grosse-hornke

DORA SPRINT

DIE NEUE EU-VERORDNUNG PÜNKTLICH UND SICHER UMSETZEN

Ermitteln Sie Ihren DORA-Score: Welche Kriterien erfüllen Sie heute schon?

Ein Berg namens DORA

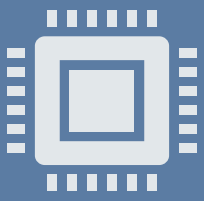
Wer muss sich der Aufgabe stellen?

Der „Digital Operational Resilience Act“,
kurz DORA, ist eine neue EU-Verordnung.

Ihr Unternehmen ist davon betroffen, wenn es
der Finanzbranche angehört oder für diese tätig ist:

Banken

Versicherungen



IT-Dienstleister

grosse-hornke

Hohe Ziele

Worum geht es bei DORA?

Standards für einen sicheren IT-Betrieb

Finanzinstitute sollen sich EU-weit so gut wie möglich gegen Cyberrisiken wappnen. DORA definiert darum einheitliche Standards für das IT-Risikomanagement.

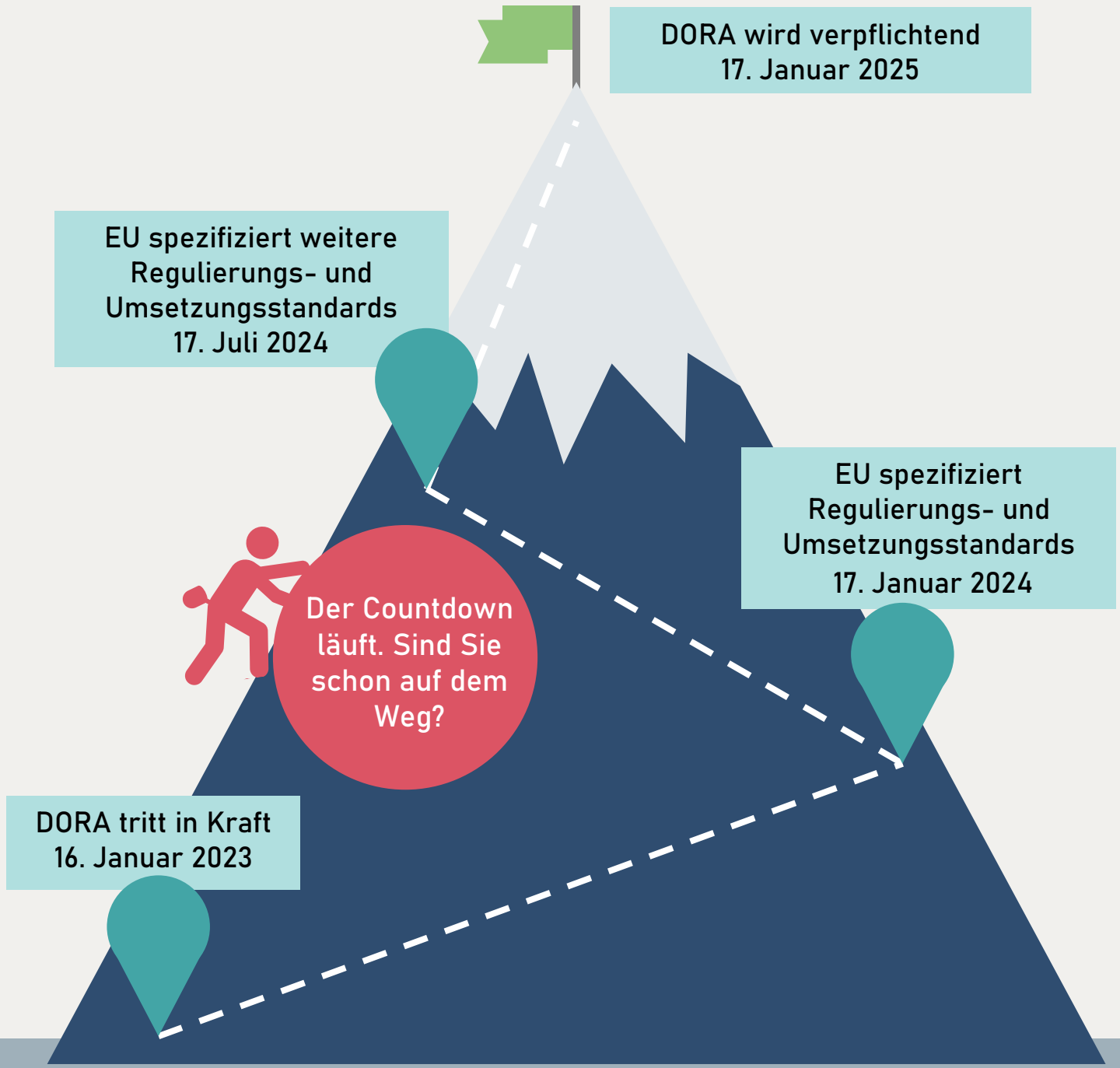
Schnelle Reaktion auf Bedrohungen

Behörden sollen IT-Sicherheitsrisiken für das europäische Finanzsystem früh erkennen und schnell Gegenmaßnahmen einleiten. Dazu definiert DORA spezielle Meldeverfahren.

Augenmerk auf Drittanbieter

IT-Dienstleister sind zentral für die Digitalisierung der Finanzbranche, dürfen jedoch keine Sicherheitslücken zulassen. DORA schafft einen Rechtsrahmen für eine behördliche Aufsicht.

Die beste Zeit zu handeln: jetzt



grosse-hornke

Ein Schritt nach vorn

Was bringt DORA Ihrem Unternehmen?

Gleiche Regeln

Prozesse automatisieren, KI implementieren, Cloudstrategie vorantreiben – ohne Abstriche bei der IT-Sicherheit. DORA kann Ihrem Unternehmen helfen, Digitalisierung mit Vorsicht in Einklang zu bringen. Wer Risiken sorgfältig managt, hat in der EU keine Nachteile, weil dieselben Regeln gelten.

Externe Sicherheit

Unternehmen der Finanzbranche passen nicht nur ihre eigenen Systeme und Prozesse an, sondern erhalten auch einen klaren, verpflichtenden Rahmen für ihre Verträge mit IT-Dienstleistern: Welche Sicherheitsvorkehrungen müssen externe Partner treffen – und wer steht dafür gerade, wenn etwas passiert? DORA bringt somit mehr Sicherheit im Third Party Risk Management (TPRM).

Gut vorbereitet als IT-Dienstleister

Wenn Sie IT-Services für die Finanzbranche erbringen, haben Sie Klarheit, wie Kunden ihre Verträge in Zukunft gestalten werden, und können sich auf die neuen Standards einstellen.

grosse-hornke

Was liegt vor Ihnen?

4 Herausforderungen auf dem Weg ans Ziel (1/2)

1. IT-Resilienz wird Chefsache

Ein solider IT-Betrieb wird zur strategischen Priorität. DORA nimmt die Unternehmensführung in die Pflicht, ein IT-Risikomanagement aufzubauen und regelmäßig zu überprüfen, ob die Maßnahmen greifen.

2. BaFin-feste Pläne für den Krisenfall

Unter dem Stichwort „Geschäftsfortführung“ erlegt die EU den Unternehmen auf, einen umfassenden Aktionsplan bereitzuhalten. Dieser Plan umfasst auch IT-Dienstleistungen.

Unternehmen der Finanzbranche müssen Schritt für Schritt festlegen, was Sie bei einem Vorfall unternehmen. Dazu gehört auch die Entscheidung, wie gravierend ein Incident ist, und ob die zuständige Behörde davon erfahren muss.

Nicht nur die Aufsicht ist zu informieren. Für den Ernstfall brauchen Unternehmen auch Leitlinien für die Kommunikation mit weiteren Stakeholdern, zum Beispiel mit Kunden, Mitarbeitenden, Partnern und der Öffentlichkeit.

grosse-hornke

Was liegt vor Ihnen?

4 Herausforderungen auf dem Weg ans Ziel (2/2)

3. Neuartige Stesstests

Unternehmen müssen regelmäßig einen sogenannten Threat-Led-Penetration-Test (TLPT) vornehmen, also Angriffe mit hohem Bedrohungspotenzial simulieren. Welche Art Attacken dies sind, ist in einer speziellen Analyse vorab zu ermitteln. Mindestens alle drei Jahre müssen diese Tests stattfinden, abhängig vom Risikoprofil Ihres Unternehmens eventuell häufiger. Dies stellt die zuständige Behörde fest.

4. Provider rücken in den Fokus

DORA verpflichtet Finanzunternehmen, auch ihre IT-Dienstleister einem Sicherheitscheck zu unterziehen: Stehen sie dafür ein, dass ihre Services sicher und zuverlässig sind? Beauftragende Unternehmen müssen gegebenenfalls Verträge umgestalten und Audits bei den Drittanbietern vornehmen.

Für IT-Dienstleister bedeutet das entsprechend, dass sie die Sicherheit ihrer Systeme nachweisen und dafür einen Prozess gestalten müssen.

grosse-hornke

Perfekter Start

Von der Gap-Analyse zum Aktionsplan

Erfassen relevanter Bereiche & Planung	• Welche Organisationseinheiten müssen mitwirken? • Welche Arbeitspakete sind zu erledigen? • Wer sind die Stakeholder des Projekts?
Interviews mit Stakeholdern	• Wie sehen aktuelle Prozesse des IT-Risikomanagements aus? • Welche IT-Projekte sind zu berücksichtigen? • Bestehen Ressourcenkonflikte?
Analyse vorhandener Dokumente	• Sind Prozesse des IT-Risikomanagements DORA-konform dokumentiert? • Müssen wir die internen Leitlinien sowie Verträge mit IT-Dienstleistern überarbeiten?
Abstimmung der Gap-Analyse-Resultate	• Welche Anmerkungen haben die Verantwortlichen für IT und weiterer relevanter Fachbereiche? • Gibt die Unternehmensführung grünes Licht für die Umsetzung?
Priorisieren der Maßnahmen	• Welche Arbeiten haben Vorrang mit Blick auf Relevanz, Umfang und Verfügbarkeit von Ressourcen?
Ihre Roadmap	• Detaillierter Projekt- und Zeitplan • Inklusive Vorlaufzeiten, so dass Ihr Unternehmen alle Vorgaben pünktlich umsetzt

grosse-hornke

Wo stehen Sie heute?

Ermitteln Sie Ihren DORA-Score

Beruhigend: Kein Unternehmen fängt bei Null an, denn eine Reihe von Vorschriften der BaFin finden sich auch in DORA wieder.

Wo aber bestehen noch Lücken?

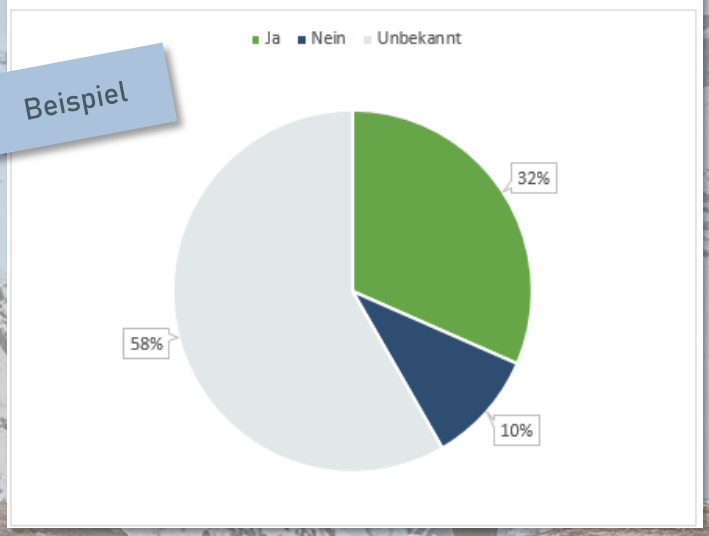
Für eine erste qualifizierte Antwort haben wir zwei Checklisten erstellt – für Unternehmen der Finanzbranche und speziell für IT-Dienstleister.

Anhand der Excel-Listen können Sie sofort ihren DORA-Score ablesen – so werden die wesentlichen Lücken transparent:

Auswertung

Ja	32%	(53 der Anforderungen sind erfüllt)
Nein	10%	(17 der Anforderungen sind nicht erfüllt)

98 der Fragen sind nicht beantwortet oder unbekannt



Beispiel

Jetzt Checklisten anfordern für
> Finanzbranche
> IT-Dienstleister

Hinweis: Anhand der Checklisten können Sie sich einen ersten Überblick verschaffen: Wo liegt der größte Handlungsbedarf? Um Ihr Unternehmen DORA-konform aufzustellen, empfehlen wir, anschließend weiter ins Detail zu gehen.

grosse-hornke

Guide gesucht?

Wir bringen Sie sicher ans Ziel

Sturmerprobtes IT-Projektmanagement für DAX-40-Unternehmen

Erfahren in Regulatorik-Projekten und IT-Security-Themen der Finanzbranche

Wachsames Auge für Risiken und Ihr Budget

Stark im Change-Management bei komplexen Fachthemen

grosse-hornke

Sie haben Fragen zu DORA?

Kontaktieren Sie uns gerne unverbindlich:

Silke Grosse-Hornke

Telefon: Tel. +49 (0)2501 59435-10
E-Mail: silke.grosse@grosse-hornke.de

www.grosse-hornke.de

Herausgeber

grosse-hornke
Am Dornbusch 54
48163 Münster

grosse-hornke