

NIS2 Schulungsnachweis für die Geschäftsleitung

Artikel 20 Abs. 2, Richtlinie (EU) 2022/2555 · § 38 Abs. 3 BSIG (NIS2UmsuCG)

KOSTENLOSE VORLAGE — XLSX · PDF · MD | Version 1.0 · Stand 2026-07-21

Was die Arbeitsmappe enthält

Geschäftsleitungs-Regi-ster	Eine Zeile pro Mitglied des Leitungsorgans: Name, Rolle, Organ, Beststellungsdatum, Anwendbarkeit der Art.-20-Pflicht (mit Begründung), Status sowie zwei berechnete Spalten — letzte absolvierte Sitzung und nächste Fälligkeit. Prüfer gleichen Schulungsnachweise gegen genau diese Liste ab; überfällige Mitglieder werden automatisch markiert.
Schulungsprotokoll	Eine Zeile pro Mitglied und Sitzung: Titel, Anbieter und Anbietertyp, Datum, Dauer in Stunden, Format, welche der drei Ziele aus Art. 20 Abs. 2 abgedeckt wurden (Risiken erkennen / Praktiken bewerten / Auswirkungen auf die Dienste), Wiederholungsintervall, berechnete Fälligkeit, Nachweisreferenz (Zertifikat, Teilnehmerliste, LMS-Export) und Abschlussstatus.
Sitzungskatalog	Das Schulungsprogramm nach vorn: geplante Sitzungen mit Zielgruppe, Zielen, Frequenz, Durchführungsform, Anbieter und — zunehmend gefragt — einer Wirksamkeitsmessung je Sitzung. Das Programmdokument, das neben den Einzelnachweisen erwartet wird.
Länderreferenz	Wie die Schulungspflicht dort quantifiziert ist, wo Sie tätig sind: EU-Basis, Deutschlands § 38 Abs. 3 BSIG mit dem Richtwert von ~4 Stunden mindestens alle 3 Jahre aus der Gesetzesbegründung, Lettlands Regelmäßigkeitsregel mit jährlicher Inhaltsprüfung, Tschechiens Schulungspflicht für Leitungsorgane, Belgiens CCB-Ermessensmodell, Norwegens Digital sikkerhetsloven und der freiwillige UK Cyber Governance Code of Practice.

Die rechtliche Leiter

Art. 20 Abs. 1	Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen die Risikomanagementmaßnahmen nach Artikel 21 billigen , ihre Umsetzung überwachen und können für Verstöße verantwortlich gemacht werden . Billigung setzt dokumentiertes Verständnis voraus — genau dafür existiert die Schulungspflicht.
Art. 20 Abs. 2	Die Mitglieder der Leitungsorgane sind verpflichtet, an Schulungen teilzunehmen , um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie von Risikomanagementpraktiken und deren Auswirkungen auf die Dienste zu erwerben. Mitarbeiterschulungen werden hier nur <i>empfohlen</i> — die verpflichtende Schulung der Beschäftigten steht in Artikel 21 Abs. 2 Buchst. g und wird getrennt geführt.
§ 38 BSIG	Deutschlands Umsetzung, in Kraft seit dem 6. Dezember 2025 ohne Übergangsfrist: Geschäftsleiter müssen regelmäßig an Schulungen teilnehmen (Abs. 3) — eine persönliche, nicht delegierbare Pflicht — und haften bei schuldhaften Verstößen persönlich (Abs. 2); ein Verzicht der Gesellschaft auf Regressansprüche ist unwirksam. Das Gesetz sagt nur „regelmäßig“; die Gesetzesbegründung nimmt als Richtwert etwa einen halben Tag (~4 Stunden) mindestens alle drei Jahre an.
Nachweis	Aufsichtsbehörden prüfen Einzelnachweise , keine Dashboards: Name, Rolle, Datum, Dauer, Inhalte gemappt auf die Ziele des Art. 20 Abs. 2, Anbieter, Abschlussnachweis, nächste Fälligkeit — plus Programmdokument und die Protokolle, in denen das geschulte Organ das Art.-21-Maßnahmenset tatsächlich billigt.

Wie oft ist „regelmäßig“? — nationale Quantifizierungen

Jurisdiktion	Regel	Quantifizierung
EU-Basis	Art. 20 Abs. 2: Mitglieder der Leitungsorgane müssen an Schulungen teilnehmen	Keine — nur zweckbestimmt
Deutschland	§ 38 Abs. 3 BSIG: regelmäßig, persönlich, nicht delegierbar; in Kraft seit 6.12.2025	~4 Std. mindestens alle 3 Jahre (Richtwert der Begründung, nicht Gesetz)

Lettland	Kiberdrošības likums (1.9.2024) + VO 397 (2.7.2025): Leitungsschulung Pflicht; regelmäßige Mitarbeiterschulung, Inhalte mindestens jährlich geprüft	Regelmäßig — meist jährlich umgesetzt
Tschechien	Gesetz Nr. 264/2025 Slg. (1.11.2025): Leitungsorgane müssen Cybersicherheit beaufsichtigen und geschult sein	Keine feste Vorgabe — Nachweise dokumentieren
Belgien	Gesetz vom 26.4.2024 Art. 31 §2 + CCB: regelmäßige Schulung, Umfang im Ermessen der Einrichtung	Keine — höhere Erwartungen an wesentliche Einrichtungen
Norwegen	Digitalsikkerhetsloven (1.10.2025): Leitung billigt das Sicherheitsmanagementsystem, jährliche Überprüfung; Schulung gemäß NIS2 erwartet	Keine feste Vorgabe
UK	Cyber Security and Resilience Bill: keine gesetzliche Schulungspflicht; freiwilliger Cyber Governance Code of Practice	Keine

Das prüfungsreife Nachweispaket

Der Schulungsnachweis ist ein Artefakt in einem Fünfer-Paket, auf das sich Aufsichtsbehörden zubewegen: **(1)** das namentliche Register des Leitungsorgans; **(2)** individuelle Schulungsnachweise je Mitglied — diese Arbeitsmappe; **(3)** das Programmdokument — der Sitzungskatalog; **(4)** Protokolle, in denen das geschulte Organ die Art.-21-Maßnahmen billigt (Version, Datum, Teilnehmer namentlich); und **(5)** Wirksamkeitsnachweise — Tabletop-Berichte, protokollierte Briefings mit Folgemaßnahmen. Halten Sie die Nachweisreferenzen auf real abgelegte Artefakte gerichtet: Ein Zertifikat, das auf Anfrage nicht vorgelegt werden kann, existiert aus Sicht einer Prüfung nicht.

Warum das jetzt zählt: Artikel 20 verknüpft Schulung mit Haftung — und § 38 Abs. 2 BSIg macht daraus seit dem 6. Dezember 2025 eine persönliche, verzichtsfeste Haftung der Geschäftsleiter. Eine Leitung, die Risikomanagementmaßnahmen billigt, ohne die eigene Schulung nachweisen zu können, liefert der Aufsicht eine einfache Feststellung frei Haus. Dieses Protokoll ist die günstigste Versicherung im NIS2-Nachweistapel.

Vom Schulungsnachweis zum käufersichtbaren Nachweis. Dieselben Governance-Nachweise, die Ihre Aufsicht prüft, fragen Enterprise-Käufer in Sicherheitsfragebögen ab („Erhält das Management Cybersicherheitsschulungen?“). Orbiq veröffentlicht Governance- und Schulungsnachweise in einem kontrollierten Trust Center — ein Datensatz beantwortet Behörde und Kunde zugleich. Die vollständige kostenlose Vorlagenbibliothek: orbiqhq.com/de/vorlagen.