ÆNIX

NIS2-Compliance-Readiness-Checkliste

35 architektonische Kontrollpunkte, um zu prüfen, ob Ihre Cloud-Plattform die von der Richtlinie (EU) 2022/2555 geforderten Risikomanagementmaßnahmen für Cybersicherheit trägt.

Für CISOs, Security- & Compliance-Verantwortliche · aenix.io

35 architektonische Kontrollpunkte für wesentliche und wichtige Einrichtungen. Ausgerichtet auf die Richtlinie (EU) 2022/2555. Umsetzungsfrist der Mitgliedstaaten: 17. Oktober 2024. v1.1 — September 2026.

So verwenden Sie diese Checkliste

Die Richtlinie über Netz- und Informationssicherheit 2 (NIS2, Richtlinie (EU) 2022/2555) erweitert Geltungsbereich und Strenge der EU-Cybersicherheitspflichten erheblich. Die Mitgliedstaaten haben sie zum 17. Oktober 2024 in nationales Recht umgesetzt (einige finalisieren die sektorspezifische Umsetzung noch). NIS2 erfasst wesentliche Einrichtungen (Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung, Weltraum) und wichtige Einrichtungen (Post- und Kurierdienste, Abfallwirtschaft, Herstellung kritischer Produkte, Lebensmittelvertrieb, Herstellung bestimmter digitaler Dienste, Forschung).

Diese 35-Punkte-Checkliste bietet CISOs, Compliance-Verantwortlichen und Platform-Engineering-Managern eine strukturierte Möglichkeit zu beurteilen, ob ihre Architektur die geforderten Risikomanagementmaßnahmen für Cybersicherheit trägt, wie sie in Art. 21 Art. 23 und angrenzenden Bestimmungen verankert sind.

Nutzen Sie sie auf drei Arten:

1. **Selbstbewertung** — gemeinsam mit Security-, Platform-Engineering- und Compliance-Teams durchgehen.
2. **Vorbereitung des Behördendialogs** — die Abschnittszusammenfassungen lassen sich direkt in eine Kontrollnarrative für ein nationales CSIRT oder die zuständige Behörde überführen.
3. **Lieferanten-Scoping** — an IKT-Drittanbieter (insbesondere Anbieter von IKT-Dienstverwaltung) weitergeben, damit diese anhand derselben Angriffsfläche antworten.

> Diese Checkliste ist eine Hilfe zur architektonischen Bereitschaft, keine Rechtsberatung. Die NIS2-Konformität ist durch Ihre Rechtsberatung zu bestätigen und gegen die nationale Umsetzung in jedem Mitgliedstaat zu validieren, in dem Sie in den Anwendungsbereich fallen. Sektorale Lex specialis (DORA für Finanzunternehmen, eIDAS für Vertrauensdienste) kann in bestimmten Bereichen Vorrang haben.

Abschnittsübersicht:

ABSCHNITT	SCHWERPUNKT	PUNKTE
1	Risikomanagement Art. 21	10
2	Incident-Handling & Meldung Art. 23	6
3	Geschäftskontinuität & Schwachstellenmanagement	7
4	Lieferkette & Kryptografie	6
5	Zugriffskontrolle & Audit	6

1. Risikomanagement Art. 21

Artikel 21 zählt die Risikomanagementmaßnahmen für Cybersicherheit auf, die wesentliche und wichtige Einrichtungen umsetzen müssen. Es handelt sich um strukturelle Kontrollen — sie müssen nachgewiesen und nicht nur behauptet werden.

- [ ] **Risikoregister je kritischem Workload dokumentiert** — inventarisiert, mit Verantwortlichkeit, regelmäßig geprüft. Art. 21(2)(a)
- [ ] **Jährliche Cybersicherheits-Risikoprüfung** — durchgeführt und vom Leitungsorgan gezeichnet. Art. 21(2)(a)
- [ ] **IKT-Asset-Register vollständig und aktuell** — sämtliche Hardware, Software, Daten und Abhängigkeiten erfasst. Art. 21(2)(i)
- [ ] **Bedrohungsmodell je kritischem Workload dokumentiert** — bei wesentlichen architektonischen Änderungen aktualisiert. Art. 21(2)(a)
- [ ] **Cybersicherheitsrichtlinie vom Leitungsorgan genehmigt** — dokumentiert, jährlich aktualisiert. Art. 20
- [ ] **Netzwerksegmentierung / Zero-Trust-Durchsetzung** — Mikrosegmentierung zwischen Vertrauenszonen; Default-Deny-Haltung. Art. 21(2)(a)
- [ ] **Pod Security Standards / NetworkPolicies durchgesetzt (Kubernetes)** — sofern Kubernetes im Einsatz ist, oder gleichwertige Isolationsprimitive auf anderen Substraten. Art. 21(2)(a)
- [ ] **Wirksamkeitsprüfung der Kontrollen — vierteljährlich** — dokumentierte Nachweise aufbewahrt. Art. 21(2)(f)
- [ ] **Verpflichtende Cybersicherheitsschulung für alle Mitarbeitenden** — einschließlich der oberen Leitungsebene; Abschluss nachverfolgt. Art. 21(2)(g) Art. 20
- [ ] **Risikoregister jährlich durch Audit geprüft** — interne oder externe Prüfung; Feststellungen bis zur Behebung nachverfolgt. Art. 21(2)(f)

> Artikel 20 begründet eine unmittelbare Verantwortlichkeit der Leitungsorgane für die Genehmigung der Cybersicherheitsmaßnahmen und die Überwachung ihrer Umsetzung. „Das Risiko liegt bei der IT“ ist keine haltbare Position mehr.

2. Incident-Handling & Meldung Art. 23

NIS2 führt enge Meldefristen ein — Frühwarnung innerhalb von 24 Stunden, Meldung des Vorfalls innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats.

- [ ] **24×7-Erkennungsfähigkeit für kritische Workloads** — abgestimmt auf die für die Meldung verwendete Schweregradklassifizierung. Art. 23
- [ ] **Dokumentierte Incident Response mit benannten Rollen** — IR-Plan mit Rufbereitschaft, Eskalationspfaden, Entscheidungsbefugnis und Kommunikations-Playbook.
- [ ] **Prozess zur Vorfallklassifizierung dokumentiert** — Schwellenwerte für „erheblich“ vs. nicht erheblich explizit definiert.

- [ ] **Vorab eingerichtete Kommunikationskanäle zu CSIRT / zuständiger Behörde** — benannte Ansprechpartner, sichere Kanäle, Probeübung durchgeführt.
- [ ] **Meldevorlagen für 24-Stunden / 72-Stunden / 1-Monat** — Vorlagen getestet, Verantwortliche zugewiesen. Art. 23(4)
- [ ] **Jährliche Incident-Response-Übung** — Tabletop oder live; Ergebnisse aufbewahrt.

> Die Frühwarnung binnen 24 Stunden ist bewusst kurz — sie erfordert einen Prozess, in dem die Rufbereitschaft der Security sehr schnell die Entscheidung „melden oder nicht“ treffen kann. Verankern Sie das Entscheidungsraster im IR-Plan, nicht erst im Vorfall.

3. Geschäftskontinuität & Schwachstellenmanagement

- [ ] **BCP-Plan je kritischem Workload** — dokumentiert, mit Verantwortlichkeit, geprüft. Art. 21(2)(c)
- [ ] **RTO / RPO dokumentiert und jährlich getestet** — mit Testnachweis, nicht nur einem Plan. Art. 21(2)(c)
- [ ] **Backup-Wiederherstellung in den letzten 12 Monaten getestet** — erfolgreiche Wiederherstellung aus einem Produktions-Backup in eine saubere Umgebung.
- [ ] **DR-Standort betriebsbereit und getestet** — Failover in den letzten 12 Monaten für kritische Workloads geübt.
- [ ] **SLA für CVE-Reaktion dokumentiert** — Triage- / Patch- / Verifikationsfenster nach Schweregrad. Art. 21(2)(e)
- [ ] **SAST / DAST in der CI; Container-Scanning + SBOM** — Sicherheits-Gates zur Build-Zeit; Provenienz der Abhängigkeiten nachverfolgt.
- [ ] **Richtlinie zur koordinierten Offenlegung von Schwachstellen veröffentlicht** — Eingangskanal, Triage-Zusage, Anerkennung. Art. 12

> Für Container-Workloads sollte „SBOM“ ein generiertes, signiertes und aufbewahrtes Artefakt bedeuten (z. B. im Format SPDX oder CycloneDX) — keine manuelle Tabelle. Verwenden Sie Sigstore / Cosign oder Gleichwertiges für die Signatur.

4. Lieferkette & Kryptografie

NIS2 legt ausdrückliches Gewicht auf das Lieferkettenrisiko Art. 21(2)(d) und auf Kryptografie und Verschlüsselung Art. 21(2)(h).

- [ ] **Inventar der IKT-Drittanbieter vollständig** — alle IKT-Anbieter, einschließlich mittelbarer (unterbeauftragter). Art. 21(2)(d)
- [ ] **Abhängigkeiten kritischer Funktionen bis zur zweiten Ebene abgebildet** — Unterauftragnehmer der Lieferanten, sofern sie kritische Funktionen erbringen.
- [ ] **Vertragsinhalte gemäß Artikel 21(2)(d) in Verträgen zu kritischen Funktionen** — einschließlich Bestimmungen zur koordinierten Offenlegung von Schwachstellen und zur Vorfallkommunikation. Art. 21(2)(d)

- [ ] **Laufende Lieferantenüberwachung dokumentiert** — mindestens jährliche Prüfung; anlassbezogen bei Vorfall oder M&A-Auslöser.
- [ ] **Verschlüsselung im Ruhezustand, bei der Übertragung und (soweit anwendbar) in Verwendung** — mit dokumentierter Chiffrenwahl und Rotation. Art. 21(2)(h)
- [ ] **Kundenkontrollierte Verschlüsselungsschlüssel, soweit anwendbar** — für Tier-1- / sensible Workloads. Schlüsselverwahrungsprozess dokumentiert.

> „Lieferkette bis zur zweiten Ebene“ klingt aufwendig, geht aber vor allem um Kennen, nicht um Kontrollieren. Das Register offenbart häufig eine Konzentration auf denselben zugrunde liegenden Anbieter über verschiedene Zwischenhändler — eine wertvolle Erkenntnis, unabhängig vom NIS2-Bezug.

5. Zugriffskontrolle & Audit

NIS2 erwartet MFA, Privileged-Access-Management und Audit-Vollständigkeit als Basiskontrollen — nicht als fortgeschrittene.

- [ ] **MFA für privilegierte Konten (durchgängig)** — alle Admin- / Break-Glass- / IAM-Konten; ohne Ausnahmen. Art. 21(2)(j)
- [ ] **MFA für Endnutzerzugriff, wo angemessen** — risikobasiert für nicht privilegierten Zugriff.
- [ ] **Privileged-Access-Management eingeführt** — Just-in-Time-Erhöhung, Sitzungsaufzeichnung, Tresor für geteilte Zugangsdaten.
- [ ] **Joiner-Mover-Leaver automatisiert** — Identitätslebenszyklus vom HR-System bis zu allen betroffenen Systemen; Entzug des Zugriffs verifiziert.
- [ ] **Aufbewahrung der Audit-Logs erfüllt die längste anwendbare Anforderung** — oft 5+ Jahre bei sektoralen oder nationalen Vorgaben; manipulationssichere Speicherung.
- [ ] **Prozess für Behördenzugriff dokumentiert und getestet** — Verfahren zur Gewährung des Zugriffs für ein nationales CSIRT oder die zuständige Behörde; Probeübung durchgeführt.

> Viele Organisationen haben MFA an der SSO-Oberfläche, aber nicht bei Root-Konten der Cloud-Anbieter, bei Admin-Konsolen von SaaS-Drittanbietern oder bei alten Break-Glass-Pfaden. Prüfen Sie umfassend — nicht nur die Haustür.

Empfehlungen auf Architekturebene

Für die meisten NIS2-Kontrollen ist die Architektur die wirkungsvollste Abhilfefläche. Trägt die zugrunde liegende Plattform strukturell Mandantenisolierung, kundenkontrollierte Verschlüsselung, einen unveränderlichen Audit-Trail, kontrollierten Lieferantenzugriff sowie getestete Exit-/Restore-Mechaniken, so werden viele der 35 Kontrollpunkte zur Folge des Designs statt zu separaten Compliance-Projekten.

Wenn die Architektur NIS2-Lücken strukturell schließt

- Tenant-CRD-Mandantenfähigkeit adressiert Art. 21(2)(a) Netzwerksegmentierung und Isolierung zwischen Vertrauenszonen.
- Kundenkontrollierte Verschlüsselung auf Plattform-, Speicher- und Observability-Ebene adressiert Art. 21(2)(h).
- Air-Gap-Unterstützung adressiert Anforderungen an souveräne / regulatorisch isolierte Workloads, wenn nationales Recht über die NIS2-Grundlinie hinausgeht.
- Vollständigkeit des Audit-Trails (anbieterseitig über VictoriaLogs, kundenseitig per Export) adressiert Art. 21(2)(i) und die Erwartungen an den Behördenzugriff.
- Getestete Exit- und Restore-Mechaniken adressieren Art. 21(2)(c) BCP und die Lieferanten-Exit-Erwartungen aus Art. 21(2)(d).

Wenn die bestehende Architektur nachgerüstet werden kann

- Viele Kontrollen (durchgängige MFA, CVE-SLA, CVD-Richtlinie, Schulung, Kadenz des Risikoregisters, JML-Automatisierung) sind organisatorische und werkzeugseitige Ergänzungen, die keinen Plattformwechsel erfordern.
- Netzwerksegmentierung und Mikrosegmentierung lassen sich auf Kubernetes-basierten Plattformen meist über NetworkPolicy / Cilium-Policy ohne architektonischen Umbau nachrüsten.
- BCP / DR und die Kadenz der Backup-Tests sind Prozessdisziplin — keine Plattformänderung nötig.

Wenn eine Teil-Nachrüstung wirklich nicht ausreicht

- Auf VMware Cloud Director basierende Plattformen tun sich mit Portabilität (Art. 21(2)(d) Lieferanten-Exit) und kundenkontrollierten Schlüsseln auf jeder Ebene schwer.
- Ausschließlich anbieterverwaltete Verschlüsselung, insbesondere für Backups und Observability, scheitert an Art. 21(2)(h), wo die Prüfung durch die Regulierungsbehörde hoch ist.
- Geteilte Multi-Tenant-SaaS-Infrastruktur tut sich mit den Erwartungen an die Vollständigkeit des Audit-Trails unter behördlicher Prüfung schwer.

> Die kosteneffizienteste Reihenfolge zur Lückenschließung ist meist: (1) durchgängige MFA + JML, (2) Backup-Test + DR-Test, (3) CVE-SLA + SBOM, (4) Lieferantenregister + Vertragsaktualisierung, (5) architektonische Änderungen dort, wo die Schritte 1–4 die Lücke nicht schließen können.

NIS2-konforme Cloud-Architektur — Referenzmuster

Eine Plattform, die um Isolierung, kundenkontrollierte Kryptografie und unveränderliche Nachvollziehbarkeit herum gebaut ist, kann die meisten Artikel-21-Kontrollen auf Plattformebene schließen, statt als 35 kompensierende Verfahren. Das folgende Referenzmuster stapelt drei Ebenen.

Mandantenebene

Voneinander isolierte Mandanten nebeneinander — zum Beispiel ein Produktionsmandant, ein audit-isolierter Mandant, ein Mandant für souveräne Workloads und ein Testmandant. Jeder trägt eigene Verschlüsselungsschlüssel, einen eigenen Audit-Log-Stream und MFA-geschützten Zugriff.

Plattform-Steuerungsebene

Eine einzige Kubernetes-native Steuerungsebene mit Tenant-CRD, Identität (OIDC), NetworkPolicy- / Cilium-Segmentierung, Verschlüsselung (BYOK / HYOK), einer Audit-Pipeline (VictoriaLogs in ein unveränderliches Backend) und Backup-Orchestrierung.

Substrat

Rechenzentrum in der Region, ein DR-Standort in der Region und ein optionales Air-Gap-Enklave für regulatorisch isolierte Workloads.

ARCHITEKTURELEMENT	NIS2-KONTROLLBEREICH
Verschlüsselungsschlüssel je Mandant	Art. 21(2)(h) Kundenkontrollierte Verschlüsselung
NetworkPolicy / Cilium	Art. 21(2)(a) Segmentierung
Audit-Pipeline	Art. 21(2)(i) Art. 23
Mehrere Rechenzentren + DR-Standort	Art. 21(2)(c) Kontinuität & DR
MFA-geschützter Mandantenzugriff	Art. 21(2)(j) Zugriffskontrolle
Tenant-CRD-Isolierung	Art. 21(2)(d) Lieferanten-Exit / Portabilität

Dieses Muster ist nicht die einzige gültige NIS2-konforme Architektur — es zeigt jedoch, wie Isolierung, kundenkontrollierte Kryptografie und unveränderliche Nachvollziehbarkeit die meisten Artikel-21-Kontrollen auf Plattformebene schließen.

Nächste Schritte

Option 1 — Selbst beheben mit dieser Checkliste. Gehen Sie sie mit Security-, Platform- und Compliance-Teams durch. Überführen Sie nicht abgehakte Punkte in einen 90-Tage-Behebungsplan.

Option 2 — NIS2-konformes Readiness-Engagement mit Aenix (4–6 Wochen). Wir arbeiten die Checkliste mit Ihnen durch, prüfen die Architektur gegen jede Kontrolle und erstellen einen Behebungsplan mit Aufwandsschätzungen und Entwürfen der Behördennarrative. Festpreis-Engagement.

Option 3 — Gemeinsames Mapping von NIS2 + DORA + DSGVO. Für Einrichtungen, die in den Anwendungsbereich mehrerer Rahmenwerke fallen. Wir bilden die Kontrollen ab, um Doppelarbeit zu vermeiden, und zeigen auf, wo ein Rahmenwerk mehrere zugleich erfüllt.

Vereinbaren Sie ein Erstgespräch: aenix.io/services/platform-readiness-assessment/

Aktualisierungsrhythmus

- **Vierteljährlich:** Abgleich mit neuen nationalen Umsetzungen und aufsichtsbehördlichen Mitteilungen.
- **Jährlich:** strukturelle Prüfung des Checklisten-Umfangs.
- **Anlassbezogen:** bei wesentlichen Änderungen an NIS2 selbst oder an sektoraler Lex specialis.

Aenix ist das Team hinter Cozystack (einem CNCF-Projekt) und bietet die Ænix Platform — unser kommerzielles, produktisiertes Angebot auf Basis von Cozystack. aenix.io

Aenix · aenix.io · NIS2-Compliance-Readiness-Checkliste · v1.1 — September 2026. Aenix is the team behind Cozystack (CNCF, Apache 2.0).