DORA Health Check

DORA kommt – sind Sie vorbereitet?
Kompakte Konformitätsprüfung & GAP-Analyse.

Die EU-Verordnung DORA (Digital Operational Resilience Act) verpflichtet Finanzunternehmen und ihre IT-Dienstleister dazu, ihre digitale Betriebsstabilität umfassend abzusichern. Ziel ist es, widerstandsfähige IT-Systeme und Prozesse zu gewährleisten, die auch in Krisensituationen funktionieren. Ab dem 17.01.2025 müssen betroffene Unternehmen umfassende Anforderungen an Risikomanagement, Incident Reporting, Tests der digitalen Resilienz, Drittparteienmanagement und Governance-Strukturen erfüllen. Mit unserem DORA Health Check erhalten Sie eine strukturierte, praxisnahe Bewertung Ihrer digitalen Resilienz – transparent, umsetzungsorientiert und gezielt auf die Anforderungen der EU-Verordnung zugeschnitten.

[at] alexanderthamm × isys

Der Fokus liegt auf zwei zentralen Themenbereichen:

Datenstrategie & Governance

Im Bereich **Prozesse & Governance**, verantwortet durch die Alexander Thamm GmbH, erfolgt eine gezielte Analyse zentraler DORA-Compliance-Faktoren. Dazu zählen unter anderem: bestehende Governance-Strukturen, das IKT-Risikomanagement, Notfall- und Wiederanlaufprozesse sowie die regulatorischen Berichts- und Meldepflichten. Ziel dieser Prüfung ist es, die aktuelle organisatorische Aufstellung zu bewerten, regulatorische Lücken zu identifizieren und praxisnahe Handlungsempfehlungen zur Erreichung der DORA-Konformität abzuleiten.

Technologische Resilienz & Sicherheit

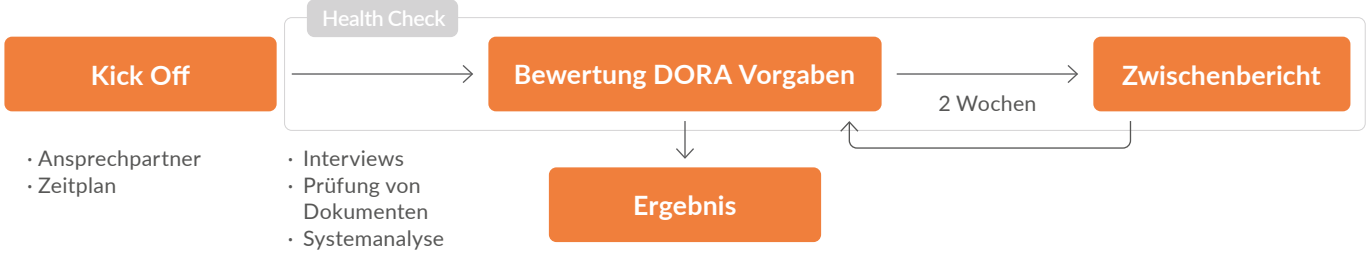
Die **technologische Resilienzprüfung**, durchgeführt durch die iSYS GmbH, liefert eine erste Einschätzung Ihrer IT-Landschaft im Hinblick auf Infrastrukturrisiken und die Fähigkeit, systemische Schwachstellen zu erkennen und zu managen. Im Fokus stehen hierbei:

- die **strukturelle Resilienz Ihrer IT-Infrastruktur,**
- ein **Maßnahmenkatalog für ein effizientes Monitoring**
- sowie ein **Testplan für Cyber-Resilienzmaßnahmen.**

Die Bewertung orientiert sich an aktuellen regulatorischen Vorgaben und sicherheitstechnischen Standards im Kontext der DORA-Verordnung.

Vorgehensweise

Der **DORA Health Check** startet mit einem gemeinsamen Kick-off. Dabei wird die Zielsetzung ausführlich erläutert, sodass alle Beteiligten ein einheitliches Verständnis haben. Anschließend stimmen wir Zeitplan und Ansprechpartner gemeinsam ab. Die eigentliche Analyse basiert auf strukturierten Interviews mit Schlüsselpersonen, auf der gezielten Auswertung zentraler Dokumente und einer umfassenden Analyse der relevanten IT-Systeme. Für eine fundierte Bewertung ist es entscheidend, dass relevante Unterlagen und Systemzugänge bereitgestellt werden – so können wir gemeinsam mit den zuständigen Fachbereichen eine präzise Einschätzung vornehmen.



Bewertungsumfang nach zentralen DORA-Kapiteln

Im DORA Health Check bewerten wir relevante Vorgaben aus den folgenden zentralen DORA-Abschnitten und verifizieren die technische Resilizenz der betroffenen IT-Systeme:

DORA Artikel	Bewertungsbereich	Prüfschwerpunkte
IKT-Risikomanagement (Art. 5 – 15) [at]	Aufbau und Reifegrad des IKT-Risikomanagements	• IKT-Risikomanagement-Framework • Rollen-, Zuständigkeits- und Eskalationsmodell • Awareness- & Schulungskonzept für IKT-Risiken & DORA • Dokumentationsrichtlinie & Templates
IKT-Vorfallmanagement & Meldungen (Art. 17 – 23 DORA) [at]	Prozesse zur Vorfallreaktion und Kommunikation	• Incident Response Plan inkl. Meldeprozesse • Major-Incident-Response-Prozess • Kommunikationsplan für Vorfälle
IKT-Vorfallmanagement & Meldungen (Art. 17–23 DORA) isys	Bewertung der IKT-Überwachung	• Bestandsaufnahme Monitoring / Observability • Bewertung nach Kritikalität • Handlungsempfehlung für Umsetzung
Digitale Resilienz-Tests (Art. 24 – 27 DORA) isys	Teststrategie und Resilienz-bewertung	• Analyse bestehender Teststrategien • Bewertung kritischer Businessfunktionen • Testplan für Cyber-Resilienzmaßnahmen
Drittparteienmanagement (Art. 28 – 41 DORA) [at]	Steuerung und Überwachung externer IKT-Dienstleister	• Richtlinie zum Drittparteien-Risikomanagement • Verzeichnis wesentlicher IT-Dienstleister & kritischer Services • Vertragsrichtlinie mit Sicherheits- & Exitanforderungen • Exitstrategie für kritische Anbieter

Auf Basis der bereitgestellten Unterlagen und im engen Austausch mit Ihren Ansprechpartnern führen wir eine strukturierte Analyse hinsichtlich **Vollständigkeit, Aktualität, Kohärenz und DORA-Konformität** durch. Die Ergebnisse fließen in eine **systematische GAP-Analyse** ein, die entlang der zentralen DORA-Kapitel aufgebaut ist und eine fundierte Einschätzung des Umsetzungsstandes ermöglicht.
Ziel der Analyse ist die Bestimmung des aktuellen Reifegrads Ihres Unternehmens im Kontext der DORA-Anforderungen – mit Fokus auf das Aufdecken regulatorischer und technischer Lücken sowie der Identifikation erster Risiken, die frühzeitig adressiert werden sollten.

Ergebnis

Sie erhalten eine **strukturierte GAP-Analyse**, differenziert nach den zentralen DORA-Kapiteln und individuell auf Ihre organisatorische und technologische Ausgangssituation abgestimmt. Der Ergebnisbericht umfasst:

- eine fundierte Einschätzung Ihres aktuellen **Reifegrads** im Hinblick auf DORA
- die **Identifikation regulatorischer Lücken** und technologischer Schwachstellen und Risiken
- **konkrete Handlungsempfehlungen** – priorisiert nach Umsetzungsbedarf und Risikopotenzial

Optional erarbeiten wir gemeinsam mit Ihnen eine maßgeschneiderte **Roadmap zur Umsetzung** erforderlicher Maßnahmen und begleiten Sie auf Wunsch auch in der weiteren Umsetzung.

Projektlaufzeit

Der DORA Health Check ist auf einen kompakten Zeitraum von ca. **4 bis 6 Wochen** ausgelegt. Der konkrete Zeitplan hängt maßgeblich von der Verfügbarkeit relevanter Ansprechpartner sowie vom Zugriff auf notwendige Dokumente und Systeme ab. Durch eine enge und effiziente Abstimmung lässt sich die Durchführung zügig und zielgerichtet realisieren.