NIS2 IN DER PRAXIS:

Die Checkliste für auditfähige Prozesse

Mehr Sicherheit, mehr Struktur, mehr Nachweisfähigkeit

Die NIS2-Richtlinie erhöht die Anforderungen an Cybersecurity, Risikomanagement und Nachweisfähigkeit. Dabei geht es nicht nur um technische Schutzmaßnahmen, sondern auch um operative und organisatorische Prozesse, die nachvollziehbar dokumentiert werden müssen.

Genau hier liegt für viele Unternehmen die Herausforderung: Maßnahmen sind oft vorhanden, doch für tägliche Abläufe wie Melden, Prüfen, Freigeben und Nachverfolgen fehlen saubere, auditfähige Nachweise.

Diese Checkliste hilft, die eigene NIS2-Readyness schnell einzuordnen, Lücken sichtbar zu machen und konkrete nächste Schritte abzuleiten. Im Fokus stehen drei besonders relevante Prozesse für eine belastbare Umsetzung: Schulungen, Lieferantenmanagement und Berechtigungsmanagement.

So wird die Checkliste genutzt

Beantworten Sie jede Frage mit:

Ja,
wenn der Prozess klar geregelt, umgesetzt und nachvollziehbar dokumentiert ist.

Teilweise,
wenn es bereits Ansätze gibt, diese aber nicht vollständig, nicht einheitlich oder nicht durchgängig dokumentiert sind.

Nein,
wenn der Prozess fehlt, nicht geregelt ist oder keine belastbaren Nachweise vorhanden sind.

Nutze die NIS2-Checkliste auch digital als smap

Beantworte die Fragen direkt im Browser und prüfe deine Prozesse Schritt für Schritt. **Zur Online-NIS2-Checkliste**

Checklisten

1. Schulungen und Awareness-Nachweise

Ziel: Nachweisbare Sensibilisierung aller relevanten Personen sicherstellen.

Prüffrage	Ja	Teilweise	Nein
Ist definiert, welche Zielgruppen geschult werden müssen, z.B. alle Mitarbeitenden, Führungskräfte, Administratoren oder externe Nutzer?	◯	◯	◯
Gibt es einen verbindlichen Schulungsplan mit Intervallen, Fristen und Verantwortlichen?	◯	◯	◯
Sind Pflichtschulungen für neue Mitarbeitende fest im Onboarding verankert?	◯	◯	◯
Werden Awareness-Maßnahmen wie Phishing-Hinweise, Kurztrainings, Sicherheitsupdates oder interne Informationskampagnen dokumentiert?	◯	◯	◯
Werden Teilnahmebestätigungen, Testergebnisse oder Verständniserklärungen zentral gespeichert?	◯	◯	◯
Gibt es einen Prozess für überfällige Schulungen inklusive Reminder und Eskalation?	◯	◯	◯
Wird dokumentiert, welche Eskalation erfolgt ist und ob die Schulung anschließend abgeschlossen wurde?	◯	◯	◯
Ist dokumentiert, welche Inhalte vermittelt wurden und wann diese Inhalte zuletzt aktualisiert wurden?	◯	◯	◯
Werden externe Personen mit Systemzugang ebenfalls in die Awareness-Logik einbezogen?	◯	◯	◯
Können Reports erzeugt werden zu Schulungsquote, offenen Nachweisen und Risikobereichen?	◯	◯	◯
Können Schulungsnachweise bei Audits, Kundenanfragen oder internen Prüfungen schnell bereitgestellt werden?	◯	◯	◯
Ist für die Geschäftsleitung separat dokumentiert, dass relevante Schulungspflichten erfüllt wurden?	◯	◯	◯

2. Lieferanten, neue Tools und Dienstleister

Ziel: Externe Risiken, digitale Werkzeuge und Dienstleister nachvollziehbar prüfen, freigeben und überwachen.

Prüffrage	Ja	Teilweise	Nein
Gibt es einen klar benannten Owner für jedes Tool, jede Anwendung oder jeden Dienstleister?	◯	◯	◯
Wird vor Einführung die Kritikalität systematisch bewertet, z. B. anhand von Daten, Prozessen, Abhängigkeiten oder Zugriffsrechten?	◯	◯	◯
Gibt es einen definierten und einheitlichen Freigabeprozess für neue Tools und Dienstleister – fachlich, technisch und sicherheitsseitig?	◯	◯	◯
Ist klar geregelt, wer Freigaben erteilt und wer die finale Verantwortung trägt?	◯	◯	◯
Werden Sicherheitsnachweise und relevante Anforderungen strukturiert eingeholt und geprüft?	◯	◯	◯
Wird dokumentiert, welche Nachweise fehlen, abgelaufen oder erneut anzufordern sind?	◯	◯	◯
Sind Zugriffe, Rollen und Berechtigungen für das Tool oder den Dienstleister klar definiert?	◯	◯	◯
Werden technische Anbindungen, Datenflüsse und Schnittstellen geprüft und dokumentiert?	◯	◯	◯
Werden alle relevanten Unterlagen zentral und nachvollziehbar abgelegt?	◯	◯	◯
Gibt es regelmäßige Überprüfungen bestehender Tools und Dienstleister, z.B. Re-Assessments?	◯	◯	◯
Werden Re-Assessments automatisch oder verbindlich angestoßen?	◯	◯	◯
Ist der gesamte Lifecycle geregelt – von Einführung über Betrieb bis Offboarding?	◯	◯	◯
Wird der Abschluss des Offboardings inklusive Rechteentzug, Datenrückgabe oder Datenlöschung dokumentiert?	◯	◯	◯
Gibt es eine zentrale Übersicht über aktive, kritische, in Prüfung befindliche und außer Betrieb genommene Tools oder Dienstleister?	◯	◯	◯

3. Berechtigungsmanagement: Eintritt, Wechsel, Austritt

Ziel: Zugriffskontrolle nachvollziehbar, revisionssicher und fristgerecht gestalten.

Eintritt

Prüffrage	Ja	Teilweise	Nein
Sind nur die minimal erforderlichen Zugriffe vorgesehen?	◯	◯	◯
Gibt es eine Freigabe durch Fachbereich und IT- oder Systemverantwortliche?	◯	◯	◯
Ist dokumentiert, welche Systeme freigeschaltet wurden?	◯	◯	◯
Ist Multi-Faktor-Authentifizierung für relevante Systeme aktiviert oder zumindest geprüft?	◯	◯	◯
Wird die tatsächliche Einrichtung der freigegebenen Rechte bestätigt und dokumentiert?	◯	◯	◯
Gibt es einen Termin für einen ersten Review der vergebenen Rechte?	◯	◯	◯

Rollenwechsel

Prüffrage	Ja	Teilweise	Nein
Werden Altberechtigungen aktiv entzogen, statt nur neue Rechte hinzuzufügen?	◯	◯	◯
Wird bei einem Rollenwechsel systematisch geprüft, welche Rechte entfallen und welche neu benötigt werden?	◯	◯	◯
Werden privilegierte Rechte separat geprüft und freigegeben?	◯	◯	◯
Ist nachvollziehbar, wer die Änderung beantragt, geprüft und genehmigt hat?	◯	◯	◯
Wird nach der Änderung überprüft, ob die tatsächlichen Rechte dem neuen Rollenprofil entsprechen?	◯	◯	◯
Gibt es einen Nachweis, dass nicht mehr benötigte Rechte tatsächlich entzogen wurden?	◯	◯	◯

Austritt

Prüffrage	Ja	Teilweise	Nein
Werden alle Zugänge zum definierten Zeitpunkt vollständig gesperrt oder entzogen?	◯	◯	◯
Werden Konten in allen relevanten Systemen deaktiviert oder gelöscht?	◯	◯	◯
Wird sichergestellt, dass auch privilegierte Zugänge vollständig erfasst und entzogen werden, z.B. Admin-, VPN- oder SaaS-Zugänge?	◯	◯	◯
Wird bestätigt, dass keine aktiven Schattenzugänge oder Ausnahmen bestehen bleiben?	◯	◯	◯
Gibt es einen nachvollziehbaren Nachweis, dass das Offboarding vollständig und fristgerecht erfolgt ist?	◯	◯	◯
Wird das Offboarding durch Fachbereich, IT oder Systemverantwortliche final bestätigt?	◯	◯	◯

Auswertung NIS2-Readiness: Wo steht Ihr Unternehmen aktuell?

So funktioniert Ihre erste Selbsteinschätzung. Werten Sie jede der drei Checklisten separat aus.
Zählen Sie Ihre „Nein"-Antworten. Zwei „Teilweise" zählen hier als ein „Nein", denn im Audit gilt: Halb dokumentiert ist nicht dokumentiert. Ihre NIS2-Readiness können Sie dann der folgenden Einteilung entnehmen:

0 bis 2-mal NEIN

Ihre Prozesse sind bereits weitgehend strukturiert, nachvollziehbar und dokumentiert. Der Fokus liegt vor allem darauf, bestehende Abläufe weiter zu vereinheitlichen, Medienbrüche zu reduzieren und Reports schneller verfügbar zu machen.

3 bis 5-mal NEIN

Es bestehen bereits Prozesse und einzelne Nachweise. Diese sind jedoch noch nicht durchgängig geregelt, nicht einheitlich dokumentiert oder nicht zentral auswertbar.

Typisches Risiko:

Im Tagesgeschäft funktionieren die Abläufe möglicherweise, aber bei Audits, Kundenanfragen oder konkreten Nachweisanforderungen entstehen Lücken, Verzögerungen oder hoher Abstimmungsaufwand.

6-mal oder häufiger NEIN

Es besteht deutlicher Handlungsbedarf. Wichtige Prozesse sind noch nicht geregelt oder nicht ausreichend dokumentiert.

Typisches Risiko:

Audit Probleme durch fehlende Nachweise, unklare Verantwortlichkeiten, uneinheitliche Abläufe und mögliche Sicherheits- oder Compliance-Lücken.

Ihr 5-Schritte-Fahrplan für die nächsten 30 Tage

1. Kritische Prozesse priorisieren

Wählen Sie 2–3 Prozesse, die folgende Kriterien erfüllen:

- Regelmäßigkeit: Mindestens monatlich durchgeführt
- Mehrere Beteiligte: Abteilungsübergreifend oder mit externen Partnern
- Nachweispflicht: Dokumentation für Audits, Zertifizierungen oder gesetzliche Vorgaben erforderlich (z.B. Berechtigungen, Schulungen oder Lieferanten)

2. Verantwortlichkeiten klar festlegen

Definieren Sie für jeden Prozess drei Rollen:

Rolle	Aufgabe	Beispiel
Prozessverantwortlicher	Gesamtverantwortung, Eskalation	Teamleiter IT
Durchführender	Operative Umsetzung	Sachbearbeiter
Freigebender	Finale Prüfung und Genehmigung	Abteilungsleiter

3. Einheitliche Regeln für den Ablauf festlegen

Erstellen Sie für jeden Prozess eine Checkliste mit maximal 10 Schritten, die folgende Fragen beantwortet:

- Wer startet den Prozess?
- Welche Informationen müssen vorliegen?
- Welche Schritte folgen in welcher Reihenfolge?
- Welche Dokumente entstehen dabei?
- Wann gilt der Prozess als abgeschlossen?

4. Nachweise zentral bündeln

Legen Sie einen festen Ablageort fest, an dem alle Nachweise dokumentiert werden.
Stellen Sie sicher, dass jeder Beteiligte weiß, wo und wie dokumentiert wird.

5. Einen festen Review-Termin setzen

Tragen Sie jetzt einen Termin in 4 Wochen in Ihren Kalender ein:

Leitfragen:

- Wurde der Prozess wie definiert durchgeführt?
- Wo gab es Abweichungen oder Probleme?
- Was kann vereinfacht oder verbessert werden?

Dokumentieren Sie die Ergebnisse und passen Sie die Prozessbeschreibung bei Bedarf an.

smapOne

Von einzelnen Maßnahmen zu auditfähigen Prozessen

NIS2 zeigt: Cybersecurity muss nicht nur technisch umgesetzt, sondern auch organisatorisch nachweisbar gemacht werden. Genau hier können strukturierte, digitale Workflows unterstützen. Sie helfen dabei, Prozesse klar zu führen, Verantwortlichkeiten sichtbar zu machen und relevante Nachweise auditfähig bereitzustellen.

Mit smapOne lassen sich solche Workflows einfach per No Code umsetzen, zum Beispiel für Schulungsnachweise, Freigaben, Berechtigungsprozesse, Incident-Meldungen oder Maßnahmenverfolgung. So werden manuelle Abläufe schnell digital strukturiert, ohne zusätzliche Komplexität im Alltag.

WE ENABLE SMARTER WORK

Nutze die NIS2-Checkliste auch digital als smap

Beantworte die Fragen direkt im Browser und prüfe deine Prozesse Schritt für Schritt.

Zur Online-NIS2-Checkliste

Jetzt smapOne kostenlos testen

Prüfen Sie, welche Ihrer NIS2-relevanten Prozesse heute noch manuell, uneinheitlich oder schwer nachweisbar ablaufen.
Mit einem Testaccount können Sie smapOne 14 Tage uneingeschränkt testen. Einfach mit der geschäftlichen E-Mail-Adresse registrieren. Eine automatische Verlängerung erfolgt nicht.