

[Startseite](#) / [NIS2/KSC-Audit](#) / [NIS2-Checkliste](#)

NIS2/KSC · CHECKLISTE

NIS2-Checkliste zum polnischen KSC-Gesetz: 40 Fragen vor dem Audit

Diese NIS2-Checkliste zur Selbsteinschätzung richtet sich an Teams, die ihre Organisation auf die Anforderungen des polnischen Gesetzes über das nationale Cybersicherheitssystem (KSC-Gesetz) vorbereiten: 40 Fragen in sechs Bereichen, jede mit der zugehörigen Vorschrift. Haken Sie erfüllte Punkte direkt am Bildschirm ab, drucken Sie die Liste aus oder speichern Sie sie als PDF - ohne Angabe einer E-Mail-Adresse.

Checkliste: innovix.pl/de/nis2/checkliste/ · Innovix sp. z o.o., Aleja Ślaska 1, 54-118 Wrocław, Polen · audyty@innovix.pl · [+48 575 621 877](tel:+48575621877)

Die Fragen folgen der Reihenfolge, in der sich Organisationen üblicherweise vorbereiten: zuerst Status und Eintragung in das Verzeichnis, dann die Verantwortung der Leitung der Einrichtung, das Informationssicherheits-Managementsystem, erhebliche Sicherheitsvorfälle, die Dokumentation und zum Schluss das Audit. Jedes „Nein“ und jedes „Weiß nicht“ ist ein Punkt für den Umsetzungsplan - Einrichtungen, die die Voraussetzungen bereits am Tag des Inkrafttretens der Novelle erfüllten, haben für die Umsetzung Zeit bis zum 3. April 2027.

Die Checkliste gilt für wesentliche Einrichtungen (im deutschen BSI-Gesetz: besonders wichtige Einrichtungen) und wichtige Einrichtungen nach dem

polnischen KSC-Gesetz, also für Organisationen, die in Polen tätig sind; für Gesellschaften in Deutschland gilt das BStG. Sie wissen noch nicht, ob das Gesetz Ihre Organisation erfasst? Beginnen Sie mit der NIS2-Betroffenheitsprüfung. Fragen zur Checkliste besprechen wir gern mit Ihnen – auf Englisch oder Polnisch.

Status und Eintragung in das Verzeichnis

Ausgangspunkt: ob und wie das Gesetz die Organisation erfasst.

1. ☐ Haben Sie den Status der Organisation ermittelt (wesentliche oder wichtige Einrichtung oder nicht vom Gesetz erfasst) und die Begründung dokumentiert: Sektor, Art der Einrichtung und Größe einschließlich verbundener Unternehmen und Partnerunternehmen? (Art. 5)
2. ☐ Wissen Sie, welche Behörde für Ihren Sektor zuständig ist und an welches CSIRT Sicherheitsvorfälle gemeldet werden? (Art. 41 und 41a; Art. 44 des Änderungsgesetzes)
3. ☐ Haben Sie den Antrag auf Eintragung in das Verzeichnis im System S46 gestellt oder Ihre Angaben nach Aufforderung durch den Minister für Digitalisierung ergänzt? (Art. 7c Abs. 1, Art. 7b Abs. 2)
4. ☐ Sind die Angaben im Verzeichnis aktuell, und melden Sie Änderungen innerhalb von 14 Tagen? (Art. 7c Abs. 3)
5. ☐ Nutzt die Organisation das System S46, und hat sie einen Kontoadministrator benannt? (Art. 9 Abs. 1 Nr. 4, Art. 7 Abs. 2 Nr. 11)

Leitung und Organisation

Für die Pflichten ist die Leitung der Einrichtung verantwortlich – auch dann,

wenn sie diese anderen Personen übertragen hat.

- 6. ☐ Hat die Leitung der Einrichtung Entscheidungen über Vorbereitung, Umsetzung, Überprüfung und Überwachung des Informationssicherheits-Managementsystems getroffen? (Art. 8c, Art. 8d Nr. 1)
- 7. ☐ Sind angemessene finanzielle Mittel für die Cybersicherheit eingeplant? (Art. 8d Nr. 2)
- 8. ☐ Haben die Leitung und die Person, der sie Cybersicherheitspflichten übertragen hat, in diesem Kalenderjahr eine dokumentierte Schulung absolviert? (Art. 8e)
- 9. ☐ Sind die Aufgaben zugewiesen - einer internen Struktur oder auf Grundlage eines Vertrags einem Anbieter verwalteter Sicherheitsdienste? (Art. 14)
- 10. ☐ Haben die Personen, die Aufgaben nach Art. 8 und 11 wahrnehmen, vor Arbeitsbeginn eine Auskunft aus dem polnischen Strafregister (KRK) vorgelegt? (Art. 8f)

Informationssicherheits-Managementsystem

Anforderungen nach Art. 8 Abs. 1 - für Einrichtungen, die beim Inkrafttreten der Novelle bereits erfasst waren, bis zum 3. April 2027.

- 11. ☐ Wird das Risiko eines Sicherheitsvorfalls systematisch nach einer dokumentierten Methode bewertet und gesteuert? (Art. 8 Abs. 1 Nr. 1)
- 12. ☐ Haben Sie Sicherheitsrichtlinien für das Informationssystem und themenspezifische Richtlinien, die von der Leitung beschlossen wurden? (Art. 8 Abs. 1 Nr. 2 Buchst. a)

- 13. ☐ Wird die Sicherheit bei Erwerb, Entwicklung, Wartung und Betrieb der Systeme berücksichtigt, und werden die Systeme getestet – z. B. mit Penetrationstests? (Art. 8 Abs. 1 Nr. 2 Buchst. b)
- 14. ☐ Umfassen Zutrittskontrolle und umgebungsbezogene Schutzmaßnahmen auch Serverräume und andere Orte der Datenverarbeitung? (Art. 8 Abs. 1 Nr. 2 Buchst. c)
- 15. ☐ Werden bei Einstellung, Rollenwechsel und Ausscheiden von Beschäftigten Berechtigungen vergeben und entzogen? (Art. 8 Abs. 1 Nr. 2 Buchst. d)
- 16. ☐ Bewerten Sie die Sicherheit Ihrer Lieferanten von IKT-Produkten, – Diensten und –Prozessen, und enthalten Ihre Verträge Sicherheitsanforderungen? (Art. 8 Abs. 1 Nr. 2 Buchst. e, Abs. 2)
- 17. ☐ Sind Pläne zur Aufrechterhaltung des Betriebs, Notfallpläne und Wiederherstellungspläne umgesetzt, dokumentiert und getestet? (Art. 8 Abs. 1 Nr. 2 Buchst. f)
- 18. ☐ Sind Datensicherungen von den Produktivsystemen getrennt, und wird die Wiederherstellung daraus regelmäßig getestet? (Art. 8 Abs. 1 Nr. 2 Buchst. f; Anhang 4, Teil I Nr. 10-11)
- 19. ☐ Wird das Informationssystem kontinuierlich überwacht? (Art. 8 Abs. 1 Nr. 2 Buchst. g)
- 20. ☐ Haben Sie Verfahren zur Bewertung der Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen? (Art. 8 Abs. 1 Nr. 2 Buchst. h)
- 21. ☐ Wird das Personal zur Cybersicherheit geschult, und sind die Grundregeln der Cyberhygiene bekannt und in der Praxis umgesetzt? (Art. 8 Abs. 1 Nr. 2 Buchst. i-j)

22. ☐ Haben Sie Regeln für den Einsatz von Kryptografie, einschließlich Verschlüsselung? (Art. 8 Abs. 1 Nr. 2 Buchst. k)
23. ☐ Setzen Sie, wo dies angemessen ist, Multi-Faktor-Authentifizierung und gesicherte Kommunikationsmittel ein? (Art. 8 Abs. 1 Nr. 2 Buchst. l)
24. ☐ Haben Sie eine aktuelle Bestandsaufnahme der Assets und eine Zugriffskontrollrichtlinie nach dem Prinzip der geringsten Berechtigungen? (Art. 8 Abs. 1 Nr. 2 Buchst. m-n)
25. ☐ Sammeln Sie Informationen über Cyberbedrohungen und Schwachstellen - z. B. Warnmeldungen von CSIRTs und Softwareherstellern? (Art. 8 Abs. 1 Nr. 3)
26. ☐ Wird die Software regelmäßig und mit einer Analyse der Auswirkungen aktualisiert, und werden erkannte Schwachstellen unverzüglich behoben? (Art. 8 Abs. 1 Nr. 5 Buchst. b und d)
27. ☐ Schützen Sie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten, auch vor unbefugter Veränderung? (Art. 8 Abs. 1 Nr. 5 Buchst. a und c)
28. ☐ Wenn Sie Anbieter digitaler Infrastruktur oder Dienste sind (z. B. Cloud, Rechenzentrum, verwaltete Dienste): Umfasst Ihr Managementsystem die Maßnahmen aus der Durchführungsverordnung (EU) 2024/2690 der Kommission? (Art. 8b Abs. 1)
29. ☐ Wenn Sie eine wichtige Einrichtung und zugleich eine öffentliche Stelle sind: Erfüllt Ihr Managementsystem die Anforderungen aus Anhang 4 des Gesetzes, und wird es mindestens einmal jährlich überprüft? (Art. 8 Abs. 3; Anhang 4, Teil III)

Sicherheitsvorfälle

Meldungen über das System S46 mit Fristen von 24 und 72 Stunden sowie einem Monat.

30. ☐ Haben Sie ein Verfahren zur Bewältigung von Sicherheitsvorfällen: Erkennung, Erfassung, Einstufung und Behandlung? (Art. 8 Abs. 1 Nr. 4, Art. 11)
31. ☐ Wissen Sie, wann ein Sicherheitsvorfall erheblich ist - nach den Schwellenwerten der polnischen Verordnung, bei Anbietern digitaler Infrastruktur oder Dienste nach der Durchführungsverordnung (EU) 2024/2690? (Art. 2 Nr. 7, Art. 11 Abs. 4)
32. ☐ Können Sie einen erheblichen Sicherheitsvorfall über S46 melden: Frühwarnung innerhalb von 24 Stunden, Meldung innerhalb von 72 Stunden, Abschlussbericht innerhalb von einem Monat? (Art. 11 Abs. 1 Nr. 4-4c)
33. ☐ Haben die Nutzer Ihrer Dienste Zugang zu Informationen über Cyberbedrohungen und einen Kanal für die Meldung von Sicherheitsvorfällen und Schwachstellen? (Art. 9 Abs. 1 Nr. 2-3)
34. ☐ Sieht das Verfahren vor, dass die Nutzer über erhebliche Cyberbedrohungen und Sicherheitsvorfälle informiert werden, die sich auf den Dienst auswirken? (Art. 11 Abs. 2a-2b)

Dokumentation und Kontakte

Nachweise, dass das System funktioniert - für Audit und Aufsicht.

35. ☐ Haben Sie eine normative und operative Dokumentation (Vorgaben und Nachweise, einschließlich Logs) mit Versionskontrolle, die mindestens 2 Jahre nach dem Ende ihrer Nutzung aufbewahrt wird? (Art. 10)

36. ☐ Haben Sie Personen für den Kontakt mit den Stellen des nationalen Cybersicherheitssystems benannt (mindestens zwei; in Kleinst- und kleinen Unternehmen sowie in wichtigen Einrichtungen, die öffentliche Stellen sind, eine)? (Art. 9 Abs. 1-3)
37. ☐ Können Sie der Behörde bei einer Aufsichtsmaßnahme Dokumente und Nachweise (Aufzeichnungen, Testberichte, Register der Sicherheitsvorfälle) auf Verlangen schnell übermitteln? (Art. 53c)

Sicherheitsaudit (wesentliche Einrichtungen)

Eine wichtige Einrichtung durchläuft ein Audit nur auf Anordnung der Behörde - auch dann helfen Ihnen diese Fragen.

38. ☐ Haben Sie das erste Sicherheitsaudit (bis zum 3. April 2028 für Einrichtungen, die seit dem Inkrafttreten der Novelle wesentliche Einrichtungen sind) und die folgenden Audits - mindestens alle 3 Jahre - geplant? (Art. 15 Abs. 1, Art. 33 Abs. 2 des Änderungsgesetzes)
39. ☐ Erfüllt der Auditor die Anforderungen des Gesetzes (akkreditierte Stelle oder mindestens zwei Auditoren mit Zertifikaten oder Auditerfahrung), und ist er unabhängig - hat er in Ihrer Einrichtung innerhalb eines Jahres vor dem Audit keine Aufgaben nach Art. 8-13 wahrgenommen? (Art. 15 Abs. 2-2a)
40. ☐ Wissen Sie, dass eine Kopie des Auditberichts innerhalb von 3 Arbeitstagen nach Erhalt an die zuständige Behörde zu übermitteln ist? (Art. 15 Abs. 1a)



DIE CHECKLISTE IST KEINE RECHTSBERATUNG

Die Fragen fassen die Pflichten aus dem Gesetz über das nationale Cybersicherheitssystem in der Fassung der Novelle zusammen. Sie ersetzen

weder eine rechtliche Analyse noch die Bewertung, ob die Maßnahmen dem Risiko angemessen sind - diese liefert die NIS2-Gap-Analyse.
 Rechtsstand: 8. Oktober 2026 · Quelle: Gesetz vom 23. Januar 2026 zur Änderung des Gesetzes über das nationale Cybersicherheitssystem und einiger anderer Gesetze (Dz.U. 2026 Pos. 252) (auf Polnisch)

Häufig gestellte Fragen

Ersetzt die Checkliste die Gap-Analyse oder das Audit nach Art. 15?



Gilt die Checkliste auch für wichtige Einrichtungen?



Woher weiß ich, ob meine Organisation überhaupt unter das Gesetz fällt?



Quellen

Gesetz vom 23. Januar 2026 zur Änderung des Gesetzes über das nationale Cybersicherheitssystem und einiger anderer Gesetze (Dz.U. 2026 Pos. 252) (auf Polnisch)
 (8. Oktober 2026)

Gesetz über das nationale Cybersicherheitssystem - Metadaten des Rechtsakts und Änderungsakte (ELI-API des Sejm) (auf Polnisch) (8. Oktober 2026)

Ministerium für Digitalisierung - Q&A zur Novelle des KSC-Gesetzes, Aktualisierung Oktober 2026 (01.10.2026; Erläuterungsdokument, nicht rechtsverbindlich) (auf Polnisch)
 (8. Oktober 2026)

Durchführungsverordnung (EU) 2024/2690 der Kommission - technische und methodische Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit (6. Oktober 2026)

Rechtsstand: 8. Oktober 2026 · Aktualisiert am 8. Oktober 2026

