DORA – EU-Regelung für den Finanzsektor

Um die Betriebsstabilität und Widerstandsfähigkeit u.a. gegen Cyberangriffe maßgeblich zu stärken, wurden 2025 Vorgaben zum Schutz vor IT-Störungen und anderen Bedrohungen, die Finanzmarktteilnehmer und deren Drittanbieter gefährden, beschlossen.

Dem IT-Betrieb kommt im Rahmen der Stärkung der digitalen operationalen Resilienz eine gesteigerte Bedeutung zu.

Dies beginnt mit der Identifikation kritischer Systeme und Assets: Es muss evaluiert werden, welche Anwendungen, Server, Netzwerke und Datenverbindungen als „kritisch“ im Sinne von DORA eingestuft sind, etwa weil sie für Zahlungsprozesse, Marktinfrastruktur oder regulatorische Berichterstattung essenziell sind.

Daraus ergeben sich Anforderungen an Monitoring, Härtung und Schutz dieser Systeme auf technischer Ebene.

Weiter verlangt ist die Störungs- und Vorfallbehandlung. Schwere IT-Vorfälle (z. B. Systemausfälle oder Cyberangriffe) müssen nicht nur dokumentiert, sondern auch innerhalb bestimmter Fristen an Aufsichtsbehörden gemeldet werden. Zentral ist die technische Umsetzung von Incident-Response-Prozessen – inklusive Alarmierung, Analyse, Abgrenzung und Wiederherstellung.

Auch das regelmäßige Testen der digitalen Resilienz gehört zu den technischen Vorgaben: Dazu zählen IT-Notfallübungen, Simulationen von Cyberangriffen und Recovery-Tests unter realitätsnahen Bedingungen.

Verlangt ist des Weiteren der Ausbau eines effektiven IT-Risikomanagements. Gewonnene Erkenntnisse aus Schwachstellen- und Pentests sowie Resultate aus Logananlysen sollen Risiko- und Maßnahmenkataloge informieren, die in technische Roadmaps übersetzt werden.

Um eine informierte Entscheidungsfindung zu erlauben, schreibt DORA vor, dass Unternehmen über eine lückenlose Protokollierung sicherheitsrelevanter Ereignisse verfügt und diese nachvollziehbar auswerten können. Hierfür sind SIEM-Systeme, zentrale Log-Server und korrelierende Analysewerkzeuge erforderlich.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Noch ein kritischer Punkt ist das Management von Drittanbietern, insbesondere von IKT-Dienstleistern. Es müssen Verfügbarkeits-, Sicherheits- und Integritäts-anforderungen eingehalten und kontrolliert werden, etwa durch regelmäßige SLA-Überprüfungen, Sicherheitszertifikate oder technische Zugriffsbeschränkungen. Schnittstellen zu Cloud-Anbietern oder Outsourcing-Partnern müssen so gestaltet sein, dass auch im Notfall die Datenverfügbarkeit, Transparenz und Handlungsfähigkeit erhalten bleibt.

Insgesamt verlangt die DORA-Implementierung nicht nur tiefgehendes technisches Know-how, sondern auch die Fähigkeit, IT-Sicherheit, Betriebsstabilität und regulatorische Anforderungen in einem ganzheitlichen Konzept zu verbinden. Die Herausforderung liegt dabei nicht allein in der Einführung neuer Technologien, sondern in der dauerhaften Integration robuster Resilienzmaßnahmen in den IT-Alltag – ohne dabei die Flexibilität und Innovationsfähigkeit der Systeme zu .

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

DORA-Betroffenheits-Checkliste

1. Grundlegende Einstufung

A. Sind wir ein Finanzunternehmen gemäß DORA?

(Mind. eine Aussage mit „Ja“ → direkt betroffen)

Fragen:	Ja	Nein
Sind wir eine Bank, ein Kreditinstitut oder eine Sparkasse?	☐	☐
Sind wir ein Versicherungs- oder Rückversicherungsunternehmen?	☐	☐
Sind wir ein Zahlungsdienstleister oder E-Geld-Institut?	☐	☐
Sind wir eine Wertpapierfirma oder ein Fondsverwalter?	☐	☐
Bieten wir Krypto-Dienstleistungen oder Blockchain-basierte Finanzprodukte an?	☐	☐
Unterliegen wir der Aufsicht einer EU-Finanzaufsicht (z. B. BaFin, CSSF, FMA etc.)?	☐	☐

B. Erbringen wir digitale Dienste für Finanzunternehmen?

(Mind. eine Aussage mit „Ja“ → evtl. als kritischer IKT-Dienstleister betroffen)

Fragen:	Ja	Nein
Erbringen wir Cloud-Dienste (IaaS, PaaS, SaaS) für Finanzunternehmen?	☐	☐
Stellen wir Softwarelösungen bereit, die Finanzunternehmen zur Abwicklung ihrer Kernprozesse nutzen?	☐	☐
Bieten wir Cybersecurity- oder Netzwerk-Infrastruktur-Dienste für regulierte Finanzunternehmen an?	☐	☐
Verarbeiten oder speichern wir Daten im Auftrag von Finanzunternehmen?	☐	☐
Sind unsere Dienste vertraglich als „kritisch“ oder „wesentlich“ für den Finanzkunden definiert?	☐	☐
Haben wir (Cloud-/IT-)Kunden aus dem Finanzsektor in der EU?	☐	☐

---

2. Art und Umfang der Tätigkeit

C. Kritikalität & Risiko der Leistung

(Je mehr „Ja“, desto wahrscheinlicher DORA-Relevanz)

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Fragen:	Ja	Nein
Würde ein Ausfall unserer Leistung den Geschäftsbetrieb eines Finanzunternehmens gefährden?	☐	☐
Haben wir Zugriff auf vertrauliche oder sensible Finanzdaten?	☐	☐
Haben unsere IT-Leistungen direkten Einfluss auf regulatorische oder Compliance-relevante Prozesse?	☐	☐

---

3. Vertragliche & Aufsichtsrechtliche Hinweise

D. Hinweise auf regulatorische Verpflichtungen

(Wenn „Ja“, DORA-Relevanz wahrscheinlich)

Fragen:	Ja	Nein
Gibt es in unseren Verträgen mit Kunden aus dem Finanzsektor spezielle Anforderungen zu IT-Sicherheit oder Resilienz?	☐	☐
Wurden wir von einem Kunden bereits über Anforderungen im Zusammenhang mit DORA informiert?	☐	☐
Wurden wir von einer Behörde oder Aufsicht (z. B. BaFin, EZB) kontaktiert wegen DORA?	☐	☐

Auswertung

Anzahl "Ja" Antworten	Einschätzung
0–2	Wahrscheinlich **nicht betroffen**

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Anzahl "Ja" Antworten	Einschätzung
3–5	**Möglicherweise betroffen** – nähere Prüfung empfohlen
6 oder mehr	**Höchstwahrscheinlich betroffen** – Maßnahmen gemäß DORA einleiten

---

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg