

Vorbereitung auf die NIS2-Bewertung

Leitfaden für Leitung und IT • Ergänzt den Excel-Fragebogen mit Antwortauswahl

Dieses Material ergänzt die anfängliche Checkliste „Gilt NIS2 für Ihr Unternehmen?“, die unverändert bleibt. Es hilft uns, den Umfang, die Verantwortlichkeiten und die bekannte Situation vor einer Bewertung oder Prüfung zu verstehen. Wir bitten Sie nicht, technische Untersuchungen durchzuführen, um zu antworten.

Ergebnis dieser Phase

Eine deklarierte Sicht der Situation, die Informationen, die geklärt werden müssen, und eine Grundlage für die Auswahl des geeigneten Dienstes, die nicht zu einem offiziellen DNSC-Score, einem Zertifikat oder einer Bestätigung der Einhaltung führt.

So füllen Sie die Datei aus

WER	WO AUSFÜLLEN	WELCHE ANGABEN
Anfragekoordinator	01_Profil und 05_Fristen	Die Entität, ungefähre Volumina, Kontrollen und bekannte Phasen.
Leitung / benannte Person	02_Leitung — 14 Fragen	Verantwortlichkeiten, kritische Aktivitäten, Risiken, Entscheidungen und Ressourcen.
Interne IT, IT-Dienstleister oder Konzern	03_IT — 24 Fragen; 04_Sonderfalle — 6	Vorliegen von Maßnahmen, abgedeckter Anwendungsbereich und etwaige Unbekannte.

Richtzeit: 10-15 Minuten für das Management und 15-25 Minuten für die IT zuzüglich der Profildaten. Dies sind Schätzungen, keine festgelegten Fristen. Für jede juristische Person wird eine Kopie ausgefüllt.

Fünf Antworten ohne lange technische Erläuterungen

Ja — die Situation ist für den gesamten relevanten Umfang bekannt. Teilweise — nur ein Teil ist abgedeckt. Nein — nach bekanntem Stand besteht die Maßnahme nicht. Unbekannt — die Information lässt sich nicht bestätigen. Möglicherweise nicht anwendbar — begründen Sie dies; die Anwendbarkeit wird später geprüft.

Nur die hellgelben Felder ausfüllen. Bei „Ja“ wird der Nachweis später überprüft. Bei „Möglicherweise nicht zutreffend“ stellt die Erklärung keinen rechtlichen Ausschluss dar. Die Zusammenfassung zählt die Antworten aus; sie berechnet keinen Prozentsatz der Einhaltung.

Klärung vor der Bewertung

Der Fragebogen trennt Leitungsentscheidungen von technischer Umsetzung. Eine Lizenz allein belegt keine Konformität. Ein Dienstleister übernimmt nicht automatisch alle Leitungspflichten. [R1–R3]

FUNKTION	KERNFRAGE	ORIENTIERUNGSBEISPIELE
Steuern — GV	Wer entscheidet und überwacht?	Zuständigkeiten, Richtlinien, Risiken, Lieferanten, Budget und Berichte.
Identifizieren — ID	Was muss geschützt werden?	Bekannte Ressourcen und Anwendungen, kritische Tätigkeiten, Schwachstellen und Abhängigkeiten.
Schützen — PR	Was verringert das Risiko?	Zugriff, Authentifizierung, Geräte, Daten, Schulung, Sicherungen und Segmentierung.
Erkennen — DE	Wer erkennt Probleme?	Warnungen, Protokolle, Ereignisüberwachung und tatsächliche Überwachungszeiten.
Reagieren — RS	Was tun wir bei einem Vorfall?	Eskalation, Entscheidungen, Begrenzung der Auswirkungen, Kommunikation und Beweissicherung.
Wiederherstellen — RC	Wie läuft der Betrieb wieder an?	Getestete Wiederherstellung, Wiederanlaufprioritäten und alternative Kanäle.

Die sechs Funktionen sind der Struktur der DNSC-Maßnahmen entnommen. Die Fragen sind unsere eigene Synthese, keine Reproduktion des Katalogs oder ein Ersatz für die Überprüfung aller anwendbaren Kontrollen. [R3]

Beispiele für den passenden Detailgrad

Für die Authentifizierung: „Ja, für IT-Administratoren; für alle anderen unbekannt.“ Für das Backup: „Wir haben Backups, aber wir wissen nicht, wann die Wiederherstellung zuletzt getestet wurde.“ Für eine Gruppe: „Sicherheit wird zentral verwaltet; die lokale verantwortliche Person kann ermitteln, wer die Abdeckung bestätigt.“

Keine ausnutzbaren Informationen oder Kundendaten senden

Geben Sie keine Passwörter, Tokens, Schlüssel, IP-Adressen, Konfigurationen, Benutzerlisten, Systemauszüge oder Schwachstellenberichte ein, sondern nur das Vorhandensein von Maßnahmen und die Rolle, die diese bestätigen können.

Spezielle Bereiche – Entwicklung, Cloud, Managed Services, OT/IoT/Medizin, Public Exposure und die physische Umgebung – werden gesondert geklärt. Für DORA und digitale Kategorien, die unter die Verordnung 2024/2690 fallen, wird die anwendbare Regelung überprüft, ohne dass die vollständige kumulative Anwendung der Verpflichtungen angenommen wird. [R6]

Mögliche Folgeleistungen

Der Vorschlag wird erstellt, nachdem der Anwendungsbereich und der ermittelte Bedarf verstanden wurden. Das Pre-Audit ist eine kommerzielle Vorbereitungsphase, keine separate universelle Verpflichtung. Ein Kunde muss möglicherweise direkt zu einem Audit übergehen oder muss nur bestimmte Beweise ausfüllen.

PHASE	DURCHGEFÜHRTE ARBEITEN	KONKRETES ERGEBNIS
P1 • Erstbewertung / Pre-Audit	Anwendbarkeit, Risiken, Dokumente und Umsetzung; Gespräche und autorisierte Prüfungen. Vorbereitung der Selbstbewertung nach geltendem Verfahren.	Lagebericht, Lücken, Nachweise und Unterstützung bei freizugebenden oder einzureichenden Dokumenten.
P2 • Unabhängiges Audit	Reguliertes Audit, das von einem unabhängigen DNSC-zertifizierten Auditor durchgeführt wird; Werkzeuge, Dokumente, Interviews und Tests im genehmigten Umfang.	Auditbericht und Feststellungen. Ein Scan allein ist kein Audit.
P3 • Plan und Budget	Risikobasierte Prioritäten, Behandlungsoptionen, Zuständige, Fristen, Abhängigkeiten und einmalige/laufende Kosten.	Freigegebener Plan und transparentes Budget; Vorbereitung der Einreichung, sofern erforderlich.
P4 • Umsetzung	Technische und organisatorische Lösungen, Konfiguration, Schulung, Abnahmetests und Nachweissammlung.	Umgesetzte und geprüfte Maßnahmen; dokumentierte Grenzen und Restrisiken.
P5 • Wartung und Berichterstattung	Überprüfungen und Wiederholungstests, Dokumentationspflege, Unterstützung bei Neubewertungen und nötigen Mitteilungen.	Aktuelle Nachweise und Managementberichte; Unterstützung beim Maßnahmenabschluss.

Inhalt des Angebots

Die Entitäten, Websites und Systeme enthalten; Dienstleistungen und Methoden; Anzahl der Interviews und Überprüfungen; Leistungen; Zugangsbeschränkungen; Annahmen; Verantwortlichkeiten der Kunden; anfängliche und wiederkehrende Kosten; Ausschlüsse; Akzeptanzkriterien; und Bedingungen für die Änderung des Umfangs.

Wir gehen von den bestehenden Maßnahmen aus. Je nach Risiko kann eine Anforderung durch Konfiguration, ein Verfahren, eine Schulung oder ein Produkt adressiert werden. Die Wahl einer Marke ist an sich keine Bedingung für die Einhaltung.

Klare Trennung der Leistungen

Der Kunde ist nicht verpflichtet, jede Stufe beim gleichen Anbieter zu kaufen. Die Durchführung und das unabhängige Audit haben unterschiedliche Funktionen. Lizenzen, Hardware und Sonderoperationen werden im Angebot gesondert festgelegt.

Ablauf der technischen Prüfung

Ein Tool kann bei der Bestandsaufnahme und bei der Überprüfung bestimmter Konfigurationen, Berechtigungen, Schwachstellen oder Protokolle entsprechend seinen tatsächlichen Fähigkeiten helfen. An sich kann sie weder die Governance noch die Risikoakzeptanz, die Anwendung jedes Verfahrens oder die vollständige Erfüllung der Anforderungen nachweisen.

Vor jedem Zugriff

PUNKT	SCHRIFTLICHE VEREINBARUNG
Umfang und Methode	Eingeschlossene/ausgeschlossene Systeme, Erfassungsverfahren, genehmigte Scans/Tests, Zeitfenster und Stoppregeln.
Zugriff und Änderungen	Mindestrechte; schreibgeschützter Zugriff, wenn die Methode dies zulässt; kontrollierte Konten nach der Arbeit widerrufen; Änderungen bedürfen einer gesonderten Genehmigung.
Daten und Vertraulichkeit	Erfasste Daten, Speicherort, Empfänger, Aufbewahrung und Löschung. Gegebenenfalls Vertraulichkeits- und Verarbeitungsvereinbarungen.
Dritte und sensible Systeme	Genehmigung von Eigentümern/Anbietern; eine sichere Methode und genehmigte Fenster für OT, medizinische und kritische Systeme; standardmäßig kein aktives Scannen.
Lieferung und Nachvollziehbarkeit	Tätigkeitsprotokoll, Feststellungen, einschlägige Nachweise, Werkzeugbeschränkungen und Angelegenheiten, die einer manuellen Überprüfung bedürfen.

Der Fragebogen erlaubt keine Scans

Die Auswahl von „Ich möchte einen Vorschlag oder die Rückgabe der Excel-Arbeitsmappe stellt keine Zustimmung zum Zugriff, zur Installation eines Agenten, zum Scannen des Systems oder zu Konfigurationsänderungen dar.“

Wer ist zuständig, wer prüft?

Das Management genehmigt und überwacht die Maßnahmen, stellt Ressourcen bereit und übernimmt die entsprechenden Verpflichtungen. Das Bewertungs-/Umsetzungsteam führt das vereinbarte Mandat aus. Der zertifizierte Wirtschaftsprüfer formuliert die Schlussfolgerungen der reglementierten Prüfung unabhängig. [R1–R2]

Die Unabhängigkeit wird auch dann überprüft, wenn der Prüfer und der ausführende Hersteller verschiedenen Unternehmen derselben Gruppe angehören: aktuelle und frühere Dienstleistungen, berufliche/finanzielle Beziehungen und die Unvereinbarkeiten nach Artikel 58 werden geprüft. Die bloße Existenz von zwei Unternehmen reicht nicht aus. [R2]

Wir versprechen keine „Genehmigung der Selbsteinschätzung durch einen Auditor und stellen das Tool nicht als NIS2-Zertifizierung vor. Rollen, Bescheinigungen und eventuelle Anerkennungen werden vor der Auftragsvergabe in der Praxis überprüft.

Von Befunden zu Umsetzung und Bericht

Ein sinnvoller Plan ist keine Produktliste. Jeder Befund wird mit einer Anforderung, einem Nachweis, dem Unternehmensrisiko und einem Kriterium für die Behebung verknüpft.

IM PLAN	WAS KLAR SEIN MUSS
Befund und Risiko	Was wurde überprüft, was die Lücke ist, welche Aktivität betroffen sein kann und warum sie eine besondere Priorität hat.
Optionen und Kosten	Mit bestehenden Lösungen Behebbares; Alternativen; einmalige und laufende Kosten sowie Schätzannahmen.
Verantwortliche und Frist	Interne Verantwortung, Umsetzung, Abhängigkeiten, nötige Ausfallzeit und vereinbarte Frist.
Abnahme und Nachweise	Durchzuführender Test, aufzubewahrende Nachweise, abnehmende Person und weiter zu behandelndes Restrisiko.
Kommunikation	Eingereichtes Dokument, Rechtsgrundlage und Frist, Freigabe der Leitung und Nachweis der Behördenmitteilung.

Der Zeitplan gilt je Rechtsträger

Die erste Checkliste und die 05_Fristen zeichnen die Meilensteine Registrierung, Entscheidung, Risikobewertung, Selbsteinschätzung, Plan und Audit auf. Die Frist für die Vorlage des Plans nach der Selbstbewertung ist getrennt von der Umsetzungsfrist und dem Weg für den Prüfplan. Die Artikel 12, 18 und 57 der Verordnung werden gesondert geprüft. [R2]

Compliance folgt nicht nur aus der Einreichung eines Dokuments. Die Unterstützung bei der Vorlage des Plans oder der Mitteilung des Abschlusses der Maßnahmen basiert auf einem Mandat, der tatsächlich geltenden Verpflichtung und den Nachweisen. Unvollständige Maßnahmen werden nicht für vollständig erklärt; Blocker und überarbeitete Fristen werden im geltenden Rahmen behandelt.

Vorfälle warten nicht auf das Projektende

Das Betriebsverfahren muss die Meldung signifikanter Vorfälle berücksichtigen: Warnung innerhalb von 24 Stunden und Benachrichtigung innerhalb von 72 Stunden nach Bekanntwerden, gefolgt von einem Abschlussbericht und etwaigen Aktualisierungen innerhalb der geltenden Fristen, vorbehaltlich der gesetzlichen Ausnahmen. [R1–R2]

Was Sie uns jetzt zurücksenden

Nur die ausgefüllte Excel-Arbeitsmappe mit den bekannten Informationen und den Personen/Rollen, die sie bestätigen können. Wir legen dann die Präzisierungen, den Anwendungsbereich und den Vorschlag fest. Belegdokumente und technischer Zugang werden später angefordert, über einen sicheren Kanal und innerhalb der vereinbarten Grenzen.

Grundlagen und Grenzen dieses Dokuments

Der vorliegende technische CSAT/CISv8-Fragebogen umfasst 63 Fragen zu 20 Themen. Sie wurden thematisch zu 44 Fragen auf Rumänisch zusammengefasst und um Bereiche des NIS2/DNSC-Rahmens ergänzt. Das interne Register enthält die Originalfragen, ihre Position in Excel und die erstellten Zuordnungen.

Die Stufen Basis, Standardisiert, Rationalisiert und Dynamisch, die Risikowerte und die kommerziellen Produktempfehlungen der Quelle wurden nicht in DNSC-Bewertungen, Budgets oder Kaufpflichten umgewandelt. Ein „Ja“ ist eine zu prüfende Aussage, kein Nachweis. Die Antwort „Möglicherweise nicht anwendbar“ begründet oder genehmigt für sich allein keinen rechtlichen Ausschluss.

Rechtliche Grundlagen

REF.	QUELLE UND VERWENDUNG
R1	Richtlinie (EU) 2022/2555: Artikel 20 (Management), Artikel 21 (Cybersecurity-Risikomanagement-Maßnahmen), Artikel 23 (Vorfälle). EUR-Lex: CELEX 32022L2555.
R2	Dringlichkeitsverordnung Nr. 155/2024, mit Änderungen durch Gesetz Nr. 124/2025 genehmigt, konsolidierte Fassung: Art. 11–15, 18, 57–58 und Anhänge. Rumänisches Gesetzgebungsportal: Dokument 293121.
R3	DNSC Order Nr. 1/2026, veröffentlicht am 27. August 2026, Anhänge zu den Maßnahmen und der Selbsteinschätzung. Rumänisches Legislativportal: Dokumente 314681 / 314360 / 314683.
R4	DNSC-Verordnung Nr. 2/2026: Änderungen zur Nichtanwendbarkeit und zu Gruppenkontrollen. Rumänisches Gesetzgebungsportal: Dokument 314676.
R5	DNSC-Beschluss Nr. 3/2026 und die Regeln für Gruppen: Antrag und lokale Beweise, Verantwortlichkeiten. rumänisches Gesetzgebungsportal: Dokumente 314698 / 314699.
R6	Verordnung (EU) 2022/2554 — DORA und Durchführungsverordnung (EU) 2024/2690, im jeweiligen Geltungsbereich. EUR-Lex: CELEX 32022R2554 / 32024R2690.

Die vollständigen Adressen und die Rolle der einzelnen Quellen finden sich im Blatt 08_Referenzen in Excel. Bezugsdatum des Pakets: 6. Oktober 2026. Die zum Zeitpunkt der Bewertung des Unternehmens geltenden Rechtsvorschriften und Verfahren müssen verwendet werden.

Begriffe in Kürze

MFA: Zugriffsbestätigung durch mehrere Faktoren. OT: Systeme zur Steuerung physischer Prozesse oder Geräte. Backup: Sicherungskopie; ihre Existenz belegt keine erfolgreiche Wiederherstellung. Nachweis: Dokument, Aufzeichnung oder Testergebnis, das eine Feststellung stützt. Restrisiko: das nach den Maßnahmen verbleibende Risiko.

Koordination Ihrer Anfrage

Cristian Apostol • office@clarified.ro • +40 774 456 127
it.clarified.ro/nis2