ÆNIX

DORA-Compliance-Checkliste für die Cloud-Architektur

35 Kontrollpunkte, die zeigen, ob Ihre Cloud-Architektur die DORA-Anforderungen tatsächlich erfüllt.

Für CISOs, Cloud-Architekten und Compliance-Verantwortliche · aenix.io

35 Kontrollpunkte für Finanzunternehmen und IKT-Drittdienstleister. Ausgerichtet auf die Verordnung (EU) 2022/2554. Anwendbar ab dem 17. Januar 2025. v1.1 — September 2026.

So verwenden Sie diese Checkliste

Der Digital Operational Resilience Act (DORA, Verordnung (EU) 2022/2554) ist seit dem 17. Januar 2025 in Kraft. Er gilt für die meisten regulierten Finanzunternehmen, die in der EU tätig sind, sowie für die IKT-Drittdienstleister, die sie beliefern — darunter Cloud-Plattformen, Hosting-Anbieter, Managed Services und Softwareanbieter.

Diese Checkliste mit 35 Punkten gibt CISOs, Cloud-Architekten und Compliance-Teams eine strukturierte Möglichkeit zu beurteilen, ob ihre Cloud-Architektur die DORA-Verpflichtungen unterstützt. Es ist dasselbe Ausgangsframework, das Aenix bei DORA-orientierten Readiness-Projekten mit Finanzunternehmen und IKT-Drittdienstleistern einsetzt.

Nutzen Sie sie auf drei Arten:

1. **Selbstbewertung** — gehen Sie sie gemeinsam mit den Teams für Sicherheit, Platform Engineering und Compliance durch. Jedes nicht angekreuzte Kästchen wird zu einer Maßnahme im Remediationsplan.
2. **Vorbereitung des Aufsichtsdialogs** — die Abschnittszusammenfassungen lassen sich direkt in ein Kontroll-Narrativ-Dokument überführen.
3. **Scoping von Drittanbietern** — teilen Sie sie mit Cloud- / IKT-Anbietern, damit diese gegen dieselbe Oberfläche antworten (hilfreich für die vertragliche Prüfung nach den Artikeln 28-30).

> Diese Checkliste ist eine Hilfe zur architektonischen Readiness, keine Rechtsberatung. Die DORA-Konformität muss von Ihrer Rechtsabteilung bestätigt und gegen etwaige sektorale oder nationale aufsichtsrechtliche Erwartungen validiert werden. RTS/ITS entwickeln sich weiter — gleichen Sie vor jedem Prüfzyklus mit der konsolidierten Fassung auf EUR-Lex ab.

Abschnittsübersicht:

ABSCHNITT	KONTROLLPUNKTE
1. Workload-Portabilität & Exit-Readiness	**5 Punkte**
2. Konzentrationsrisiko	**4 Punkte**
3. Operationelle Resilienz	**5 Punkte**
4. Souveränität & Aufsichtszugang	**5 Punkte**
5. Drittanbieterrisiko & Vertragsgestaltung	**4 Punkte**
6. Risikomanagement & Umgang mit Vorfällen	**12 Punkte**

1. Workload-Portabilität & Exit-Readiness

DORA erwartet von regulierten Unternehmen den Nachweis, dass sie einen IKT-Anbieter wechseln können, ohne den Betrieb zu gefährden. Die Architektur bildet dafür die Grundlage.

- [ ] **Dokumentierter Exit-Plan je kritischem Workload** — mindestens alle 24 Monate getestet. Art. 28(8)
- [ ] **Workload-Portabilität ist strukturell verankert, nicht bloß angestrebt** — Workloads als IaC (Kubernetes-Manifeste, Terraform usw.) ausdrückbar und ohne Neuentwicklung auf einer zweiten Umgebung einsetzbar.
- [ ] **Anbietergebundene Managed Services inventarisiert** — jeder Dienst gekennzeichnet als ersetzbar / neu implementierbar / gebunden. Für „gebundene" Posten existiert ein Plan.
- [ ] **Datenexport getestet** — kundengesteuerter Export aller Datenklassen (Transaktionsdaten, Archiv, Secrets) innerhalb der angegebenen RTO verifiziert. Exit-Kosten modelliert (Egress, Lizenzübertragung, Parallelbetriebsphase).
- [ ] **Exit-Unterstützungspflichten des Anbieters vertraglich geregelt** — der IKT-Anbieter verpflichtet sich vertraglich zu Unterstützung, Datenrückgabe und Zusammenarbeit nach Vertragsende. Art. 30(2)(d) & 30(3)(f)

> Ein „dokumentierter Exit-Plan" ohne regelmäßige Tests ist ein reines Papierartefakt. Aufsichtsbehörden verlangen zunehmend einen Testnachweis, nicht nur die Existenz des Dokuments.

2. Konzentrationsrisiko

DORA hebt das IKT-Konzentrationsrisiko besonders hervor — die übermäßige Abhängigkeit von einem einzelnen Anbieter, Rechenzentrum oder einer einzelnen Jurisdiktion.

- [ ] **Register zur Anbieterkonzentration geführt** — je kritischem Workload: welcher IKT-Anbieter, welche Rechenzentrumsregion, welche souveräne Jurisdiktion. Bei Vertragsänderung aktualisiert. Art. 28(3) & 29(1)
- [ ] **Exponierung gegenüber Einzelanbietern quantifiziert** — aggregierter Anteil der Ausgaben / des Volumens kritischer Workloads je Anbieter. Schwellenwert für die Prüfung durch das Leitungsorgan definiert.
- [ ] **Multi-Region-Design für kritische Workloads** — mindestens zwei physisch getrennte Standorte mit unabhängigen Fehlerdomänen. Für Tier-1-Workloads mindestens ein Standort innerhalb der regulierten Jurisdiktion.
- [ ] **Tragfähigkeit mehrerer Lieferanten bewertet** — auch wenn heute nicht im Einsatz, wurde ein zweiter Lieferant (kaufmännisch und technisch) bewertet, sodass die Konzentration aufgelöst werden kann. Art. 28(2)

> Viele Finanzunternehmen entdecken das Konzentrationsrisiko erst, wenn sie es messen. Eine einzige Hyperscaler-Region für „Produktions"-Workloads ist ein verbreitetes — und zunehmend kritisch geprüftes — Muster.

3. Operationelle Resilienz

DORA verlangt nachgewiesene Resilienz, nicht bloß eine auf Resilienz ausgelegte Konzeption. Testfrequenz und Nachweise stehen im Mittelpunkt.

- [ ] **RTO und RPO je kritischem Workload dokumentiert** — mit der Grundlage der Schätzung (Workload-Klasse, regulatorische Anforderung, Abhängigkeitsanalyse). Art. 11
- [ ] **Backup-Wiederherstellung in den letzten 12 Monaten getestet** — erfolgreiche Wiederherstellung aus einem Produktions-Backup in eine saubere Umgebung. Testbericht aufbewahrt.
- [ ] **Disaster-Recovery-Test durchgeführt** — Failover auf den sekundären Standort, mit gemessenen RTO-Istwerten, aufbewahrt für die aufsichtsrechtliche Prüfung. Art. 25
- [ ] **TLPT (bedrohungsorientierter Penetrationstest) durchgeführt** — für Unternehmen im Anwendungsbereich von TLPT (Artikel 26-27): alle 3 Jahre durchgeführt, Ergebnisse aufbewahrt, Remediation nachverfolgt. Art. 26
- [ ] **Programm für operationelle Resilienz durch das Leitungsorgan gesteuert** — jährlicher Bericht an das Leitungsorgan. Art. 5

> Das Scoping eines TLPT ist ein umfangreiches Vorhaben. Wenn Ihr Unternehmen im Anwendungsbereich liegt, aber noch keinen durchgeführt hat, planen Sie 12-18 Monate Vorbereitung ein, einschließlich Anbieterbeschaffung, Scope-Abstimmung mit der Aufsicht und Remediationsbudget.

4. Souveränität & Aufsichtszugang

DORA setzt voraus, dass Aufsichtsbehörden IKT-Dienste abrufen, prüfen und inspizieren können. Die Architektur entscheidet, ob dies durchführbar ist.

- [ ] **Kundengesteuerte Verschlüsselungsschlüssel für sensible Daten** — einschließlich Bring-Your-Own-Key oder Hold-Your-Own-Key für Tier-1-Workloads. Schlüsselverwahrungsdokument vom CISO genehmigt. Art. 9(4)(d)
- [ ] **Audit-Logs unveränderlich und exportierbar** — Wer-hat-was-wann-Protokolle mit einer Aufbewahrungsdauer, die die längste geltende Anforderung erfüllt (oft 5+ Jahre). Manipulationssichere Speicherung. Kundengesteuerter Export. Art. 30(3)(e)
- [ ] **Prozess für den Aufsichtszugang dokumentiert und geübt** — ein Verfahren zur Gewährung des Aufsichtszugangs zu Systemen, Protokollen und Personal; getestet mit einer internen Simulation eines Aufsichtsszenarios. Art. 28(6) & 30(3)(e)
- [ ] **Kontrollen zur Datenresidenz je Workload durchsetzbar** — Platzierungsbeschränkungen für Workloads (nur EU, ein einzelnes Land usw.) durch die Plattform durchgesetzt, nicht auf Disziplin der Betreiber angewiesen.
- [ ] **Zugriffe von Anbieterpersonal protokolliert und überprüfbar** — einschließlich Admin- / Break-Glass-Zugriffen durch Personal des IKT-Anbieters, Jurisdiktion des Zugriffs, zeitlich begrenzte Freigaben. Art. 9(4)(c) & 30(3)(e)

> „Kundengesteuerte Schlüssel“ müssen sich auf Backup-, Replikations- und Observability-Daten erstrecken — nicht nur auf die primäre Datenbank. Eine häufige Lücke sind ruhend verschlüsselte Produktionsdaten, deren Backups durch anbieterverwaltete Schlüssel geschützt sind.

5. Drittanbieterrisiko & Vertragsgestaltung

Artikel 28 legt die allgemeinen Grundsätze für das Management des IKT-Drittparteienrisikos fest, Artikel 30 die wesentlichen Vertragsbestimmungen zwischen regulierten Unternehmen und IKT-Anbietern — einschließlich unterbeauftragter IKT-Dienste.

- [ ] **IKT-Drittanbieterregister vollständig und aktuell** — alle IKT-Anbieter, einschließlich indirekter (unterbeauftragter) mindestens bis zur zweiten Stufe. Bei Vertragsänderung aktualisiert. Art. 28(3)
- [ ] **Wesentliche Vertragsbestimmungen nach Artikel 30 in Vereinbarungen zu kritischen Funktionen vorhanden** — die Vertragsbedingungen decken ab: Leistungsbeschreibung, Zugangs- / Prüfrechte, Unterbeauftragung, Datenrückgabe, Exit-Unterstützung und Kündigung. Art. 30
- [ ] **Transparenz der Unterbeauftragung vertraglich durchgesetzt** — der Anbieter muss wesentliche Änderungen an Unterauftragnehmern, die kritische Funktionen erbringen, vorab anzeigen. Art. 30(2)(a)
- [ ] **Kontinuierliche Überwachung der Anbietersituation** — mindestens jährliche Anbieterüberprüfung; Ereignisse, die eine anlassbezogene Überprüfung auslösen (Vorfälle, M&A, aufsichtsrechtliche Maßnahmen). Art. 28(2)

> Bestehende IKT-Verträge, die vor dem Anwendungsstichtag von DORA geschlossen wurden, genießen keinen Bestandsschutz — sie müssen in Compliance überführt werden. Prüfen und nachverhandeln.

6. Risikomanagement & Umgang mit Vorfällen

Der umfangreichste Abschnitt — er umfasst das IKT-Risikomanagement-Framework (Artikel 5–16, bes. Art. 6) sowie die Klassifizierung, Meldung und Bearbeitung IKT-bezogener Vorfälle (Artikel 17–19).

6a. Risikomanagement-Framework

- [ ] **IKT-Risikomanagement-Framework dokumentiert** — vom Leitungsorgan genehmigt, mindestens jährlich überprüft. Art. 5 & 6
- [ ] **IKT-Asset-Register vollständig und aktuell** — Hardware, Software, Daten, Abhängigkeiten; mit dem Risikoregister verknüpft. Art. 8
- [ ] **Risikoregister kontinuierlich aktualisiert** — je kritischem Workload; mit Verantwortlichem, Behandlungsstatus, Restrisiko. Jährlich durch die Revision überprüft. Art. 6
- [ ] **Wirksamkeitsprüfung der IKT-Kontrollen — vierteljährlich** — dokumentierte Nachweise aufbewahrt.
- [ ] **Cybersicherheitsrichtlinie vom Leitungsorgan genehmigt** — jährlich aktualisiert.
- [ ] **Cybersicherheitsschulung für alle Mitarbeitenden verpflichtend** — einschließlich der Geschäftsleitung; Abschluss nachverfolgt.

> Abschnitt 6 ist der Bereich, in dem die meisten Lücken zutage treten. Aufsichtsbehörden suchen nach kontinuierlichen Nachweisen, nicht nach Momentaufnahmen. Nutzen Sie diesen Abschnitt als Input für Ihren jährlichen IKT-Risikobericht statt als einmalige Prüfung.

6b. Umgang mit Vorfällen

DORA hat die Klassifizierung von Vorfällen, Meldefristen und Ursachenanalyse gegenüber früheren NIS- / sektoralen Regelungen deutlich verschärft.

- [ ] **24×7-Erkennungsfähigkeit für IKT-bezogene Vorfälle** — insbesondere für kritische Workloads. Ausgerichtet an den Schwellenwerten der RTS zur Klassifizierung von Vorfällen. Art. 10 & 17
- [ ] **Prozess zur Klassifizierung von Vorfällen dokumentiert** — Schwellenwerte für „schwerwiegend“ vs. „nicht schwerwiegend“ ausdrücklich definiert und genehmigt. Art. 18
- [ ] **Meldevorlagen an DORA-Fristen ausgerichtet** — Erstmeldung innerhalb weniger Stunden, Zwischenbericht innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats (gemäß Delegierter Verordnung (EU) 2025/301). Art. 17-19 Delegierte VO (EU) 2025/301
- [ ] **Vorab eingerichtete Kommunikationskanäle mit den zuständigen Behörden** — benannte Kontakte beim CSIRT, sektoralen Aufseher und federführenden Überwacher. Art. 19(1)
- [ ] **Dokumentierte Vorfallreaktion mit benannten Rollen** — IR-Plan mit Bereitschaftsdienst, Eskalation, Entscheidungsbefugnis und Kommunikations-Playbook.
- [ ] **Jährliche Übung zur Vorfallreaktion** — Tabletop oder live; Ergebnisse aufbewahrt und in die Aktualisierung des Frameworks eingespeist. Art. 11

> Kleinere Finanzunternehmen nehmen mitunter an, DORA gelte nur für „die großen Banken“. Er gilt für die meisten regulierten Unternehmen, darunter Wertpapierfirmen, Versicherungsvermittler, Anbieter von Krypto-Dienstleistungen und viele weitere (siehe Anwendungsbereich in Artikel 2).

Empfehlungen auf Architekturebene

Bei den meisten Kontrollpunkten ist die Lücke struktureller, nicht prozeduraler Natur. Eine Plattform, die auf (1) Workload-Portabilität über Kubernetes-native Primitive, (2) kundengesteuerten Verschlüsselungsschlüsseln auf jeder Ebene, (3) unveränderlichen, kundenexportierbaren Audit-Logs, (4) durchsetzbarer, datenresidenzgebundener Workload-Platzierung und (5) getesteten Exit- / Wiederherstellungsmechaniken aufbaut, adressiert den Großteil der architektonischen Oberfläche von DORA in einem einzigen kohärenten Design — statt als 35 separate kompensierende Kontrollen.

Aenix entwirft Plattformen nach diesem Muster. Cozystack (CNCF Project) liefert die quelloffene Grundlage; die Ænix Platform ergänzt sie um ein Enterprise-SLA, Lieferantentransparenz und DORA-orientierte Betriebsdokumentation, die für die aufsichtsrechtliche Prüfung geeignet ist.

Bestehende Plattformen (VMware-basiert, OpenStack-basiert, Hyperscaler-basiert) lassen sich meist teilweise nachrüsten — doch die Erwartungen von DORA an Portabilität und Exit-Readiness sind schwer zu erfüllen, wenn die zugrunde liegende Plattform selbst die Quelle des Lock-in ist.

Nächste Schritte

Option 1 — Selbstständige Behebung mit dieser Checkliste. Weisen Sie jedes nicht angekreuzte Kästchen einem Workstream-Verantwortlichen zu. Die meisten Finanzunternehmen haben 12-18 nicht angekreuzte Kästchen, die 90 Tage strukturierte Arbeit erfordern.

Option 2 — DORA-orientiertes Readiness-Projekt mit Aenix (4-6 Wochen). Wir gehen die Checkliste gemeinsam mit Ihnen durch, prüfen die Architektur gegen jede Kontrolle und erstellen einen Remediationsplan mit Aufwandsschätzungen und Entwürfen für das Aufsichts-Narrativ. Festpreis-Projekt.

Option 3 — Gemeinsames Mapping von DORA + NIS2 + sektoralen Anforderungen. Für Unternehmen im Anwendungsbereich mehrerer Rahmenwerke. Wir bilden Kontrollen über DORA, NIS2 und sektorale Erwartungen hinweg ab, um Doppelarbeit zu vermeiden.

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

Aktualisierungsrhythmus

- **Vierteljährlich:** Abgleich mit neuen RTS/ITS-Veröffentlichungen und aufsichtsrechtlichen Mitteilungen.
- **Jährlich:** strukturelle Überprüfung der Abdeckung der Checkliste.
- **Anlassbezogen:** bei wesentlichen Änderungen an DORA selbst.

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

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