

# SEC4YOU

Advanced IT-Audit Services

RESTRICTED TLP:AMBER

# Welche Cyber-RESILIENZ-Maßnahmen helfen bei der Erfüllung von NIS-2?

Andreas Schuster / 19.01.2026 / V1.00

# Einleitung: Die NIS-2 Richtlinie (EU) und NIS-2 in Österreich

---



## Der Unterschied von EU-Richtlinie und dem NISG 2026

### Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)

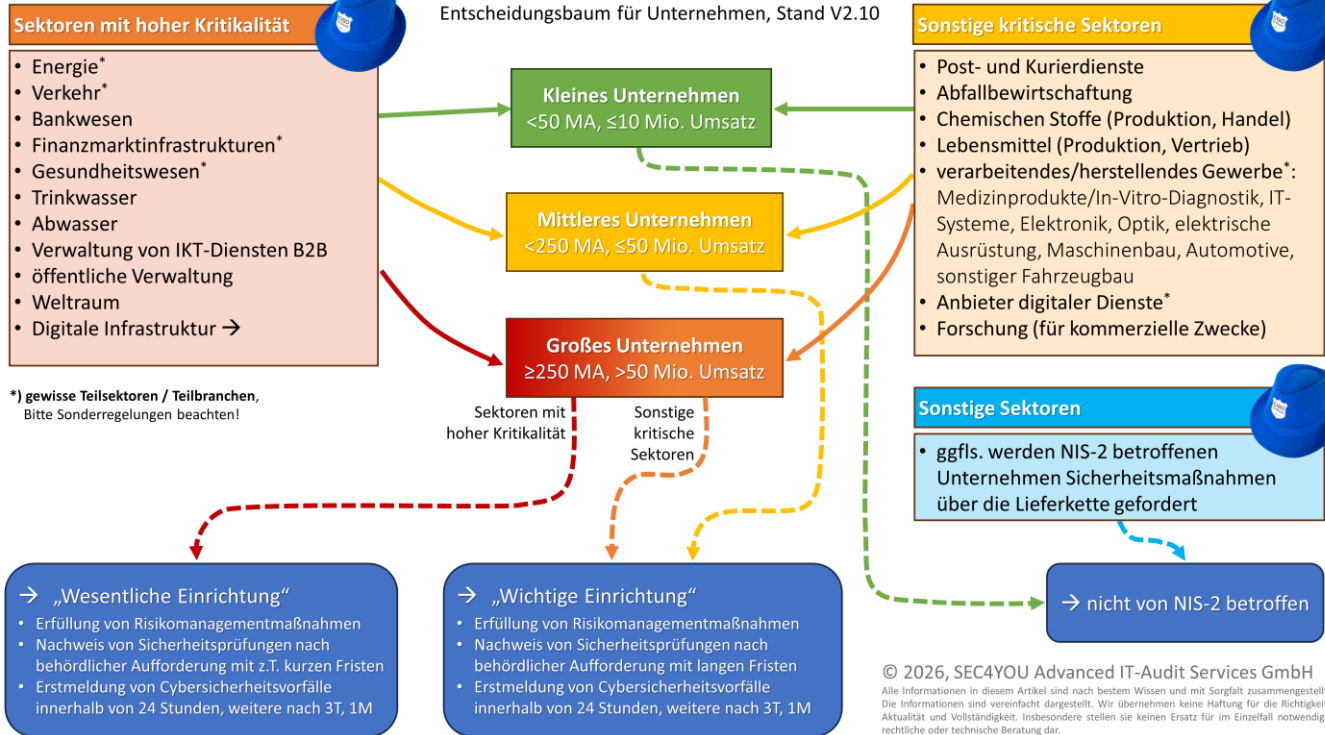
- Gültig seit 14. Dezember 2022
- Nachfolger der NIS-Richtlinie 2016
- Erforderte Umsetzung durch nationales Gesetz bis 17.10.2024 und sieht keine verlängernden Fristen vor
- Erhöhung der Cybersicherheit des öffentlichen und des privaten Sektors in der EU
- Verpflichtung zur Implementierung eines Risikomanagements und für Maßnahmen zur Behandlung
- Nationale Meldepflichten bei Vorfällen

### Österreichisches NISG 2026

- Gültig seit 23. Dezember 2025
- Großteils wurden die Anforderungen der EU-Richtlinie übernommen
- Eine Vielzahl an Fristverlängerungen implementiert für Inkrafttreten, Registrierung, Selbstdeklaration, Audits durch „unabhängige Stellen“
- §32: Verpflichtende Risikomanagementmaßnahmen sowie Referenz auf Stand der Technik und ggfls. Normen (i.d.R. ISO 27001)
- §34: 24h/72h/1M Meldepflichten von Cybersicherheitsvorfällen an sektorspezifische Meldestellen (CSIRTs)

## Betroffenheit nach NISG 2026

Entscheidungsbaum für Unternehmen, Stand V2.10



© 2026, SEC4YOU Advanced IT-Audit Services GmbH  
Alle Informationen in diesem Artikel sind nach bestem Wissen und mit Sorgfalt zusammengestellt. Die Informationen sind vereinfacht dargestellt. Wir übernehmen keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit. Insbesondere stellen sie keinen Ersatz für im Einzelfall notwendige rechtliche oder technische Beratung dar.

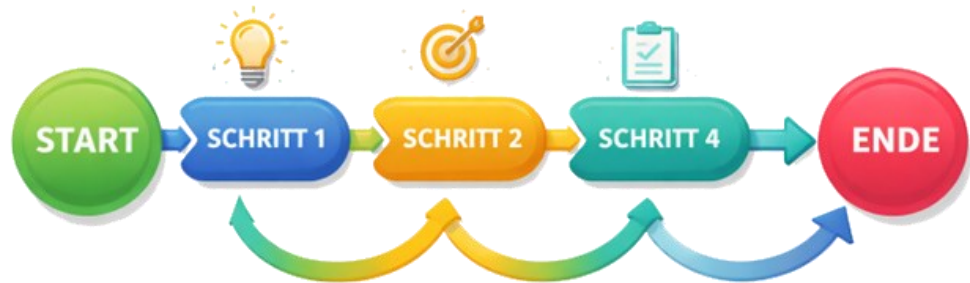
## Ernennung des Informationssicherheitsbeauftragten (ISB/CISO)

---

- Ein ISB/CISO ist keine Grundanforderung des NISG 2026, ABER ohne einen (Teilzeit-) ISB werden Unternehmen den §31 (Governance), §32 (Risikomanagementmaßnahmen) inkl. Risikomanagement und §33 (Nachweis der Wirksamkeit) nicht erfüllen können.
- Eine **Doppelbesetzung** IT-Leiter+ISB oder Geschäftsführer+CISO bringt erhebliche Nachteile in der Governance und vorprogrammierte Interessenskonflikte → dies entspricht nicht dem Stand der Technik, da ISO 27001 dagegen spricht
- Leseempfehlung: <https://www.sec4you.com/besetzung-isb-ciso/>

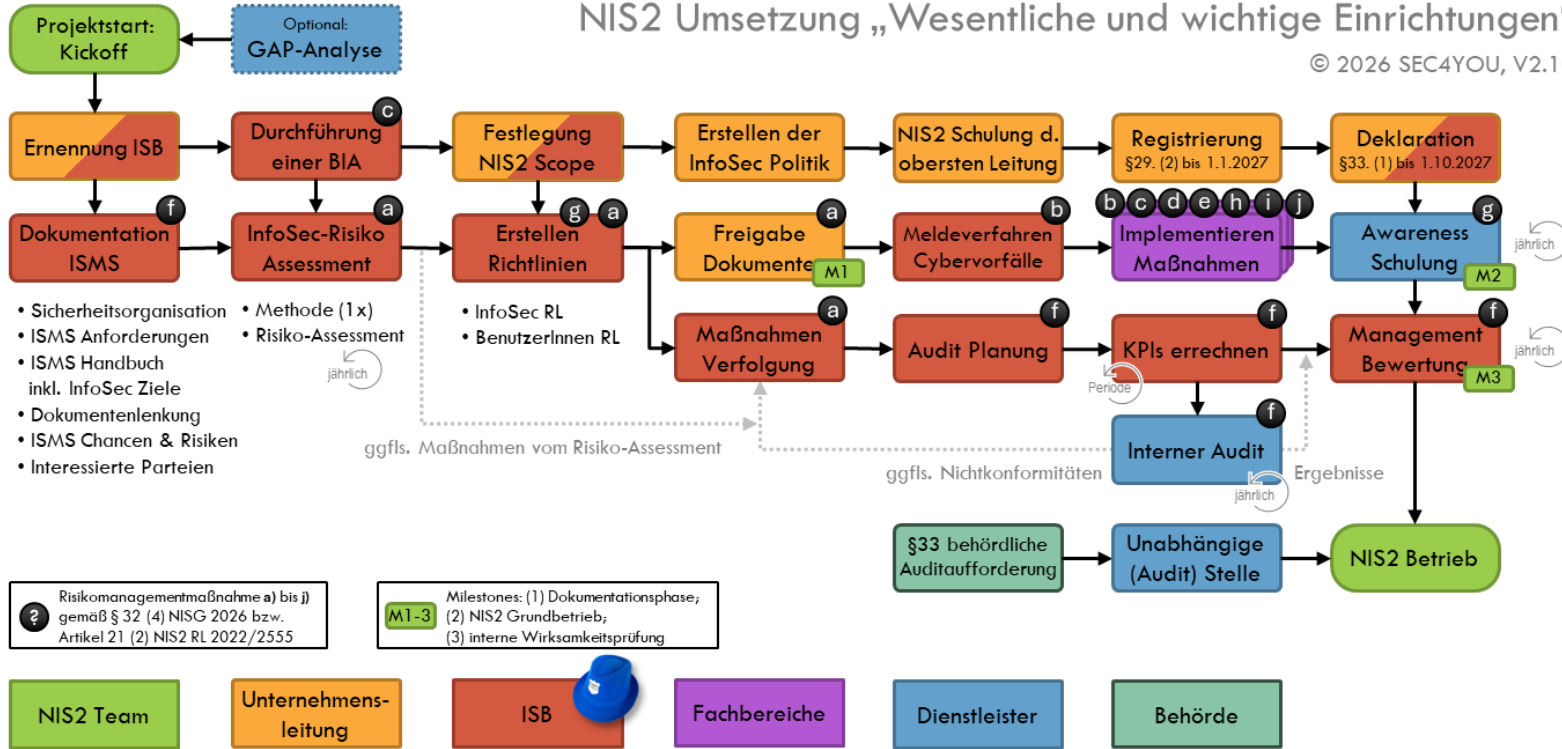
## NIS-2 Implementierung als Projekt

- Klarer Projektauftrag!
- Klarer Projektverantwortlicher!
- Regelmäßige JF!
- Meilensteine!



# NIS2 Umsetzung „Wesentliche und wichtige Einrichtungen“

© 2026 SEC4YOU, V2.10



## Braucht man eine Business Impact Analyse?

---

- Die **Business Impact Analyse (BIA)** ist ein zentrales Analysewerkzeug im Rahmen des Business Continuity Managements (BCM).
- Sie bildet die methodische Grundlage für alle nachgelagerten Schritte zur Absicherung des Geschäftsbetriebs, insbesondere in außergewöhnlichen Situationen wie IT-Ausfällen, Lieferengpässen, Naturkatastrophen, Cyberangriffen oder anderen betrieblichen Krisenszenarien. → **RESILIENZ**
- Durch die BIA können **Wiederanlaufzeiten (RTO/MTPD)** definiert, **Notfallmaßnahmen** und **Redundanzen** dimensioniert, sowie **Wiederherstellungsaktivitäten** priorisiert und der **Schutzbedarf** sowie der **NIS-2 Scope** abgeleitet werden.

## Business-Impact-Analyse (BIA) und NIS-2

- Es gibt keine konkrete Anforderung für die Durchführung einer Business-Impact-Analyse im NISG 2026.
- Ein Großteil der Anforderungen aus §32 Risikomanagementmaßnahmen (3) und (4) basieren direkt aus den Ergebnissen einer Business-Impact-Analyse.
- Empfehlung zum kostenfreien BIA Booklet / Leitfaden „Pia erklärt die BIA“  
<https://www.sec4you.com/produkt/business-impact-analyse-leitfaden/>



## Anforderung zur Schulung der obersten Leitung (Leitungsorgane)

---

- Das NISG 2025 §31 (2) fordert „*Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen an für diese spezifisch gestalteten Cybersicherheitsschulungen teilnehmen.*“
- Es gibt noch keine Definition über Art und Umfang, aber es muss eine spezifische Schulung sein, d.h. auf das Unternehmen, den Scope, den spezifischen Schutzbedarf angepasst sein.
- Theoretisch kann der ISB diese Schulung selbst halten, aber ggfls. ist es sinnvoll diese von einem Dienstleister durchführen zu lassen.



## Erforderliche Maßnahmen in NIS-2 – § 32 (4) - Teil 1

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Cybersicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern, unter Berücksichtigung der spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, der Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, sowie der Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen;

ISO 27001:  
6.1 Risikomanagement  
+ Maßnahmen

A5.24-28 Sicherheitsvorfälle

A5.30 BCM  
A8.13 Sicherung/Backup  
A8.14 Redundanzen  
Disaster-Recovery-Plan

A5.19 InfoSec Lieferkette  
A5.20 Lieferantenvereinbarungen  
A5.21 InfoSec Lieferkette  
A5.22 Überwachung von  
Lieferanten Leistungen

## Erforderliche Maßnahmen in NIS-2 – § 32 (4) - Teil 2

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

A.8.26 Anforderungen an die Anwendungssicherheit  
A5.15 Zugangssteuerung  
A8.32 Änderungssteuerung  
A8.8 Technische Schwachstellen

27001: 9.1 KPIs  
9.2 interne Audits  
9.3 Managementbewertung

A5.9 Assetmanagement  
A5.10 zulässiger Gebrauch Assets  
A5.18 Zugangsrechte  
A8.19 Installation von Software  
A8.1 Schutz gegen Schadsoftware  
A8.22 Trennung von Netzwerken  
A6.3 Security Awareness  
u.v.m

A8.24 Kryptografie

## Erforderliche Maßnahmen in NIS-2 – § 32 (4) - Teil 3

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

ii) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung,

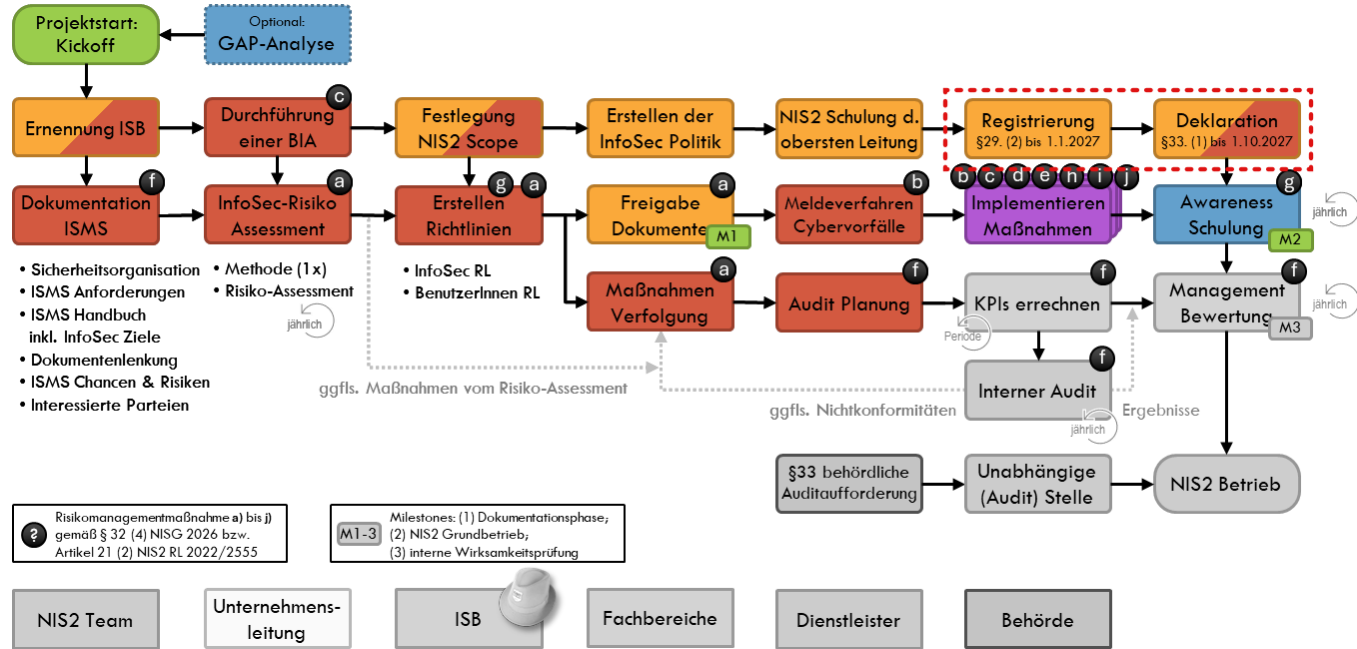
gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

A6.1 Bewerber Sicherheitsüberprüfung  
A5.19 InfoSec bei Lieferanten  
A5.20 Lieferantenvereinbarungen  
A6.6 Vertraulichkeitsvereinbarungen  
A8.5 Sichere Authentisierung  
A8.22 Trennung von Netzwerken  
A8.16 Überwachung von Aktivitäten  
A8.32 Änderungssteuerung

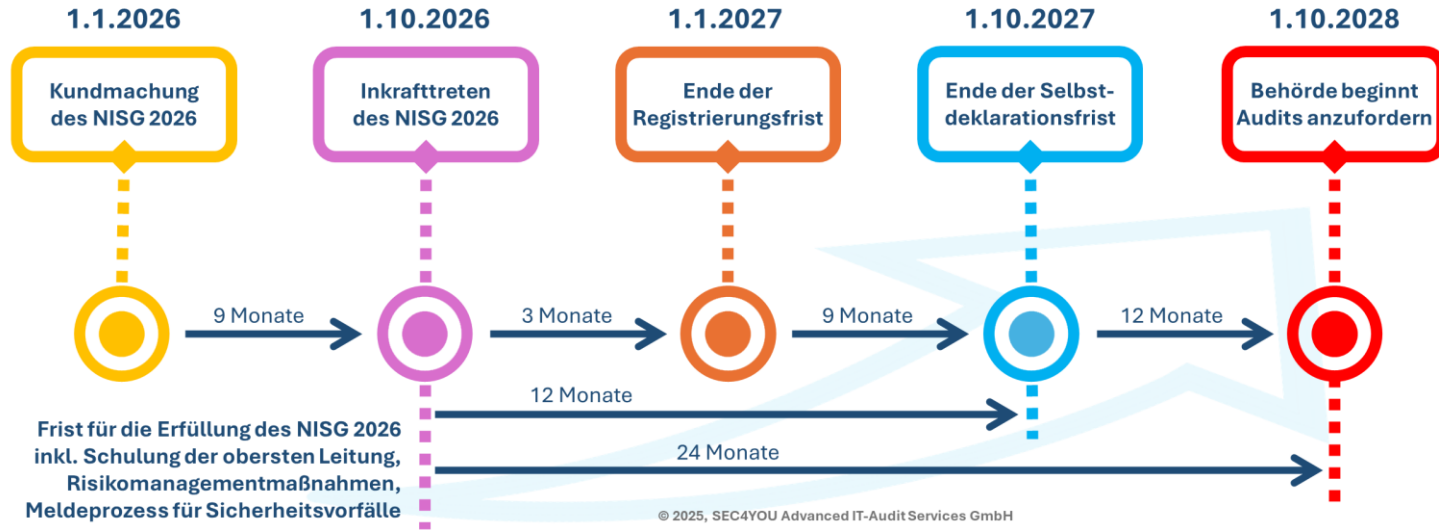
A8.5 Sichere Authentisierung

A5.10 zulässiger Gebrauch von Assets  
A5.30 BCM

# NIS-2 Registrierung und Selbstdeklaration



# Die Fristen für die Registrierung und Deklaration nicht verpassen!



© 2025, SEC4YOU Advanced IT-Audit Services GmbH

Die Fristen basieren auf der voraussichtlichen Veröffentlichung des NISG 2026 im Dezember 2025. Alle Informationen sind nach bestem Wissen und mit Sorgfalt zusammengestellt. Wir übernehmen keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit. Insbesondere stellen sie keinen Ersatz für im Einzelfall notwendige rechtliche Beratung dar.

## Was kann/wird passieren? → § 33 Nachweis der Wirksamkeit

---

- Ab dem **1.10.2028** kann das Bundesamt für Cybersicherheit (Teil des BMI) beginnen Audits durch unabhängige Stellen (früher QuaSte) zu fordern. Die Audits sind dreigeteilt in **organisatorische, operative** und **technische** Audits.
- Eine **aktive ISO 27001 Zertifizierung** mit passendem Scope kann **organisatorische und operative** Audits nachweisen, andernfalls haben **wesentliche Einrichtungen** nur **2 Monate** Zeit solche Audits nachzuweisen, **wichtige Einrichtungen** jedoch haben **24 Monate** Zeit.
- **Technische** Audits durch unabhängige Stellen müssen von allen Einrichtungen innerhalb von 24 Monaten nachgewiesen werden.

## Tipps für die erfolgreiche NIS-2 Umsetzung

- Lokale Anforderungen in anderen EU-Ländern berücksichtigen
- Verantwortlichkeiten klar festlegen
- Wirksamkeit von Maßnahmen in den Fokus stellen
- Dokumentation / Nachweise – Was nicht dokumentiert ist existiert nicht!
- Silobildung für NIS-2 Anforderungen vermeiden (z.B. DSGVO, RKEG)
- Andere Managementsysteme einbinden (z.B. QM)
- Von anderen Branchen lernen (z.B. IKS in Finanzunternehmen)
- Rechtzeitig beginnen (Implementierung, externes Audit)



## Offene Fragen

---



Andreas.Schuster@sec4you.com

<https://sec4you.com>

Tel.: +43 678 1216943

