MATERNA

Whitepaper

EU-DORA – Warum Tools allein nicht reichen

Erst die Compliance verstehen, dann die Technik umsetzen

Seit Januar 2025 gilt der Digital Operational Resilience Act, kurz DORA. Zahlreiche Tools werben damit, DORA-Features zu bieten – aber das reicht nicht. Wer die regulatorischen Anforderungen nicht versteht, scheitert trotz bester Technologie.

Das Tool-Missverständnis

„Wir kaufen ServiceNow mit DORA-Features, dann sind wir compliant." Dieser Gedanke ist verständlich, aber falsch. Denn DORA-Compliance beginnt mit dem Verständnis der Anforderungen, nicht mit der Technologie. Moderne ITSM-Tools bieten durchaus DORA-Funktionen. Aber diese decken nur Teilbereiche ab. Die fachliche Integration der Anforderungen aus der EU-Verordnung bleibt Ihre Aufgabe.

DORA fordert strukturiertes Reporting nach dem Data Point Model (DPM) der Europäischen Bankenaufsichtsbehörde. Erfolgreiche Meldungen erfordern komplexe Datenselektion und individuelle Interpretation. Ein Tool kann Berichte erstellen, aber Sie entscheiden, was berichtet werden muss.

Entscheidend
DORA-Compliance beginnt mit dem Verständnis der Anforderungen, nicht mit der Technologie.

Was DORA wirklich verlangt

DORA definiert fünf Kernbereiche, die Versicherer beherrschen müssen. Jeder Bereich stellt fachliche Anforderungen, die kein Tool automatisch löst.

IKT-Risikomanagement: Sie müssen alle IT-Risiken systematisch identifizieren und bewerten. Welche Systeme sind kritisch? Das entscheiden Ihre Experten im Kontext Ihrer Unternehmensarchitektur, nicht die Tools. Ihr Schadenmanagement-System fällt aus – ist das DORA-meldepflichtig? Das hängt von der Ausfallzeit und den betroffenen Kunden ab.

Incident-Reporting: Schwerwiegende IKT-Vorfälle müssen binnen 24 Stunden gemeldet werden. DORA definiert Kriterien für „schwerwiegend". Aber deren Anwendung auf Ihre IT-Landschaft erfordert Expertenwissen. Ein Server-Ausfall kann je nach Kontext kritisch oder belanglos sein. Und die Optimierung der Resilienz erfordert eine IKT-Referenzarchitektur als Basis.

Operative Resilience-Tests: DORA fordert Threat-Led Penetration Testing (TLPT), und zwar alle drei Jahre. Diese Tests müssen von der Europäischen Bankenaufsicht genehmigt werden. Weder ITSM-Tools noch Cyber-Security-Suites organisieren dies automatisch, denn Bedrohungen sind so individuell wie Ihr Unternehmen.

Third-Party-Risikomanagement: Sie müssen alle kritischen IKT-Dienstleister identifizieren, bewerten und überwachen. Welche Dienstleister sind kritisch, und warum? Wie bewerten Sie deren Risiken und was sind valide Handlungsoptionen? Das sind fachliche Entscheidungen, die im Kontext des ganzheitlichen IKT-Risikomanagements gefällt werden müssen.

Informationsaustausch: DORA etabliert neue Meldewege zwischen Finanzinstituten. Diese Prozesse müssen Sie verstehen und in Ihre Abläufe integrieren, da Sie für die Richtigkeit geradestehen.

Fachliche Bewertung entscheidet
Ein Server-Ausfall kann DORA-kritisch oder belanglos sein – je nach Kontext. Das entscheiden Ihre Experten, nicht die Tools.

Das Legacy-Daten-Problem

Ihre DORA-relevanten Daten liegen oft verstreut in dutzenden Alt-Systemen. Asset-Management-Tools dokumentieren Hardware. Monitoring-Systeme protokollieren Verfügbarkeit. Andere Tools verfolgen Systemänderungen.

Diese Systeme sprechen meist nicht miteinander. Jedes Repository hat eigene Datenstrukturen und Klassifikationen. Die manuelle Zusammenführung für DORA-Meldungen ist aufwendig und fehleranfällig.

Das Data Point Model der EBA definiert präzise Datenfelder, doch Ihre Legacy-Daten passen selten direkt in diese Struktur. Sie müssen komplexe Zuordnungen entwickeln und pflegen.

Ein Beispiel: DORA verlangt die Klassifikation von IT-Vorfällen nach Kritikalität. Ihr Incident-Management verwendet andere Kategorien. Welche Ihrer „High-Priority"-Tickets sind DORA-meldepflichtig? Das müssen Sie fachlich bewerten.

KI-gestützte Zulieferung als Lösung

Hier hilft KI-gestützte Datenaufbereitung. Machine Learning analysiert Ihre Datenbestände, normalisiert sie und identifiziert DORA-relevante Informationen. Natural Language Processing erschließt unstrukturierte Daten aus Incident-Reports.

Die KI lernt dabei aus Ihren Datenstrukturen und erkennt Muster in Systembezeichnungen. Sie schlägt DORA-Klassifikationen und Zuordnungen zu DPM-Kategorien vor. Die KI kombiniert Informationen aus verschiedenen Quellsystemen und bereitet konsistente Datensätze vor.

Aber: Die KI liefert nur zu. Die finale Bewertung und Freigabe bleibt Aufgabe Ihrer IT-GRC-Teams. KI bereitet vor, Ihre Experten entscheiden. Dieser Ansatz verbindet Effizienz mit Compliance-Sicherheit.

Der Ansatz
KI bereitet vor, Ihre Experten entscheiden. Dieser Ansatz verbindet Effizienz mit Compliance-Sicherheit.

Tool-unabhängiger Ansatz

Wir arbeiten mit Ihren bestehenden Systemen. Nutzen Sie ServiceNow? Wir nutzen deren DORA-Features optimal und liefern die richtigen Daten zu. Setzen Sie andere ITSM-Tools und EAM-Werkzeuge ein? Auch gut – wir konfigurieren diese für DORA-Compliance. Haben Sie noch kein zentrales ITSM oder kennen Architekturen nur aus Visio? Dann entwickeln wir eine passende Lösung.

Das Tool ist Mittel zum Zweck. Entscheidend ist die richtige Interpretation der DORA-Anforderungen und deren Umsetzung in Ihrer IT-Landschaft.

Warum Expertise den Unterschied macht

DORA ist primär ein Compliance-Projekt. Die fachlichen Anforderungen stehen zwar im Mittelpunkt, deren Umsetzung profitiert jedoch von KI-gestützter Datenaufbereitung.

Standard-Tool-Anbieter decken nur Teilbereiche ab. Systemintegratoren hingegen können Daten verknüpfen, aber kennen DORA-Anforderungen nicht. Compliance-Berater wiederum verstehen die Verordnung, können sie meist aber technisch nicht umsetzen.

Alleinstellungsmerkmal
Standard-Tool-Anbieter erklären Features, aber nicht die regulatorischen Hintergründe. Wir können beides.

Ein Beispiel: DORA fordert die Überwachung „kritischer ICT-Systeme". Was ist kritisch? Das hängt von Ihrer IT-Architektur ab. Wie überwachen Sie diese? Das hängt von Ihren Geschäftsprozessen ab. Beides müssen Sie verstehen und verknüpfen.

Unser dreistufiges Vorgehen

Phase 1: DORA-Readiness-Analyse
Welche Ihrer IT-Systeme sind DORA-relevant?
Wo liegen die größten Compliance-Lücken?
Welche Daten sammeln Sie bereits, welche fehlen?
Diese Analyse führen unsere DORA-Spezialisten mit Ihren Stakeholdern durch.

Phase 2: KI-gestützte Datenaufbereitung
Wir integrieren Legacy-Daten in Ihre ITSM-Tools oder neue Lösungen. KI bereitet Daten vor und schlägt DORA-Klassifikationen vor. Ihre Experten prüfen und entscheiden.

Phase 3: Kontinuierliche Datenaufbereitung
DORA-Compliance ist ein laufender Prozess. Wir sorgen dafür, dass Ihre Compliance-Prozesse mit regulatorischen Änderungen und IT-Entwicklungen Schritt halten.

Investition und Nutzen

DORA-Compliance ohne richtige Strategie ist teuer und riskant. Falsche Tool-Entscheidungen müssen später korrigiert werden. Unvollständige Datenintegration führt zu manuellen Nacharbeiten.

Unsere DORA-Expertise reduziert diese Risiken erheblich. Sie treffen von Anfang an die richtigen Entscheidungen für Tools, Prozesse und Datenintegration.

Die Investition in professionelle DORA-Beratung amortisiert sich durch vermiedene Fehlentscheidungen und effiziente Prozesse. Richtig umgesetzte DORA-Compliance kostet langfristig deutlich weniger als nachgebesserte Lösungen.

Unser dreistufiges Vorgehen

Ihr Weg zur sicheren DORA-Compliance

Beginnen Sie mit dem Verständnis der Anforderungen, nicht mit Tool-Experimenten. Wir analysieren Ihre aktuelle DORA-Readiness und zeigen konkrete Handlungsfelder auf.

Dann entwickeln wir eine Compliance-Strategie, die zu Ihrer IT-Landschaft passt. KI unterstützt dabei die Datenaufbereitung, Ihre IT-GRC-Teams treffen die fachlichen Entscheidungen. Die Reihenfolge stimmt: Erst verstehen, dann umsetzen.

DORA-Compliance ist komplex, aber machbar – mit dem richtigen Partner an Ihrer Seite:
Materna – DORA verstehen, intelligent umsetzen.

Ihr Kontakt im #TeamMaterna

Bernd Lohmeyer
Insurance Transformation Strategist
bernd.lohmeyer@materna.group
Tel. +49 162 230 41 44

So erreichen Sie uns:

Materna Information & Communications SE
Robert-Schuman-Straße 20, 44263 Dortmund
Tel.: + 49 231 - 5599 - 00
E-Mail: marketing@materna.group
www.materna.de