EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

NIS2 UND CER IN LUXEMBURG

Verantwortung der Leitung

Pflichten, Entscheidungen und persönliche Risiken

Geschäftsführung, Verwaltungsrat und leitende Führungskräfte
Rechtsstand und Quellenprüfung: 22. November 2026



KI-Illustration · keine reale Einrichtung

Was die Leitung selbst verantwortet

Freigabe und Überwachung gehören ausdrücklich zur Leitungsaufgabe.

Risiken verstehen	Risikoanalyse und Handlungsbedarf vorlegen lassen, hinterfragen und bewerten.
Umsetzung ermöglichen	Angemessene Maßnahmen beschließen und erforderliche Mittel, Personal sowie Zuständigkeiten bereitstellen.
Wirksamkeit nachhalten	Umsetzung kontrollieren, Mängel beheben lassen und selbst regelmäßig an Schulungen teilnehmen.

> **Eine technische Delegation beseitigt diese eigenen Leitungspflichten nicht.**

NIS2 Art. 20–21 · LU-NIS2 Art. 12–13 · ILR-Leitungsleitfaden

Rechtsrahmen und Geltungsstand

EU-Richtlinien und Luxemburger Umsetzung werden getrennt zitiert.

NIS2	Richtlinie (EU) 2022/2555. Luxemburger Gesetz vom 5. Mai 2026, Mémorial A225, in Kraft seit 10. Mai 2026.
CER	Richtlinie (EU) 2022/2557. Luxemburger Gesetz vom 5. Mai 2026, Mémorial A226, in Kraft seit 10. Mai 2026.
Geltungsbereich	Rechtsform, Tätigkeit, Einstufung und sektorale Sonderregeln bestimmen die konkret geltenden Pflichten.

> **Diese Präsentation erläutert Luxemburg. Andere Staaten setzen die Richtlinien teilweise anders um.**

NIS2: LU-Gesetz A225 · CER: LU-Gesetz A226 · EU 2022/2555 und 2022/2557

LU NIS2 LU CER EU NIS2 EU CER

Welche Einrichtungen und Personen betroffen sind

Die Bezeichnung „kritisch“ im Alltag genügt für die rechtliche Einordnung nicht.

Thema	Pflicht und Konsequenz
NIS2-Einrichtung	Wesentliche oder wichtige Einrichtung nach Tätigkeit, Größe und gesetzlichen Sonderfällen. Auch öffentliche Stellen können erfasst sein.
CER-Einrichtung	HCPN oder CSSF ermittelt die Einrichtung. Die förmliche Bezeichnung erfolgt durch großherzoglichen Erlass; die Einrichtung erhält eine Mitteilung.
Leitungsperson	Organstellung, Vertretungs-, Entscheidungs- und Kontrollbefugnisse sind entscheidend. Ein IT-Jobtitel allein begründet keine Organstellung.

Einstufung, zuständige Behörde und tatsächlich zuständiges Leitungsorgan schriftlich klären.

NIS2 Art. 2–4, 20, 32(6) · LU-NIS2 Art. 1, 3, 11, 13, 22(6), 23(5) · CER Art. 6–8 · LU-CER Art. 3, 7–8

EU NIS2 LU NIS2 EU CER LU CER EU – DORA

Freigabe und Aufsicht bleiben bei der Leitung

Das Gesetz nennt die Verantwortung des Leitungsorgans ausdrücklich.

Genehmigung	Die Leitung genehmigt die Maßnahmen zur Beherrschung der Cyberrisiken.
Überwachung	Sie verfolgt Umsetzung, Wirksamkeit und die Behebung erkannter Mängel.
Eigene Verantwortung	Sie kann für Verletzungen dieser gesetzlichen Pflichten verantwortlich gemacht werden.

> **Ein Vertrag mit einem Dienstleister oder eine CISO-Benennung ersetzt keine Leitungsentscheidung.**

NIS2 Art. 20(1) · LU-NIS2 Art. 13(1), 22(6), 23(5)

EU NIS2 LU NIS2

Eine wirksame Aufgabenverteilung

Verantwortung braucht Befugnisse, Ressourcen und einen erreichbaren Entscheidungsweg.

Thema	Pflicht und Konsequenz
Leitungsorgan	Genehmigt Sicherheitsziele, Risikobehandlung und Mittel. Entscheidet über Eskalationen und kontrolliert Fortschritt.
Fachverantwortliche	Bewerten Risiken, entwickeln Maßnahmen, setzen sie im beauftragten Umfang um und berichten offen über Hindernisse.
Kontrolle und Vertretung	Fristen, Stellvertretungen, Berichtspflichten und unabhängige Prüfungen verhindern Zuständigkeitslücken.

Aufgaben, Entscheidungsbefugnisse und Eskalationswege müssen zueinander passen.

NIS2 Art. 20–21 · LU-NIS2 Art. 12–13 · praktische Umsetzungsempfehlung

Risikoanalyse als Entscheidungsgrundlage

Die Leitung muss wissen, welche Leistungen wie lange ausfallen dürfen und wodurch sie gefährdet sind.

01 Bestandsaufnahme

Wesentliche Dienste, IT und OT, Standorte, Daten, Personal und Dienstleister mit ihren Abhängigkeiten erfassen.

→ 02 Risikoszenarien

Cyberangriff, Stromausfall, Feuer, Überflutung, Sabotage und Fehlbedienung nach Eintrittswahrscheinlichkeit und Folgen bewerten.

→ 03 Risikobehandlung

Schutzbedarf, bestehende Kontrollen, verbleibende Risiken, Maßnahmen, Verantwortliche und Fristen dokumentieren.

> **Eine Maßnahmenliste ohne nachvollziehbare Risikoanalyse trägt keine belastbare Budgetentscheidung.**

NIS2 Art. 21(1)–(2)(a) · LU-NIS2 Art. 12(1)–(2) · ILR-Leitungsleitfaden

CER-Risikoanalyse für den gesamten Betrieb

Die Resilienz kritischer Dienste umfasst auch Gefahren außerhalb der IT.

9
Monate

4
Jahre

Frist und Wiederholung

Ab Mitteilung: Risikoanalyse binnen 9 Monaten; Kapitel 4 grundsätzlich nach 10 Monaten. Analyse bei Bedarf und mindestens alle 4 Jahre erneuern.

Alle relevanten Gefahren

Natürliche und menschengemachte Risiken, Unfälle, Gesundheitsnotlagen sowie hybride, terroristische und andere vorsätzliche Bedrohungen.

Abhängigkeiten

Ausfälle anderer Sektoren und grenzüberschreitender Dienste sowie die eigenen Auswirkungen auf andere Einrichtungen berücksichtigen.

> **Nationale Risikobewertung und konkrete Standort- und Betriebsrisiken zusammenführen.**

CER Art. 6(3), 12 · LU-CER Art. 7(4), 8, 11

EU CER LU CER

NIS2-Maßnahmen: Organisation und Versorgung

Der gesetzliche Mindestkatalog umfasst zehn Themenbereiche. Hier die ersten fünf.

Thema	Pflicht und Konsequenz
1. Risikopolitik	Verfahren zur Risikoanalyse und zur Sicherheit der Informationssysteme.
2. Vorfälle	Erkennung, Bearbeitung und Begrenzung von Sicherheitsvorfällen.
3. Kontinuität	Sicherungen, Wiederherstellung, Fortführung des Betriebs und Krisenmanagement.
4. Lieferkette	Sicherheitsanforderungen an direkte Lieferanten und Dienstleister.
5. Lebenszyklus	Sicherheit bei Beschaffung, Entwicklung und Wartung sowie Behandlung und Offenlegung von Schwachstellen.

Für jedes Thema müssen Verantwortlichkeit, erforderliche Mittel und überprüfbare Ergebnisse feststehen.

NIS2 Art. 21(2)(a)–(e) · LU-NIS2 Art. 12(2), Nr. 1–5

EU NIS2 LU NIS2

NIS2-Maßnahmen: Menschen und Zugänge

Die weiteren fünf Themen verbinden technische Sicherheit mit verlässlichen Abläufen.

Thema	Pflicht und Konsequenz
6. Wirksamkeit	Verfahren zur Bewertung, ob Sicherheitsmaßnahmen tatsächlich funktionieren.
7. Wissen	Cyberhygiene und Schulungen zur Cybersicherheit.
8. Kryptografie	Regeln für Kryptografie und, soweit erforderlich, Verschlüsselung.
9. Berechtigungen	Personalsicherheit, Zugangskontrolle und Verwaltung der schutzbedürftigen Werte.
10. Sichere Anmeldung	Mehrfaktor- oder kontinuierliche Authentifizierung sowie sichere Kommunikation und Notfallkommunikation nach Bedarf.

> **Kontrollen müssen umgesetzt, getestet und bei Mängeln ohne ungerechtfertigte Verzögerung verbessert werden.**

NIS2 Art. 21(2)(f)–(j), 21(4) · LU-NIS2 Art. 12(2), Nr. 6–10, 12(5)

EU NIS2 LU NIS2

Zutritt und Cybersicherheit gemeinsam planen

Ein digital geschütztes System bleibt durch seine physische Umgebung verwundbar.

Schutzzonen	Serverräume, Leitstellen, Technikräume und kritische Anlagen mit abgestuften Zutrittsrechten schützen.
Personenschutz	Flucht, Rettung und Brandschutz mit der Sicherung gegen unberechtigten Zutritt abstimmen.
Ausfallszenarien	Strom-, Netzwerk- und Systemausfälle, Notöffnung, Handbetrieb und sichere Wiederinbetriebnahme vorab festlegen.

> **Eine Türfunktion braucht eine abgestimmte Betriebs- und Notfallentscheidung.**

NIS2 Art. 21(2) · LU-NIS2 Art. 12(2) · CER Art. 13(1)(b)–(d) · LU-CER Art. 12

EU NIS2 LU NIS2 EU CER LU CER

CER-Maßnahmen für Schutz und Reaktion

Kritische Einrichtungen müssen geeignete und verhältnismäßige Maßnahmen aus ihrer Risikobewertung ableiten.

Vorsorge	Vorfälle möglichst verhindern. Dazu zählen Katastrophenvorsorge und Anpassung an relevante Klimarisiken.
Physischer Schutz	Anlagen und kritische Infrastruktur mit geeigneten Zutritts-, Überwachungs- und Objektschutzmaßnahmen sichern.
Reaktion	Folgen begrenzen, Krisenstrukturen aktivieren und festgelegte Verfahren für den Umgang mit Vorfällen anwenden.

> **Prävention, Schutz und Krisenreaktion müssen im Resilienzkonzept zusammenpassen.**

CER Art. 13(1)(a)–(c) · LU-CER Art. 12(1), Nr. 1–3

EU CER LU CER

CER-Maßnahmen für Fortführung und Personal

Resilienz endet erst mit der sicheren Wiederherstellung des wesentlichen Dienstes.

Wiederherstellung	Betriebskontinuität und alternative Lieferketten berücksichtigen, um die Bereitstellung des Dienstes wiederaufzunehmen.
Personalsicherheit	Sicherheitsrelevante Personengruppen und Funktionen bestimmen. Zugangsrechte, Qualifikation und Eignungsprüfungen rechtmäßig organisieren.
Schulung und Übungen	Mitarbeiter informieren und schulen, Bewusstsein fördern sowie Übungen zur praktischen Vorbereitung durchführen.

> **Der Resilienzplan verbindet Schutzmaßnahmen mit Personal, Abläufen und Wiederanlauf.**

CER Art. 13–14 · LU-CER Art. 12(1) Nr. 4–6, 12(2)–(3), 13–15

EU CER LU CER

Budget und Personal sind Leitungsentscheidungen

Eine genehmigte Schutzmaßnahme braucht die Voraussetzungen für ihre tatsächliche Umsetzung.

Entscheidungs-vorlage	Risiko, gesetzlicher Bezug, Handlungsoptionen, Kosten, Personalbedarf und Folgen des Unterlassens verständlich darstellen.
Freigabe	Angemessene Mittel und Kapazitäten bewilligen oder eine fachlich tragfähige Alternative mit Frist beschließen.
Eskalation	Nicht gedeckte erhebliche Risiken und blockierte Pflichtmaßnahmen an das zuständige Leitungsorgan zurückgeben.

> **„Kein Budget“ ist kein pauschaler Befreiungsgrund von gesetzlichen Schutzpflichten.**

NIS2 Art. 20–21 · LU-NIS2 Art. 12–13 · CER Art. 13 · ILR-Leitungsleitfaden

Schulung der Leitung und der Beschäftigten

Luxemburg verlangt ausdrücklich regelmäßige Schulung auf beiden Ebenen.

Leitung

\+

Personal

Leitung nimmt teil

Risiken erkennen, Maßnahmen beurteilen und Auswirkungen auf die erbrachten Dienste verstehen.

Einrichtung organisiert

Ähnliche Schulungsangebote regelmäßig für Beschäftigte bereitstellen und an Aufgaben sowie Risiken ausrichten.

Praxis und Nachweise

Teilnahmen, Inhalte und Lernziele dokumentieren. Krisenübungen und Wiederherstellungstests ergänzen die Wissensvermittlung.

> **Ein geschulter CISO ersetzt die Schulung der Geschäftsführung nicht.**

NIS2 Art. 20(2), 21(2)(g) · LU-NIS2 Art. 13(2), 12(2) Nr. 7 · CER Art. 13(1)(f)

EU NIS2 LU NIS2 EU CER LU CER ILR – Direction

Dienstleister und Produktlebenszyklus

Auslagerung verändert die Durchführung, aber nicht den Schutzbedarf der Einrichtung.

Vor der Beauftragung	Sicherheitsanforderungen, Zuständigkeiten, Meldewege, Nachweise und die Behandlung von Schwachstellen vereinbaren.
Im Betrieb	Berechtigungen, Fernzugriff, Updates, Supportende und tatsächliche Leistungsqualität überwachen.
Bei Wechsel oder Ausfall	Daten, Dokumentation und Zugänge verfügbar halten. Übergabe, Notbetrieb und alternative Versorgung vorbereiten.

> **Verträge und Zertifikate sind Belege. Die tatsächliche Leistung bleibt zu kontrollieren.**

NIS2 Art. 21(2)(d)–(e), 21(3) · LU-NIS2 Art. 12(2), 12(4) · CER Art. 13(1)(d)

EU NIS2 LU NIS2 EU CER

Kontrolle und laufende Verbesserung

Die Leitung braucht überprüfbare Ergebnisse statt einer bloßen Statusfarbe.

01 Wirksamkeit prüfen

Audits, Wiederherstellungstests, Berechtigungsprüfungen und Übungen mit klaren Prüfkriterien durchführen.

→ 02 Abweichungen verfolgen

Mängel priorisieren, Zuständigkeiten und Termine festlegen sowie überfällige Maßnahmen eskalieren.

→ 03 Ergebnisse entscheiden

Restrisiken und Zielkonflikte erneut bewerten. Personal, Verfahren und Maßnahmen bei Bedarf anpassen.

> **Ein erkannter wesentlicher Mangel darf nicht ohne Entscheidung im Bericht stehen bleiben.**

NIS2 Art. 20(1), 21(2)(f), 21(4) · LU-NIS2 Art. 12(2) Nr. 6, 12(5), 13(1)

EU NIS2 LU NIS2

Notfallplan und Krisenorganisation

Im Vorfall müssen Entscheidung, Kommunikation und operative Reaktion sofort funktionieren.

01 Auslösung

Schwellen, Alarmierung, erreichbare Kontakte und Vertretungen für unterschiedliche Szenarien festlegen.

→ 02 Krisenführung

Entscheidungsbefugnisse, Notfallbudget, Prioritäten und Zusammenarbeit mit Fachstellen sowie Behörden vorbereiten.

→ 03 Kommunikation

Interne Lagebilder, Ersatzkommunikation und rechtzeitige Information betroffener Empfänger und zuständiger Behörden organisieren.

> **Der Plan muss bei Ausfall der üblichen Systeme und Schlüsselpersonen nutzbar bleiben.**

NIS2 Art. 21(2)(b)–(c), (j), Art. 23 · LU-NIS2 Art. 12, 14 · CER Art. 13, 15

EU NIS2 LU NIS2 EU CER LU CER

Wiederanlauf bis zum sicheren Normalbetrieb

Ein vorhandenes Backup beweist noch keine Wiederherstellungsfähigkeit.

01 Prioritäten und Ziele

Kritische Dienste, zulässige Unterbrechung und vertretbaren Datenverlust festlegen. Abhängigkeiten beim Neustart berücksichtigen.

→ 02 Wiederherstellung testen

Integrität, Verfügbarkeit und tatsächliche Nutzbarkeit von Sicherungen prüfen. Wiederanlauf unter realistischen Bedingungen üben.

→ 03 Freigabe und Nachbereitung

Sicheren Zustand bestätigen, Rückkehr in den Normalbetrieb verantworten und Ursachen sowie Verbesserungen nachhalten.

> **Die Leitung muss die Wiederherstellungsfähigkeit des Dienstes kennen, nicht nur den Sicherungsplan.**

NIS2 Art. 21(2)(c), (f) · LU-NIS2 Art. 12(2) Nr. 3, 6 · CER Art. 13(1)(d)

EU NIS2 LU NIS2 EU CER LU CER

Meldungen brauchen vorbereitete Abläufe

Die beiden Rechtsrahmen verwenden unterschiedliche Meldeketten.

NIS2	Ab Kenntnis des erheblichen Vorfalls: Frühwarnung spätestens nach 24 Stunden, Vorfallmeldung nach 72 Stunden. Abschlussbericht spätestens einen Monat nach der Vorfallmeldung.
CER	Erhebliche Störung oder Störpotenzial: unverzüglich, grundsätzlich binnen 24 Stunden nach Kenntnis. Ausführlicher Bericht gegebenenfalls binnen eines Monats danach.
Leitungsaufgabe	Bewertung, Beweissicherung, Vertretung und Meldebefugnisse vorab klären. Betroffene Empfänger nach den jeweiligen Regeln informieren.

> **Unvollständige Erkenntnisse rechtfertigen kein pauschales Warten bis zum Abschluss aller Untersuchungen.**

NIS2 Art. 23 · LU-NIS2 Art. 14 · CER Art. 15 · LU-CER Art. 16

EU NIS2 LU NIS2 EU CER LU CER

Nachweise für Leitung und Aufsicht

Nachvollziehbare Dokumentation zeigt, was entschieden und tatsächlich umgesetzt wurde.

Entscheidungen	Einstufung, Risikoanalyse, Maßnahmenfreigaben, Budget, Verantwortliche und begründete Priorisierung.
Umsetzung	Konfigurationen, Wartung, Berechtigungen, Schulungen, Übungen und Ergebnisse von Wiederherstellungstests.
Korrektur	Mängelberichte, Eskalationen, Fristen, Abschlussnachweise und erneute Wirksamkeitsprüfung.

> **Dokumentation unterstützt den Nachweis. Sie ersetzt die tatsächliche Schutzwirkung nicht.**

NIS2 Art. 32–33 · LU-NIS2 Art. 22–23 · CER Art. 13, 21 · LU-CER Art. 12, 18

EU NIS2 LU NIS2 EU CER LU CER

Wesentliche Einrichtungen: neue ILR-Melderegeln

Die Verordnung ILR/N26/10 gilt seit 3. November 2026 für die Meldung an das ILR.

Drei Unterlagen	Bestehende Schutzmaßnahmen, wesentliche Cyberrisikoszenarien und mehrjähriger Maßnahmenplan mit Fristen, Verantwortlichen und Prioritäten.
Termin und Änderungen	Jährlich bis 15. März, auch ohne Änderungen. Zusätzlich bei erheblichen Risikoänderungen, neuem Hauptrisiko oder besonders wichtigen Sicherheitsmaßnahmen.
Kritische Einrichtungen	Als CER-kritisch identifizierte wesentliche Einrichtungen melden zusätzlich ihre Abhängigkeiten von direkten Lieferanten und Dienstleistern.
Sicher übermitteln	Über SERIMA oder einen vom ILR als gleichwertig anerkannten sicheren Weg. Weitere Informationen nach behördlicher Anforderung.

> **Nächster jährlicher Regeltermin: 15. März 2027. Ereignisbezogene und behördliche Fristen können früher greifen.**

LU-NIS2 Art. 12(3), 22 · ILR/N26/10 Art. 1–8 · Mémorial A532 vom 30.10.2026

LU NIS2 ILR/N26/10

Was die Aufsicht verlangen kann

Finanzielle Sanktionen sind nur ein Teil der möglichen Folgen.

Thema	Pflicht und Konsequenz
NIS2: wesentlich	Vor-Ort-Prüfungen, Fernkontrollen, Audits, Sicherheitsprüfungen, Nachweise und verbindliche Abhilfe. Auch laufende Aufsicht ist möglich.
NIS2: wichtig	Aufsicht grundsätzlich nachträglich bei Hinweisen auf Verstöße. Informations-, Prüf- und Durchsetzungsbefugnisse bleiben erheblich.
CER	Informationen, Inspektionen und Audits zur Resilienz. Festgestellte Verstöße sind innerhalb vorgegebener Fristen zu beheben.

Behördliche Abhilfe und Nachweise binden zusätzlich Zeit, Personal und externe Prüfungskapazität.

NIS2 Art. 32–33 · LU-NIS2 Art. 22–23 · CER Art. 21 · LU-CER Art. 18

EU NIS2 LU NIS2 EU CER LU CER

NIS2: hohe Bußgelder gegen die Einrichtung

Für Verstöße gegen Risikomanagement- oder zentrale Meldepflichten gilt jeweils der höhere Höchstbetrag.

Wesentliche Einrichtung

10 Mio. €

oder 2 %

weltweiter Vorjahresumsatz

Wichtige Einrichtung

7 Mio. €

oder 1,4 %

weltweiter Vorjahresumsatz

Der höhere Betrag ist maßgeblich

Bei 800 Millionen Euro maßgeblichem Unternehmensumsatz: höchstens 16 Millionen Euro beziehungsweise 11,2 Millionen Euro.

> **Das sind Obergrenzen im Einzelfall, keine Mindeststrafe und keine automatische Privatbuße der Geschäftsführung.**

NIS2 Art. 34(4)–(5) · LU-NIS2 Art. 26(4)–(5), bezogen auf Art. 12 und 14(1)–(4)

EU NIS2 LU NIS2

NIS2: weitere Sanktionen und Zwangsgeld

Auch Leitungs- und Schulungspflichten haben einen eigenen Sanktionsrahmen.

Bis 250.000 Euro	Gegen die Einrichtung für die in LU-Art. 25 genannten Pflichten, darunter Leitungsfreigabe, Überwachung und regelmäßige Schulung nach Art. 13.
Weitere Folgen	Warnung oder förmlicher Tadel. Je nach Rechtsgrundlage können verbindliche Abhilfe, Veröffentlichungen und weitere Aufsichtsmaßnahmen hinzukommen.
Zwangsgeld	Bis 1.250 Euro pro Tag, insgesamt bis 25.000 Euro je festgestelltem Verstoß, um dessen Beendigung durchzusetzen.

> **Die Beträge und Rechtsgrundlagen dürfen nicht als automatisch kumulierte Gesamtrechnung dargestellt werden.**

LU-NIS2 Art. 25(1), Art. 26(7), Art. 22–24

CER: nationaler Sanktionsrahmen

CER übernimmt nicht die NIS2-Umsatzformel.

Bis 250.000 Euro	Verwarnung, Rüge und/oder administrative Geldbuße bis 250.000 Euro gegen die kritische Einrichtung bei den gesetzlich bezeichneten Verstößen.
Abhilfe und Prüfung	Behördliche Anweisungen, Inspektionen, Audits sowie die Pflicht, festgestellte Mängel fristgerecht zu beheben.
Gesonderte Folgen	Vertrags-, Haftungs- oder strafrechtliche Folgen können hinzukommen, wenn deren eigene Voraussetzungen erfüllt sind.

> **Eine pauschale CER-Strafe von 10 Millionen Euro oder 2 % wäre für diesen Luxemburger Rahmen falsch.**

CER Art. 21–22 · LU-CER Art. 18(1)–(4), 19(1)–(5)

EU CER LU CER

Zeitweiliges Verbot einer Leitungsfunktion

Gerichtliche Eskalation bei wesentlichen NIS2-Einrichtungen; die erfasste öffentliche Verwaltung ist ausgenommen.

01 Voraussetzung

Bestimmte behördliche Abhilfemaßnahmen bleiben unwirksam. Eine zusätzliche gesetzte Frist verstreicht ohne erforderliche Umsetzung.

→ 02 Gericht entscheidet

Auf Antrag der Aufsicht kann der Präsident des Bezirksgerichts Luxemburg zeitweilig Leitungsfunktionen in dieser Einrichtung untersagen.

→ 03 Umfang und Ende

Erfasst sind Personen auf Ebene des Generaldirektors oder gesetzlichen Vertreters. Abhilfe und gerichtliche Aufhebung beenden die Maßnahme.

> **Kein automatischer Ausschluss aus dem Unternehmen und kein pauschales lebenslanges Berufsverbot.**

NIS2 Art. 32(5) · LU-NIS2 Art. 22(5)

EU NIS2 LU NIS2

Persönliche Verantwortung hat mehrere Grundlagen

Unternehmensbußgeld und persönliche Haftung sind rechtlich verschiedene Ebenen.

Thema	Pflicht und Konsequenz
NIS2-Leitungspflicht	Leitungsorgane können für Pflichtverletzungen verantwortlich sein. Personen mit Vertretungs-, Entscheidungs- oder Kontrollbefugnis müssen die Einhaltung sichern.
Zivilrecht	Die Gesellschaft oder unter besonderen Voraussetzungen Dritte können Ersatz eines zurechenbar verursachten Schadens verlangen.
Strafrecht	Persönliche Strafen setzen einen einschlägigen Straftatbestand und dessen konkrete Voraussetzungen voraus.

Auch andere leitende Personen können betroffen sein. Entscheidend sind ihre tatsächlichen Pflichten und Befugnisse.

NIS2 Art. 20(1), 32(6), 33(5) · LU-NIS2 Art. 13(1), 22(6), 23(5) · Guichet.lu

EU NIS2 LU NIS2 Guichet – Civil Guichet – Pénal

Wann Schadenersatz persönlich in Betracht kommt

Im Zivilrecht sind Pflichtverletzung, Schaden und Kausalität zentrale Fragen.

Thema	Pflicht und Konsequenz
Gegenüber der Gesellschaft	SA: Mandats- und Geschäftsführungsfehler nach Art. 441-9. SARL: Geschäftsführerhaftung über Art. 710-16 desselben Gesetzes.
Gegenüber Dritten	Gesellschaftsgesetz- oder Satzungsverstöße: besondere Haftung nach Art. 441-9. Sonstige Managementfehler benötigen eine gesonderte Anspruchsgrundlage.
Individuelle Prüfung	Rechtsform, Organstellung, Zuständigkeit, Verhalten, Kenntnis und Beitrag zum Schaden müssen beurteilt werden.

Ein Sicherheitsvorfall beweist noch kein Verschulden. Ignorierte konkrete Warnungen können aber entscheidend sein.

LSC Art. 441-8, 441-9, 710-16 · dualistische SA: Art. 442-10, 442-16 · Guichet.lu

Fahrlässigkeit, grobes Versagen und bewusste Ablehnung

Es gibt keine allgemeine NIS2-Tabelle „Verschuldensgrad gleich fester Eurobetrag“.

Fahrlässiges Versäumnis	Eine erforderliche Prüfung oder Kontrolle unterbleibt. Zu prüfen ist, was eine sorgfältige Leitung in dieser Situation hätte erkennen und tun müssen.
Besonders schweres Versagen	Offenkundige erhebliche Risiken oder wiederholte Warnungen bleiben unbeachtet. Die rechtliche Qualifikation hängt vom Einzelfall ab.
Bewusste Verweigerung	Erforderliche Maßnahmen oder verbindliche Anordnungen werden trotz Kenntnis und Handlungsmöglichkeit nicht umgesetzt.

> **Kenntnis, Dauer, Wiederholung, Folgen, Kooperation und konkrete Handlungsmöglichkeiten beeinflussen die Bewertung.**

NIS2 Art. 32(7), 34(3) · LU-NIS2 Art. 22(7), 26(3) · allgemeines Haftungsrecht

Weitere mögliche persönliche und betriebliche Folgen

Ein Vorfall kann mehrere Rechts- und Geschäftsbeziehungen gleichzeitig betreffen.

Persönliche Folgen	Schadenersatz, gesellschaftsrechtliche Abberufung oder arbeitsrechtliche Folgen nach den jeweils geltenden Regeln.
Strafrechtliche Folgen	Bei zusätzlich erfüllten Straftatbeständen können Geld- oder Freiheitsstrafen in Betracht kommen. NIS2/CER allein machen nicht jeden Vorfall strafbar.
Betriebliche Folgen	Ausfallkosten, Wiederherstellung, Kundenansprüche, Vertragsfolgen und Reputationsschäden können die eigentliche Geldbuße übersteigen.

> **Versicherung oder D&O-Schutz beseitigen die Pflichten nicht und decken nicht automatisch jeden Schaden oder jede Sanktion.**

Guichet.lu: zivil- und strafrechtliche Verantwortung · konkrete Verträge und anwendbares Sektorrecht · Code pénal Art. 418–420

Guichet – Civil Guichet – Pénal Code pénal

Gesondertes Strafrecht bei Personenschäden

Diese Tatbestände des Code pénal gelten eigenständig. Dargestellt sind die gesetzlichen Grundstrafrahmen.

Thema	Pflicht und Konsequenz
Art. 418: Voraussetzungen	Mangelnde Voraussicht oder Vorsicht verursacht Tod oder Körperverletzung ohne Verletzungsvorsatz. Fehler, Personenschaden und Kausalität sind nachzuweisen.
Art. 419: fahrlässige Tötung	3 Monate bis 2 Jahre Freiheitsstrafe und 500 bis 10.000 Euro Geldstrafe.
Art. 420: fahrlässige Körperverletzung	8 Tage bis 2 Monate Freiheitsstrafe und 500 bis 5.000 Euro Geldstrafe, oder nur eine dieser Strafen.

> **Die persönliche Zurechnung ist gesondert zu prüfen. Auch leichte Fahrlässigkeit kann den Tatbestand erfüllen.**

Code pénal Art. 418–420 · amtliche geltende Konsolidierung vom 19.12.2025, S. 100–101

Code pénal Guichet – Pénal

Beispiel: bekannte Lücke und abgelehnte Mittel

Fiktiver Fall einer wesentlichen Einrichtung mit Fernzugriff auf kritische Systeme.

Ausgangslage

Die IT meldet ein erhebliches Zugangsrisiko. Eine angemessene Absicherung und eine günstigere Übergangslösung werden erläutert.

Leitungsentscheidung

Beide Lösungen werden ohne tragfähige Alternative abgelehnt. Warnungen und Umsetzungsfristen bleiben unbeachtet.

Mögliche Folgen

Aufsicht und Abhilfe, NIS2-Bußgeld gegen die Einrichtung. Bei nachgewiesenem Pflichtverstoß und kausalem Schaden können persönliche Ansprüche hinzukommen.


KI-Illustration · keine reale Einrichtung

> **Entscheidend ist die nachweisbare Entscheidung über das bekannte Risiko und den erforderlichen Schutz.**

Fiktives Beispiel · NIS2 Art. 20–21, 32–34 · LU-NIS2 Art. 12–13, 22, 26

Beispiel: Ausfall ohne getesteten Wiederanlauf

Fiktiver Fall einer kritischen Versorgungseinrichtung mit IT, OT und gesichertem Standort.

Ausgangslage

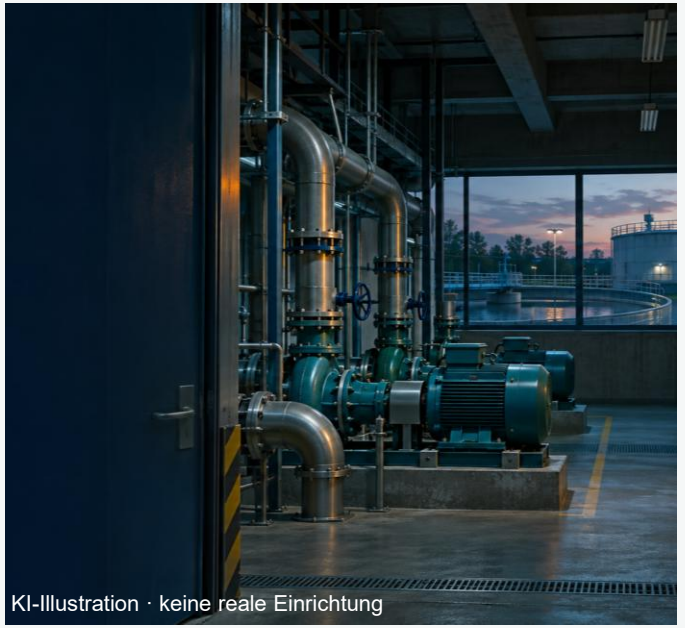
Stromausfall und Zutrittsstörung treffen gleichzeitig auf. Der Wiederanlauf wurde nie mit dem Betrieb geübt.

Organisationsmangel

Vertretung, Notöffnung, Ersatzversorgung und Wiederherstellungsreihenfolge sind ungeklärt. Erforderliche Übungen wurden wiederholt verschoben.

Mögliche Folgen

CER-Abhilfe und nationale Geldbuße, gegebenenfalls zusätzlich NIS2-Verfahren. Weitere Haftungsfragen bei zurechenbaren Personen- oder Sachschäden.



KI-Illustration · keine reale Einrichtung

> **Die Verantwortung betrifft das Zusammenspiel des gesamten Dienstes bis zum sicheren Wiederanlauf.**

Fiktives Beispiel · CER Art. 12–13, 21–22 · LU-CER Art. 11–12, 18–19 · LU-NIS2 Art. 12

Beispiel: behördliche Abhilfe wird verweigert

Fiktiver Fall einer wesentlichen NIS2-Einrichtung nach einer Aufsichtsprüfung.

Feststellung	Die Behörde verlangt konkrete Abhilfe. Die Leitung erhält klare Anforderungen und Fristen.
Weitere Eskalation	Maßnahmen bleiben unwirksam. Auch eine zusätzliche Frist verstreicht ohne erforderliche Umsetzung.
Mögliche Folgen	Gerichtlich angeordnete zeitweilige Aussetzung einer relevanten Genehmigung oder Zertifizierung sowie Verbot von Leitungsfunktionen in dieser Einrichtung.

> **Die gesetzliche Eskalation kann die persönliche Ausübung der Leitung und den Geschäftsbetrieb direkt treffen.**

Fiktives Beispiel · NIS2 Art. 32(5) · LU-NIS2 Art. 22(5)

EU NIS2 LU NIS2

Beispiel: Leitungsschulung und Meldung fehlen

Fiktiver Fall einer wichtigen NIS2-Einrichtung mit wiederholten organisatorischen Lücken.

Schulung unterbleibt	Die Leitung lehnt eigene Schulung ab und stellt kein regelmäßiges Schulungsangebot für das Personal sicher.
Meldeweg versagt	Ein erheblicher Vorfall wird erkannt. Niemand verfügt über die notwendige Vertretung und Befugnis zur fristgerechten Meldung.
Mögliche Folgen	Leitungs- und Schulungspflichten fallen unter LU-Art. 25. Verstöße gegen zentrale Meldepflichten können den Rahmen von LU-Art. 26(5) eröffnen.

> **Unterschiedliche Pflichtverletzungen haben unterschiedliche Rechtsgrundlagen und Sanktionsrahmen.**

Fiktives Beispiel · LU-NIS2 Art. 13–14, 25–26 · NIS2 Art. 20, 23, 34

Verhältnismäßig entscheiden und Pflichtlücken schließen

Die Leitung darf priorisieren. Sie muss dabei ein rechtmäßiges Schutzniveau sicherstellen.

Begründete Auswahl	Gleichwertige Maßnahmen, Umsetzungskosten, Wirksamkeit und konkrete Risiken gegeneinander abwägen.
Beherrschter Übergang	Bis zur endgültigen Lösung geeignete Zwischenmaßnahmen, Zuständigkeiten, Fristen und Kontrolle festlegen.
Grenze der Risikoakzeptanz	Eine interne Freigabe setzt gesetzliche Pflichten oder verbindliche behördliche Anordnungen nicht außer Kraft.

> **Tragfähige Alternativen sind möglich. Eine unbegründete Dauerblockade erforderlicher Maßnahmen ist keine Lösung.**

NIS2 Art. 21(1), 21(4) · LU-NIS2 Art. 12(1), 12(5), 13 · CER Art. 13

EU NIS2 LU NIS2 EU CER

Beschlussvorlage für das Leitungsorgan

Ein verwendbarer Beschluss verbindet Risiko, Entscheidung und Umsetzungsnachweis.

Thema	Pflicht und Konsequenz
Entscheidungs-grundlage	Betroffener Dienst, Risikobewertung, gesetzlicher Bezug, Handlungsoptionen und Folgen des Unterlassens.
Verbindlicher Beschluss	Gewählte Maßnahmen, Budget, Personal, verantwortliche Person, Fristen und notwendige Zwischenmaßnahmen.
Kontrolle	Berichtstermin, Wirksamkeitskriterien, Eskalationsschwelle und Nachweis der vollständigen Umsetzung.

> **Empfehlung: Jede erhebliche offene Schutzlücke erhält eine nachvollziehbare Leitungsentscheidung.**

Umsetzungsempfehlung auf Grundlage von LU-NIS2 Art. 12–13 und LU-CER Art. 11–12

LU NIS2 LU CER

Ein möglicher Arbeitsplan für die nächsten 90 Tage

Organisationsvorschlag. Bereits fällige Pflichten und behördliche Fristen haben Vorrang.

01 Tage 1–30

Betroffenheit, Leitungsverantwortung, wesentliche Dienste, offene Risiken und Sofortmaßnahmen klären.

→ 02 Tage 31–60

Risikobehandlung, erforderliche Mittel, Schulungen, Notfallorganisation und Lieferantenanforderungen beschließen und umsetzen.

→ 03 Tage 61–90

Wiederherstellung und Krisenabläufe erproben, Wirksamkeit prüfen und verbleibende Lücken verbindlich nachverfolgen.

> **Die 90 Tage sind keine gesetzliche Schonfrist und kein Aufschub für dringenden Schutzbedarf.**

Praktische Umsetzungsempfehlung · gesetzliche Bezugspunkte: LU-NIS2 Art. 12–14, LU-CER Art. 11–12, 16

LU NIS2 LU CER

Acht Fragen für die nächste Leitungssitzung

Die Antworten sollten durch aktuelle Entscheidungen und Nachweise belegt sein.

Betroffenheit und Risiken	Sind Einstufung und Zuständigkeit geklärt? Liegt eine belastbare aktuelle Risikoanalyse vor?
Maßnahmen und Ressourcen	Sind erforderliche Maßnahmen genehmigt? Reichen Budget, Personal und Befugnisse zur Umsetzung?
Schulung und Kontrolle	Nimmt die Leitung regelmäßig an Schulungen teil? Werden Wirksamkeit und Mängelbehebung überprüft?
Krise und Wiederanlauf	Funktionieren Meldewege und Notfallorganisation? Ist die sichere Wiederherstellung tatsächlich getestet?

> **Offene Antworten gehören mit Verantwortlichen und Fristen auf die Beschlussliste.**

Leitungscheck auf Grundlage von NIS2 Art. 20–23 und CER Art. 12–15

EU NIS2 EU CER LU NIS2 LU CER

Rechtsquellen und Artikelzuordnung

Die kurzen Quellenangaben jeder Folie beziehen sich auf diese amtlichen Texte.

Thema	Pflicht und Konsequenz
NIS2: Governance	EU-Art. 20 → LU-Art. 13. EU-Art. 21 → LU-Art. 12. EU-Art. 23 → LU-Art. 14.
NIS2: Durchsetzung	EU-Art. 32–34 → LU-Art. 22–23, 26. Ergänzende Sanktionen: LU-Art. 25. Datenschutz: EU-Art. 35 → LU-Art. 24.
CER	EU-Art. 12–13 → LU-Art. 11–12. EU-Art. 15 → LU-Art. 16. EU-Art. 21–22 → LU-Art. 18–19.

Maßgeblich sind die anwendbaren Luxemburger Vorschriften. Die EU-Artikel erläutern den gemeinsamen Rahmen.

Amtliche Volltexte: EUR-Lex und Legilux, Gesetzesfassungen A225 und A226 vom 5. Mai 2026

EU NIS2 LU NIS2 EU CER LU CER ILR/N26/10

Einordnung und weiterführende Grundlagen

Eine belastbare Führungsentscheidung verbindet Rechtsprüfung, fachliche Bewertung und nachweisbare Umsetzung.

Amtliche Erläuterungen	ILR: NIS2 und Leitungsleitfaden. HCPN: Resilienz kritischer Einrichtungen. Maßgeblich bleiben die anwendbaren Rechtsvorschriften.
Persönliche Haftung	Guichet.lu erläutert zivil- und strafrechtliche Verantwortung. Die Rechtsform und der konkrete Sachverhalt bestimmen die anwendbaren Regeln.
Nächster Schritt	Pflichten und offene Risiken gemeinsam mit Recht, IT, Betrieb, Sicherheit und zuständigem Leitungsorgan in einen verbindlichen Maßnahmenplan überführen.

EIWTC Security Advisory · Sicherheitsberatung und Zutrittsplanung · eiwtc.lu

Quellenprüfung: 22.11.2026 · Fiktive Beispiele · Allgemeine Information, keine individuelle Rechtsberatung

ILR ILR – Direction HCPN Guichet – Civil Guichet – Pénal