Vulnerability-Scanner, CVE-/CVSS-Bewertung, Priorisierung
- **Patch-Prozess:** regelmäßige Zyklen, Notfall-Patching, Tests vor Rollout, Dokumentation
- **Reporting:** KPIs, SLAs (Critical < 48–72h, High < 7–14 Tage)

Pflichtartefakte

- Patch-Policy
- Schwachstellenberichte
- Patch-Logs und Change-Tickets
- Priorisierungsdokumentation
- Testprotokolle
- Patch-Reports

3.16. Behördenkommunikation und Auditvorbereitung

Gemäß NIS2 müssen Unternehmen eine koordinierte, vollständige und termingerechte Zusammenarbeit mit den zuständigen Aufsichtsbehörden sicherstellen. Insbesondere mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).
Das umfasst:

- Meldungen bei Sicherheitsvorfällen
- Beantwortung von Prüf- und Informationsanfragen
- Teilnahme an Audits
- Bereitstellung von Nachweisen
- Pflege der Behördenkontakte

Behördenkommunikation ist kein „Nice-to-have“, sondern eine gesetzliche Pflicht.
Fehlende oder verspätete Antworten können zu Bußgeldern, verschärften Prüfungen und Reputationsschäden führen.
Ein klarer Prozess stellt sicher, dass Anfragen **schnell, vollständig und prüffähig** beantwortet werden.

✅ 1. Prozesse für behördliche Prüfungen und Anfragen

Typische Anfragen:

- Fragen zu Sicherheitsmaßnahmen (z. B. MFA, Netzwerktrennung, BCM)
- Anforderung von Nachweisen (Policies, Logs, Auditberichte)
- Prüfung der NIS2-Einstufung
- Review des Meldeverhaltens
- Ankündigung oder Durchführung eines Audits
- Rückfragen zu gemeldeten Vorfällen

Hinweis: Behörden dürfen tiefgehende technische Nachweise verlangen, inkl. Logs, Konfigurationen und Scans.

Verantwortlichkeiten

- **SPOC (Single Point of Contact):** nimmt Anfragen entgegen, koordiniert Bearbeitung, kommuniziert Rückmeldungen
- **ISB / CISO:** erstellt oder prüft Inhalte
- **Legal / Datenschutz:** prüft rechtliche Risiken
- **Management:** gibt sensible Antworten frei

Standardprozess bei Behördenanfragen

1. Eingang registrieren (Ticketsystem, DMS), Fristen erfassen
2. Risiko- und Prioritätsbewertung
3. Interne Eskalation (SPOC → NIS2-Verantwortliche → Legal → Management)
4. Sammlung der Nachweise (technisch & organisatorisch)
5. Review und Freigabe (4-Augen-Prinzip, rechtliche Prüfung)
6. Antwort an die Behörde (klar, vollständig, ohne Spekulation)
7. Dokumentation & Ablage (DMS/GRC-System)

Qualitätsmerkmale

- vollständig
- nachvollziehbar
- prüffähig
- fristgerecht
- mit korrekten Nachweisen

Pflichtartefakte

- Behördenkontaktliste (SPOC, Vertretung)
- Prozessbeschreibung „Umgang mit Behördenanfragen“

- Nachweis der Erfassung im System
- Antwortpakete inkl. Freigaben
- Übersicht aller Anfragen der letzten 36 Monate
- technische und organisatorische Nachweise

✅ 2. Vorbereitung auf Audits durch das BSI

Auditarten

- **Wesentliche Einrichtungen:** proaktive, tiefgehende Prüfungen
- **Wichtige Einrichtungen:** reaktive Prüfungen (anlassbezogen)

Prüfbereiche

- Einstufung nach NIS2
- Risikomanagement
- Sicherheitsmaßnahmen (Annex II)
- Incident- und Meldeprozess
- Patch-/Vulnerability-Management
- Cloud-Sicherheit
- Identitäts- und Zugriffsmanagement
- BCM / Disaster Recovery
- Lieferantenmanagement
- Governance und Nachweisführung

Auditvorbereitung

1. **Dokumente bündeln:** Policies, Reports, Verträge, Notfallpläne, Logs
2. **Verantwortlichkeiten klären:** Auditkoordinator, technische Ansprechpartner
3. **Audit-Readiness-Test:** Self-Assessment, Probeinterviews, Evidenzprüfung

4. **Logistik vorbereiten:** Auditraum, Zugriffsrechte, stabile Infrastruktur

Verhalten im Audit

- sachlich, neutral, keine Spekulation
- nur Fakten mit Nachweisen
- keine Versprechen ohne Umsetzungsplan
- kritische Punkte offen benennen + Maßnahmenplan

Nachbereitung

- Maßnahmenliste erstellen
- Verantwortlichkeiten und Fristen definieren
- Fortschritt überwachen
- Wirksamkeitsnachweise nachreichen
- Lessons Learned dokumentieren

Pflichtartefakte

- Auditplan
- Auditprotokolle
- Nachweise aller Prüfbereiche
- Verbesserungsmaßnahmen + Wirksamkeitskontrollen
- Management-Freigaben

3.17. Managementbewertung - das ISMS strategisch auf den Prüfstand stellen

Die Managementbewertung ist ein zentraler Bestandteil eines wirksamen ISMS. Sie stellt sicher, dass die Unternehmensleitung regelmäßig prüft, ob das ISMS seine Ziele erreicht, Risiken angemessen behandelt und kontinuierlich verbessert wird. Ziel ist eine **strategische Bewertung**, die auf Zahlen, Auditergebnissen und operativen Erfahrungen basiert.

Warum ist das wichtig?

- Informationssicherheit bleibt Chefsache.
- Du stellst sicher, dass das ISMS nicht nur operativ, sondern auch strategisch gesteuert wird.
- Du schaffst Transparenz und eine fundierte Basis für Entscheidungen.

So führst Du die Managementbewertung durch – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Die Geschäftsleitung prüft regelmäßig, ob das ISMS funktioniert und sinnvoll weiterentwickelt wird.

✅ 2. Bewertungs-Termin planen

- Lege einen festen Termin fest (z. B. jährlich).
- Lade relevante Führungskräfte und Verantwortliche ein (IT, Datenschutz, ISMS-Beauftragte).

✅ 3. Review vorbereiten

Sammle alle wichtigen Informationen:

- Aktuelle Sicherheitsziele und deren Status
- Ergebnisse aus internen und externen Audits
- Berichte über Sicherheitsvorfälle
- Risikoanalysen und neue Bedrohungen
- Umgesetzte und offene Maßnahmen

Bereite eine übersichtliche Präsentation oder ein Berichtsdokument vor.

✅ 4. Managementbewertung durchführen

Diskutiere:

- Welche Ziele wurden erreicht?
- Wo gibt es neue Risiken?
- Was lief gut, was muss verbessert werden?

Dokumentiere alle Erkenntnisse – z. B. in einem Protokoll.

✅ 5. Verbesserungsmaßnahmen ableiten

Für jeden Handlungsbedarf:

- Definiere eine Maßnahme
- Bestimme Verantwortliche
- Setze eine Frist
- Dokumentiere in einer Maßnahmenliste.

✅ 6. Ergebnisse dokumentieren und kommunizieren

- Speichere das Protokoll und die Maßnahmen im ISMS-Handbuch.
- Informiere betroffene Abteilungen über die Ergebnisse und nächsten Schritte.

✅ Nutzen und Vorteil

- Die Geschäftsleitung erhält einen klaren Überblick über den Status der Informationssicherheit.
- Strategische Entscheidungen basieren auf fundierten Informationen.
- Das ISMS wird kontinuierlich verbessert und bleibt relevant für das Unternehmen.

3.18. Korrektur- und Verbesserungsmaßnahmen - das ISMS kontinuierlich weiterentwickeln

Ein ISMS ist kein starres Konstrukt, sondern ein **dynamisches System**, das sich ständig weiterentwickeln muss. Um dauerhaft wirksam zu bleiben, müssen erkannte Schwächen behoben und neue Erkenntnisse in Verbesserungen überführt werden. Genau hier setzen Korrektur- und Verbesserungsmaßnahmen an. Ziel ist es, das ISMS laufend zu optimieren, Risiken zu minimieren und die Organisation widerstandsfähiger zu machen.

Warum ist das wichtig?

- Du stellst sicher, dass Sicherheitslücken nicht nur geschlossen, sondern nachhaltig vermieden werden.
- Du förderst eine Lernkultur, die Sicherheit aktiv verbessert.
- Du machst Dein ISMS robuster und anpassungsfähiger.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst Fehler, Schwachstellen oder Probleme im ISMS erkennen, beheben und daraus lernen.

✅ 2. Ursachenanalyse durchführen

Wenn ein Problem auftritt (z. B. Sicherheitsvorfall, Auditabweichung):

- Frage: **Warum ist das passiert?**
- Gehe der Ursache auf den Grund – nicht nur Symptome behandeln!
- Nutze Methoden wie:

- **5-Why-Analyse**
- **Ishikawa-Diagramm (Fischgräte)**

✅ 3. Maßnahmen definieren

Für jede erkannte Ursache:

- Lege eine konkrete Maßnahme fest
- Bestimme Verantwortliche
- Setze eine Frist

✅ 4. Maßnahmenverfolgung sicherstellen

- Führe eine Maßnahmenliste – z. B. in Excel oder einem ISMS-Tool.
- Prüfe regelmäßig:
  - Wurde die Maßnahme umgesetzt?
  - Ist sie wirksam?
  - Muss nachgebessert werden?

✅ 5. Lessons Learned dokumentieren

Nach jedem Vorfall oder Projekt:

- Was hat gut funktioniert?
- Was sollte beim nächsten Mal anders laufen?
- Teile die Erkenntnisse – z. B. in Schulungen, Meetings oder internen Leitfäden.

✅ 6. Ergebnisse dokumentieren

Halte fest:

- Ursachenanalyse
- Maßnahmen
- Umsetzungsstatus
- Lessons Learned

Speichere alles im **ISMS-Handbuch** oder einem zentralen System.

✅ Nutzen und Vorteil

- Du behebst nicht nur Fehler, sondern verhinderst Wiederholungen.
- Dein ISMS wird stärker, robuster und anpassungsfähiger.
- Du förderst eine Kultur der kontinuierlichen Verbesserung.

3.19. Awareness & Schulungen – Informationssicherheit beginnt beim Menschen

Ein ISMS kann nur wirksam sein, wenn die Menschen, die damit arbeiten, **wissen, verstehen und mittragen**, was Informationssicherheit bedeutet. Deshalb sind Awareness-Maßnahmen und Schulungen ein zentraler Bestandteil jedes ISMS. Ziel ist es, Mitarbeitende zu sensibilisieren und zu befähigen, damit sie Risiken erkennen, sich sicher verhalten und aktiv zur Sicherheitskultur beitragen.

Warum ist das wichtig?

- Menschen sind oft das schwächste Glied in der Sicherheitskette.
- Schulungen helfen, Fehler zu vermeiden und Risiken zu erkennen.
- Du verankerst Informationssicherheit als Teil der Unternehmenskultur.

Die drei Kernbausteine

1. **Rollenspezifische Schulungen**: Inhalte abgestimmt auf Funktion und Verantwortung.
2. **Awareness-Kampagnen**: Regelmäßige Kommunikation und Aktionen.
3. **Nachweisführung**: Dokumentation der Teilnahme und Inhalte.

So gehst Du vor – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Alle Mitarbeitenden sollen wissen, **was Informationssicherheit bedeutet**, wie sie sich sicher verhalten und welche Risiken es gibt.

✅ 2. Rollenspezifische Schulungen planen

Überlege:

- Wer braucht welche Inhalte? (z. B. IT, Vertrieb, Führungskräfte)
- Was ist für die jeweilige Rolle besonders wichtig?

Erstelle Schulungsinhalte, die zur Funktion passen – z. B.:

- Datenschutz für HR
- Phishing-Erkennung für alle
- Sicherheitskonfigurationen für IT-Admins

✅ 3. Awareness-Kampagnen starten

Plane regelmäßige Aktionen, um das Thema präsent zu halten:

- E-Mail-Tipps zur IT-Sicherheit
- Poster oder Bildschirmschoner mit Sicherheitshinweisen
- Quiz oder kleine Wettbewerbe
- Phishing-Testmails zur Sensibilisierung

Ziel: Informationssicherheit soll Teil der Unternehmenskultur werden – nicht nur ein einmaliges Event.

✅ 4. Schulungen durchführen

Organisiere:

- Präsenzschulungen oder Online-Kurse
- Interaktive Formate (z. B. Fallbeispiele, Gruppenarbeit)
- Wiederholungsschulungen bei Bedarf

Stelle sicher, dass die Inhalte **verständlich und praxisnah** sind.

✅ 5. Teilnahme und Inhalte dokumentieren

Führe Nachweise:

- Wer hat teilgenommen?
- Wann fand die Schulung statt?
- Was wurde vermittelt?

Nutze z. B.:

- Excel-Listen
- Lernplattformen
- Digitale Zertifikate

✅ Nutzen und Vorteil

- Mitarbeitende wissen, wie sie sich sicher verhalten sollen – das reduziert Risiken deutlich.
- Informationssicherheit wird im Alltag verankert, nicht nur auf dem Papier.
- Du erfüllst die Anforderungen der ISO/IEC 27001 und 27002 – nachvollziehbar und auditfähig.

3.20. Geschäftsleitungsschulungen: Cybersicherheit beginnt an der Spitze

Die Umsetzung der NIS2-Richtlinie verlangt, dass **Cybersicherheit als strategische Führungsaufgabe verstanden und aktiv gesteuert wird**. Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen sind gesetzlich verpflichtet, regelmäßig an Schulungen teilzunehmen, um:

- Risiken zu erkennen,
- Risikomanagementmaßnahmen zu bewerten,
- und deren Auswirkungen auf die Organisation zu verstehen.

Ziel: Die Geschäftsleitung muss befähigt werden, Cybersicherheit als integralen Bestandteil der Unternehmensführung und des Risikomanagements zu verankern.

Warum ist das wichtig?

- Die Geschäftsleitung trägt die **rechtliche und persönliche Verantwortung** für Cybersicherheit.
- Nur informierte Entscheidungen schützen vor **Haftungsrisiken und aufsichtsrechtlichen Maßnahmen**.
- Cybersicherheit wird als Teil der **Unternehmenskultur und strategischen Steuerung** etabliert.

Die drei Kernbausteine

1. **Erkennung und Bewertung von Risiken:**
   Geschäftsleitungen müssen Bedrohungen, Eintrittswahrscheinlichkeiten und Auswirkungen auf strategischer Ebene einschätzen können.

2. **Risikomanagementmaßnahmen:**
   Kenntnisse über technische und organisatorische Mindestmaßnahmen sowie deren betriebswirtschaftliche Bedeutung sind essenziell.
3. **Beurteilung der Auswirkungen:**
   Die Fähigkeit, Risiken und Maßnahmen im Kontext von Verfügbarkeit, Integrität, Vertraulichkeit und wirtschaftlicher Stabilität zu bewerten.

✅ 1. Ziel verstehen

Die Geschäftsleitung muss wissen, welche Risiken für die Organisation bestehen und wie sie diese strategisch steuert.

✅ 2. Schulungsbedarf und Inhalte planen

Überlege:

- Welche gesetzlichen und branchenspezifischen Anforderungen gelten?
- Welche Risiken und Maßnahmen sind für die eigene Einrichtung relevant?
  Erstelle Schulungsinhalte, die auf die Rolle und Verantwortung der Geschäftsleitung zugeschnitten sind – z. B.:
- Überblick NIS2 und BSIG-E
- Mindestmaßnahmen nach § 30 BSIG-E
- Haftungs- und Meldepflichten
- Nutze auch das nis-2-geschaeftsleitungsschulung.pdf vom BSI

✅ 3. Praxisbezug und Übungen einbauen

Plane interaktive Formate, um die Anwendung zu fördern:

- Szenarien und Fallstudien zu typischen Bedrohungslagen
- Planspiele zur Entscheidungsfindung und Krisenkommunikation
- Diskussion branchenspezifischer Risiken

✅ 4. Schulungen durchführen

Organisiere:

- Präsenz- oder Online-Schulungen mit Fokus auf strategische Steuerung
- Wiederholungsschulungen mindestens alle drei Jahre oder bei relevanten Änderungen
- Einbindung externer und interner Experten für spezifische Inhalte

✅ 5. Teilnahme und Inhalte dokumentieren

Führe Nachweise:

- Wer hat teilgenommen?
- Wann und wie lange fand die Schulung statt?
- Welche Inhalte wurden vermittelt?

  Nutze z. B.:
- Schulungsprotokolle
- digitale Zertifikate
- Dokumentation für Aufsichtsbehörden

3.21. Dokumentation im zentralen ISMS-Handbuch

Das ISMS-Handbuch ist das **Herzstück der Dokumentation** in Deinem Informationssicherheits-Managementsystem. Es enthält alle wesentlichen Informationen, die notwendig sind, um das ISMS **nachvollziehbar, steuerbar und auditfähig** zu machen. Ziel ist es, eine strukturierte und vollständige Übersicht über die Sicherheitsorganisation, deren Prozesse, Regelungen und Nachweise zu schaffen.

Warum ist das wichtig?

- Du schaffst Transparenz und Struktur für Dein gesamtes Sicherheitsmanagement.
- Du bist optimal vorbereitet für interne und externe Audits.
- Du stellst sicher, dass das ISMS kontinuierlich überprüfbar und verbesserbar bleibt.

Die drei Kernbausteine

1. **Grundlegende Informationen**: Kontext, Scope, Ziele.
2. **Strukturierte Inhalte**: Prozesse, Richtlinien, Rollen.
3. **Nachweise**: Schulungen, Audits, Maßnahmen.

So erstellst Du Dein ISMS-Handbuch – Schritt für Schritt

✅ 1. Verstehe Dein Ziel

Du willst ein zentrales Dokument erstellen, das alle wichtigen Informationen rund um Dein ISMS enthält – **übersichtlich und auditfähig**.

✅ 2. Grundlegende Informationen eintragen

Dokumentiere:

- **Kontext der Organisation**: Welche internen und externen Faktoren beeinflussen die Informationssicherheit?
- **Scope (Geltungsbereich)**: Welche Standorte, Systeme und Prozesse sind vom ISMS betroffen?
- **ISMS-Ziele**: Welche Sicherheitsziele verfolgt Dein Unternehmen?

✅ 3. Prozesse, Richtlinien und Rollen beschreiben

Füge alle relevanten Inhalte ein:

- **Sicherheitsrichtlinien**: z. B. Zugriffskontrolle, mobile Geräte, Backup.
- **ISMS-Prozesse**: z. B. Incident Management, Risk Management, Change-Management.
- **Rollen und Verantwortlichkeiten**: Wer ist wofür zuständig? (z. B. ISMS-Beauftragte, IT-Leitung).

✅ 4. Nachweise sammeln und einfügen

Dokumentiere, was tatsächlich umgesetzt wurde:

- Schulungsnachweise
- Auditberichte
- Maßnahmenlisten
- Ergebnisse aus Managementbewertungen

Diese Nachweise zeigen, dass Dein ISMS **aktiv betrieben und regelmäßig überprüft** wird.

✅ 5. Handbuch regelmäßig aktualisieren

- Lege fest, wie oft das Handbuch überprüft wird (z. B. quartalsweise oder nach jedem Audit).
- Bestimme eine verantwortliche Person für die Pflege des Dokuments.

✅ 6. Handbuch zugänglich machen

- Speichere das Handbuch an einem zentralen Ort (z. B. Intranet oder DMS).
- Stelle sicher, dass alle relevanten Personen Zugriff haben (Auditoren, Führungskräfte, ISMS-Team).

✅ Nutzen und Vorteil

- Du schaffst Transparenz und Struktur für Dein gesamtes Sicherheitsmanagement.
- Du bist optimal vorbereitet für interne und externe Audits.
- Dein ISMS wird nachvollziehbar, steuerbar und kontinuierlich

4. Ein ISMS muss leben! Sicherheit ist kein Papierprojekt

Ein Informationssicherheits-Managementsystem (ISMS) ist kein Ordner voller Richtlinien und Checklisten. Es ist ein **lebendiger Prozess**, der nur funktioniert, wenn Menschen ihn im Alltag umsetzen.
NIS2 gibt den Rahmen vor, aber kein Dokument ersetzt die vielen kleinen Entscheidungen, die täglich getroffen werden.

Warum ist das wichtig?

Sicherheitskultur entsteht nicht durch Audits, sondern durch gelebte Praxis.

Nur wenn Management und Mitarbeitende Informationssicherheit als Teil ihrer Arbeit verstehen, wird das ISMS wirksam.

Risiken ändern sich ständig, ein statisches System schützt nicht.

Die drei Prinzipien für ein „lebendes" ISMS

- **Führung und Vorbildfunktion**
  Management muss Informationssicherheit vorleben, nicht nur auf dem Papier, sondern in Entscheidungen und Prioritäten.
- **Integration in den Alltag**
  Sicherheit darf kein „Extra" sein. Sie gehört in alle Prozesse und Bereiche: Projektmanagement, Einkauf, HR, IT-Betrieb.
- **Kontinuierliche Verbesserung**
  Risiken ändern sich. Maßnahmen müssen angepasst werden. Lernen ist Teil des Prozesses.

✅ So bringst Du Dein ISMS zum Leben

1. Rollen und Verantwortlichkeiten klären

ISB, IT, Fachbereiche: alle müssen wissen, was ihre Aufgabe ist. Und was ist, wenn die mal nicht „da" sind?

- Erstelle eine Verantwortlichkeitsmatrix mit klaren Stellvertreterregelungen für Abwesenheiten.
- Definiere Notfallrollen für kritische Situationen (z. B. Incident Commander).
- Kommuniziere Rollen nicht nur in Policies, sondern in Onboarding-Prozessen und Teammeetings.
- Nutze digitale Tools (z. B. GRC-Systeme), um Verantwortlichkeiten transparent zu machen.

2. Kommunikation und Transparenz schaffen

Regelmäßige Statusberichte, Awareness-Kampagnen, Feedbackrunden – nicht nur einmal im Jahr.

- Führe monatliche Security-Updates im Intranet oder per Newsletter ein.
- Nutze Dashboards, um KPIs und Risiken sichtbar zu machen.
- Etabliere Feedback-Kanäle (z. B. digitale Umfragen, offene Q&A-Sessions).
- Kommuniziere auch Erfolge: z. B. „Phishing-Quote gesenkt" oder „Backup-Test erfolgreich".

3. Schulungen als Daueraufgabe etablieren

Keine Einmal-Events. Wiederholung, Praxisbezug und aktuelle Bedrohungen einbeziehen.

- Plane vierteljährliche Awareness-Aktionen (z. B. Phishing-Simulationen).
- Nutze Micro-Learning: kurze Videos oder Quizfragen im Arbeitsalltag.

- Passe Inhalte an aktuelle Bedrohungen an (z. B. KI-basierte Angriffe, Ransomware-Trends).
- Dokumentiere Schulungen in einem Learning-Management-System für Nachweisführung.

4. Sicherheitskultur fördern

Diskussionen ermöglichen, Konflikte früh erkennen, Akzeptanz schaffen.

- Integriere Security-Talks in Teammeetings.
- Schaffe Security-Champions in Fachbereichen als Multiplikatoren.
- Fördere offene Diskussionen über Risiken und Konflikte (Compliance vs. Business).
- Belohne gutes Sicherheitsverhalten (z. B. Gamification, interne Awards).

5. Fortschritt sichtbar machen

KPIs, interne Audits, Reifegradanalysen – damit Sicherheit nicht Theorie bleibt.

- Definiere KPIs wie „Patch-Compliance“, „Phishing-Erkennungsrate“, „Audit-Ergebnisse“.
- Führe Reifegradanalysen durch und kommuniziere Verbesserungen.
- Nutze Heatmaps für Risikostatus und Maßnahmenfortschritt.
- Berichte regelmäßig an das Management und die Belegschaft – nicht nur an Auditoren.

6. Risiken und Maßnahmen regelmäßig prüfen

Neue Technologien, neue Bedrohungen – ISMS muss sich anpassen.

- Etabliere einen quartalsweisen Risiko-Review.
- Nutze Threat Intelligence für aktuelle Bedrohungen.
- Prüfe regelmäßig die Wirksamkeit von Maßnahmen (z. B. Penetrationstests, Red-Teaming).

- Aktualisiere Policies und Prozesse bei technologischen oder organisatorischen Änderungen.

7. Zusätzliche Impulse für ein lebendes ISMS

- Integration in alle Prozesse: Einkauf, HR, Projektmanagement – Sicherheit muss überall mitgedacht werden.
- Kontinuierliche Verbesserung: Nutze interne Audits und Lessons Learned aus Vorfällen als Treiber.
- Management Commitment: Führungskräfte müssen Sicherheit aktiv fördern und Ressourcen bereitstellen.
- Technologie nutzen: Automatisierte Compliance-Checks, Dashboards und GRC-Tools erleichtern die Umsetzung.

Fazit

Ein ISMS ist keine Pflichtübung und kein Zertifikat. Es ist ein **strategisches Werkzeug**, das nur dann wirksam ist, wenn es **Teil der Unternehmenskultur** wird. Sicherheit lebt durch Menschen – jeden Tag.

5. Die ISMS-Menschen müssen befähigt sein

Ein ISMS lebt nicht nur durch definierte Rollen, sondern durch Menschen, die ihre Aufgaben verstehen und wirksam ausfüllen. Rollen wie ISB, CISO, Prozessowner oder Fachbereichsverantwortliche sind oft komplex und erfordern mehr als Fachwissen: Sie verlangen Einfluss ohne Macht, strategische Kommunikation und die Fähigkeit, in einem regulierten Umfeld Orientierung zu geben.

Damit diese Rollen nicht nur „benannt", sondern befähigt werden, braucht es gezielte Entwicklung. Die folgenden Methoden und Inhalte sind entscheidend.

✅ 1. Rollenklarheit und Selbstreflexion

- Canvas-Modelle und Rollenprofile: Erwartungen, Verantwortlichkeiten und Schnittstellen sichtbar machen.
- Selbstreflexion fördern: z. B. mit Profilen wie Management Drives, um Stärken, Motivationen und Entwicklungsfelder zu erkennen.
- Fragen klären: „Was wird von mir erwartet?", „Was kann ich erwarten?", „Was will ich in dieser Rolle erreichen?"

✅ 2. Strategische Kommunikation

- Gesprächsführung trainieren: Wie bekomme ich vom Vorgesetzten Ressourcen und Rückendeckung?
- Hierarchie navigieren: Methoden, um als „Dolmetscher" zwischen Ebenen zu agieren.
- Tools für Reporting und Eskalation: klare Vorlagen, Kommunikationspläne, Entscheidungslogik.

✅ 3. Stakeholder-Management und Einfluss

- Stakeholder-Analysen: Wünsche, Bedürfnisse und „Währungen" der relevanten Akteure verstehen.
- Verhandlungstechniken: Einflussstrategien entwickeln, um Ziele auch ohne Weisungsbefugnis zu erreichen.
- Beziehungssteuerung: Vertrauen aufbauen, Konflikte früh erkennen und steuern.

✅ 4. Komplexitäts- und Konfliktmanagement

- Handlungsfähigkeit in turbulenten Situationen: Rollenklarheit, Priorisierung und Stressmanagement.
- Widerstände verstehen und steuern: Gesprächstechniken für schwierige Situationen.
- Politische Dynamiken erkennen: Umgang mit Machtstrukturen und informellen Netzwerken.

✅ 5. Führung ohne Macht (Laterale Steuerung)

- Verständnis für „Währungssysteme": Was zählt in einer Matrixorganisation?
- Methoden für laterale Führung: Einfluss ohne Hierarchie, Delegation nach Reifegrad.
- Team-Entwicklung fördern: Zielorientierung schaffen, Veränderungen begleiten.

✅ 6. Praxisformate für Befähigung

- Individuelle Coachings und Self-Assessments: persönliche Entwicklung und Klarheit.

- Interaktive Workshops und Planspiele: realistische Szenarien, Krisensimulationen.
- Kollegiale Beratung: Erfahrungsaustausch zwischen Rolleninhabern.
- Fall- und Stakeholder-Analysen: praxisnahe Übungen für komplexe Situationen.

Über GreenSocks Consulting – r.evolutionary Consulting

Die GreenSocks Consulting GmbH ist ein Beratungsunternehmen, das Informationssicherheit neu denkt. Seit über 15 Jahren begleiten wir Unternehmen auf ihrem Weg zu realistisch funktionierenden, auditfähigen und praxistauglichen Informationssicherheits-Managementsystemen.

Unsere Mission ist klar:
Wir befähigen Menschen und Organisationen – statt nur zu beraten.

Denn Informationssicherheit ist kein Papierprojekt. Sie entsteht durch Klarheit, Verantwortung, gelebte Prozesse und eine Kultur, in der Sicherheit verstanden und umgesetzt wird.

Was uns auszeichnet

Praxis statt Theorie
Wir übersetzen ISO/IEC 27001, NIS2 und komplexe Anforderungen in umsetzbare Schritte, die im Alltag funktionieren.

Befähigung statt Abhängigkeit
Unsere Kunden sollen nicht von Beratern abhängig sein – sie sollen das System selbständig steuern können. Genau deshalb arbeiten wir mit Rollenbefähigung, Coaching, klaren Methoden und viel Transparenz.

Struktur ohne Bürokratie
Wir bauen ISMS so, dass sie leben – mit definierten Prozessen, klaren Rollen, wirksamen Maßnahmen und messbaren Ergebnissen. Keine überfrachteten Dokumente, kein Overengineering.

Erfahrung über alle Branchen hinweg
Vom Mittelstand bis zum Konzern – wir haben diverse Unternehmen durch Assessments, Aufbauprogramme und Zertifizierungen geführt.

Echte Partnerschaft auf Augenhöhe

Wir stehen für Klartext, Offenheit und einen ehrlichen Umgang. Oft unbequem – immer hilfreich.

Unsere Leistungen (Auszug)

- Aufbau & Optimierung von ISMS nach ISO/IEC 27001
- NIS2-Readiness & NIS2-Assessments
- Einführung moderner ISMS-Governance
- Rollenbefähigung (ISB, CISO, Prozessverantwortliche)
- Interne Audits, Managementbewertungen & Zertifizierungsvorbereitung
- Awareness-Programme & Security Culture
- Krisensimulationen und Planspiele
- Fractional ISB / CISO-Services
- Gap-Analysen, Risikoanalysen & Reifegradmodelle

Alle Leistungen folgen unserem Leitprinzip:
Befähigen statt nur beraten.

Lass uns Dein ISMS gemeinsam wirksam machen

Ein ISMS ist dann erfolgreich, wenn es im Alltag funktioniert. Wenn Menschen es verstehen. Wenn Prozesse klar sind. Wenn Risiken im Griff sind. Und wenn die Organisation wirklich sicherer wird.

Genau dabei unterstützen wir Dich.

Wenn Du Dein ISMS aufbauen, modernisieren oder auditfähig machen willst – lass uns sprechen**.**
Wenn Du NIS2-Pflichten erfüllen musst – wir begleiten Dich Schritt für Schritt**.**

Wenn Du Rollen stärken oder Strukturen professionalisieren willst – wir befähigen Deine Menschen**.**

GreenSocks Consulting GmbH

Zum Pütter Feld 17, 41751 Viersen

📞 +49 2162 3693208

📩 info@greensocks.de

🌐 www.greensocks.de

Ignoranz ist die größte Schwachstelle – wir helfen Dir, sie zu schließen.

6. Glossar

- **Asset** Ein Informations- oder Betriebswert, der für die Organisation relevant ist, z. B. Daten, IT-Systeme, Netzwerke, Prozesse oder physische Infrastruktur.
- **Auswirkungen (Impact)** Bewertung der Folgen eines Sicherheitsvorfalls für Verfügbarkeit, Integrität und Vertraulichkeit sowie für Geschäftsprozesse, Kunden, Compliance oder Reputation.
- **BCP – Business Continuity Plan** Dokumentiertes Verfahren, um kritische Geschäftsprozesse im Störfall fortzuführen oder schnell wiederherzustellen (unter NIS2 gefordert bei wesentlichen Einrichtungen).
- **Betroffene Einrichtung (NIS2-Kategorisierung)** Organisationen, die unter die NIS2-Richtlinie fallen. Unterschieden wird zwischen **wesentlichen Einrichtungen** und **wichtigen Einrichtungen**.
- **C(I)A-Prinzip** Grundwerte der Informationssicherheit:
  - **Vertraulichkeit (Confidentiality)**
  - **Integrität (Integrity)**
  - **Verfügbarkeit (Availability)**
- **CSIRT – Computer Security Incident Response Team** Nationale oder sektorale Teams, die Meldungen entgegennehmen, analysieren und koordinieren. In Deutschland sind dies die Strukturen im Umfeld des BSI.
- **Direktorenhaftung / Managementverantwortung** Unter NIS2 trägt die Geschäftsleitung explizit die Verantwortung für Cybersicherheit, Umsetzung, Überwachung und Schulungspflichten.
- **Einfache Meldung / Frühwarnung** Bei relevanten Sicherheitsvorfällen muss innerhalb von **24 Stunden** eine Frühwarnmeldung an die zuständige Behörde erfolgen (z. B. BSI).
- **Endgültige Meldung** Spätestens **72 Stunden** nach Erkennung eines meldepflichtigen Vorfalls muss eine qualifizierte Meldung mit allen verfügbaren Fakten übermittelt werden.

- **ESS – Essential Entities (Wesentliche Einrichtungen)** Organisationen mit besonders hoher gesellschaftlicher Relevanz oder potenziell erheblichem Schaden im Versagensfall (z. B. Energie, Verkehr, Gesundheit).
- **ISE – Important Entities (Wichtige Einrichtungen)** Organisationen, die für Wirtschaft und Gesellschaft relevant sind, aber geringere Kritikalität besitzen als wesentliche Einrichtungen.
- **ISO/IEC 27001** Internationaler Standard für den Aufbau eines Informationssicherheits-Managementsystems (ISMS). Viele NIS2-Pflichten lassen sich darüber erfüllen.
- **Kritische Dienste / Kritische Funktionen** Dienstleistungen oder Prozesse, deren Störung erhebliche Auswirkungen auf Gesellschaft, Wirtschaft oder öffentliche Sicherheit hätte.
- **Lieferketten-Risiko (Supply Chain Risk)** Risiken, die durch externe Dienstleister, Software-Hersteller oder Betreiber in der Lieferkette entstehen — unter NIS2 besonders betont.
- **Maßnahmenkatalog (TOMs)** Technische und organisatorische Maßnahmen, die NIS2 verpflichtend vorsieht — u. a. Risikoanalyse, Incident Management, Notfallmanagement, Schulungen, Kryptografie, Monitoring.
- **Management-Schulungspflicht** NIS2 fordert, dass die Geschäftsleitung regelmäßig geschult wird, um „ausreichende Kenntnisse in Cybersicherheit“ vorweisen zu können.
- **Meldepflicht** Pflicht, erhebliche Sicherheitsvorfälle zeitnah an die Behörde zu melden (24-h Frühwarnung, 72-h Bericht, Abschlussbericht).
- **NIS2 – Network and Information Security Directive 2** EU-Richtlinie, die ein hohes gemeinsames Cyber-Sicherheitsniveau in Europa sicherstellen soll. Sie erweitert den Geltungsbereich der ersten NIS-Richtlinie erheblich.

- **NIS-2UmsCG – NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** Deutsches Umsetzungsgesetz der NIS2-Richtlinie. Regelt branchenspezifisch, welche Organisationen betroffen sind und welche Pflichten gelten.
- **Notfallmanagement / Incident Response** Strukturierter Prozess zur Erkennung, Analyse, Behandlung und Nachverfolgung von Sicherheitsvorfällen. Unter NIS2 verpflichtend.
- **Organisatorische Maßnahmen** Nicht-technische Sicherheitsmaßnahmen, z. B. Rollen, Richtlinien, Schulungen, Awareness, Prozesse, Meldewege.
- **Risikobasierter Ansatz** Zentrale NIS2-Anforderung: Cybersicherheit muss sich an Risiken, Unternehmensgröße, Kosten/Verhältnismäßigkeit und möglichen Auswirkungen orientieren.
- **Risikomanagement** Systematisches Erkennen, Bewerten und Steuern von Risiken für IT-Systeme, kritische Prozesse und Daten.
- **Schutzbedarf** Bewertung, wie kritisch ein Informationswert für das Unternehmen ist (z. B. normal, hoch, sehr hoch).
- **Schwachstelle (Vulnerability)** Technische oder organisatorische Lücke, die eine Bedrohung ausnutzen kann.
- **Supply-Chain-Monitoring** Pflicht zur Überprüfung der Sicherheitsmaßnahmen von Lieferanten und Dienstleistern.
- **Technische Maßnahmen** Technische Sicherheitskontrollen wie Netzwerksegmentierung, Verschlüsselung, Firewalls, Multifaktor-Authentifizierung oder Überwachungssysteme.
- **Umsetzungspflichten** Verbindliche Maßnahmenbereiche der NIS2, z. B.:
    - Risikoanalyse
    - Sicherheitskultur und Schulungen
    - Incident Management
    - Business Continuity
    - Backup & Recovery
    - Kryptografie

  - Monitoring
  - Lieferketten-Sicherheit
- **Wesentliche Einrichtungen** Siehe ESS; Unternehmen mit besonders kritischer Rolle im Staat oder in der Wirtschaft. Strengere Aufsichtsmaßnahmen.
- **Wichtige Einrichtungen** Siehe ISE; Unternehmen mit relevanter, aber geringerer Kritikalität. Weniger Aufsicht, aber gleiche Pflichten.
- **Zero-Trust-Prinzip** Sicherheitsprinzip: Grundannahme, dass kein System, Nutzer oder Gerät automatisch vertrauenswürdig ist. Zugriff muss stets geprüft und begrenzt werden.

7. Rechtlicher Hinweis

Dieser Leitfaden wurde mit größter Sorgfalt erstellt und basiert auf dem aktuellen Kenntnisstand zur NIS2-Richtlinie sowie den öffentlich zugänglichen Entwürfen des deutschen Umsetzungsgesetzes.
Er ersetzt keine Rechtsberatung.
Alle Aussagen dienen der Orientierung und stellen keine verbindliche juristische Auslegung dar.

Rechtliche Anforderungen können sich ändern. Jede Organisation ist verpflichtet, die für sie geltenden gesetzlichen Vorgaben eigenverantwortlich zu prüfen und bei Bedarf qualifizierte rechtliche Beratung in Anspruch zu nehmen.

Die Autoren übernehmen keine Haftung für Schäden, die aus der Nutzung dieses Dokuments entstehen.