Digitale operationelle Resilienz

Maurus Fässler, M.A. HSG Banking and Finance

Die Verordnung über die digitale operationelle Resilienz (DORA) ist seit dem 17. Januar 2025 anwendbar. Sie setzt für Finanzmarktakteure in Europa einen verbindlichen Standard, wie mit ICT-Risiken, Cybervorfällen und Abhängigkeiten von Dienstleistern umzugehen ist. Auch Organisationen in der Schweiz, die direkt oder indirekt mit EU-Instituten, -Kunden oder -Dienstleistern verbunden sind, kommen an DORA nicht vorbei. Wichtig ist: DORA ist weniger ein IT-Projekt als vielmehr ein Organisationssystem – mit klaren Aufgaben für Verwaltungsrat, Geschäftsleitung, Fachbereiche, IT und Beschaffung.

Schweizer Unternehmen sind über mehrere Kanäle betroffen: EU-Niederlassungen und -Tochtergesellschaften unterstehen DORA unmittelbar; grenzüberschreitende Wertschöpfungsketten, Outsourcing und Cloud-Nutzung übertragen De-facto-Standards auch ohne direkte Aufsicht. Zudem schliesst DORA wichtige Lücken in bestehenden Rahmenwerken (z. B. stärkeres Augenmerk auf Registerführung, Tests und Aufsicht über kritische ICT-Drittanbieter). Wer heute «DORA-ready» ist, gewinnt Resilienz, Auditfähigkeit und Partnerfähigkeit.

Die fünf Bestandteile von DORA in der Praxis

1. **ICT Risk Management Framework (ICT-RMF)**
   Kern ist ein durchgängiger Zyklus aus Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen und Lernen – verankert in Governance und Kultur. Der Verwaltungsrat ist adressiert: Resilienz ist Chefsache, nicht nur Technik. In der Praxis bewährt sich ein kompaktes Kontrollset (z. B. Asset-/Service-Inventar, Schutzprofile, Detektions-Schwellen, Reaktionshandbuch, Wiederanlaufpläne etc.) mit klaren Verantwortlichkeiten.

2. **Incident Reporting**
   Schwere ICT-Störungen sind an die Aufsicht zu melden (Erstmeldung, Zwischenberichte, Abschlussbericht). Dafür braucht es definierte Schwellwerte, Eskalationswege und eine 24/7-Rolle als «Incident Commander». Intern zählt Geschwindigkeit, aber auch die Qualität der Evidenzen (Zeitleisten, Log-Exzerpte, Entscheidungen).

3. **Digital Operational Resilience Testing**
   Neben regelmässigen technischen Tests spielt die realistische Simulation von Angriffen (Threat-Led Penetration Testing, TLPT) eine zunehmende Rolle. Grosse oder risikoreiche Institute müssen solche Tests periodisch durchführen; kleinere Organisationen profitieren von Tabletop-Übungen mit GL/VR-Beteiligung. Entscheidend ist ein wohldosierter Mix: von Patch-Basics über Red-Teaming bis zur Krisenstabsprobe.

4. **Third-Party Risk Management (TPRM)**
   DORA verlangt eine neue Qualität in der Steuerung von ICT-Dienstleistern: ein Informationsregister für alle Services, vertragliche Mindestinhalte (Audit-/Zugriffsrechte, Exit-Readiness, Datenportabilität) und eine Stärkung der Aufsicht über kritische Dienstleister. Praktisch heisst das: Lieferantenklassifizierung und -management, Konzentrationsrisiken messen, Übergangs- und Ausstiegspläne vorbereiten.

5. **Informationsaustausch**
   Der freiwillige Austausch zu Bedrohungen und Schwachstellen erhöht die kollektive Widerstandsfähigkeit. Wer aktiv teilnimmt, profitiert frühzeitig von Mustern und Indikatoren.

Vorgehen für die «DORA-Readiness»

«DORA-Readiness» beginnt mit einem klaren Mandat aus dem Verwaltungsrat. Ziel, Geltungsbereich und Risikobild werden zu Beginn präzisiert, damit Umfang und Ambition stimmen. Ein kompaktes Programm setzt Verantwortlichkeiten und Entscheidungspfade fest, verankert die Rolle der Geschäftsleitung und definiert die Schnittstellen zu Fachbereichen, IT, Beschaffung und Recht. Bestehende Richtlinien werden aktualisiert, sodass Meldewege, Testfrequenzen und die Steuerung von ICT-Drittparteien verbindlich geregelt sind.

Den Kern bildet ein zentrales Register aller ICT-Services als verlässliche Datenquelle. Es erfasst für jeden Service die verantwortliche Person, den Zweck, Datenklassen, das Betriebsmodell (On-Prem/Cloud), Provider und Sub-Provider, Betriebsstandorte, vertragliche Grundlagen, Service Levels, Exit-Klauseln und kritische Abhängigkeiten. Parallel wird ein Evidenzmodell definiert: Welche Nachweise entstehen in welchem System, wie werden sie versioniert, aufbewahrt und für Audits verfügbar gemacht? So entsteht von Anfang an Nachweisfähigkeit, statt Nachweise hinterher mühselig zusammenzutragen.

Auf dieser Grundlage wird das Incident-Management geschärft. Schwellwerte und Klassifizierungen sind so formuliert, dass schwere Ereignisse zuverlässig erkannt und unverzüglich eskaliert werden. Eine durchgehende Führungsrolle – häufig als «Incident Commander» bezeichnet – steuert die Lage, koordiniert Technik, Fachbereiche, Recht und Kommunikation und dokumentiert Entscheidungen. Standardisierte Kommunikationsbausteine für Kunden, Partner, Aufsicht und Medien sowie eine 24/7-Einsatzbereitschaft schaffen Tempo und Konsistenz, ohne die Qualität der Evidenzen zu gefährden.

Die Widerstandsfähigkeit wird durch einen risikobasierten Testansatz belegt. Neben regelmässigen technischen Prüfungen umfasst er realitätsnahe Tabletop-Übungen mit der Geschäftsleitung und – wo sinnvoll – Threat-Led Penetration Testing. Der Jahresplan orientiert sich an Kritikalität und Veränderung: je höher die Abhängigkeit, desto dichter die Prüffrequenz. Erkenntnisse fliessen unmittelbar in Härtungsmassnahmen, das Change-Management und Architekturvorgaben zurück; so wird Resilienz nicht nur gemessen, sondern iterativ erhöht.

Die Steuerung von Drittparteien wird vom einmaligen Einkaufsakt zur laufenden Führungsaufgabe. Eine konsistente Klassifizierung der Lieferanten macht Konzentrations- und Substitutionsrisiken sichtbar. Verträge werden systematisch auf DORA-Mindestinhalte geprüft – Audit- und Zugriffsrechte, Datenportabilität, Ausstiegsfristen und Business-Continuity-Verpflichtungen – und bei kritischen Lücken nachverhandelt. Für die wichtigsten Provider werden Exit-Szenarien konkretisiert, inklusive Test-Extraktionen von Daten und einer klaren Zuordnung von Verantwortlichkeiten.

Damit DORA-Readiness nicht versandet, wird sie im Regelbetrieb verankert. Schulungen für Service-Manager, Projektleitende und Beschaffung schaffen ein gemeinsames Begriffs- und Rollenverständnis. Wenige, aussagekräftige Metriken – etwa MTTR, die Vollständigkeit und Aktualität des Registers, ein Lieferanten-Konzentrationsindex sowie die Test-Coverage – speisen ein regelmässiges Reporting an Geschäftsleitung und Verwaltungsrat. Lessons Learned aus Vorfällen und Übungen werden verbindlich nachgeführt, sodass das Resilienzniveau messbar steigt. Die Umsetzung bleibt anschlussfähig an bestehende Schweizer Vorgaben (z. B. FINMA-RS 18/3) und fördert gleichzeitig die Durchgängigkeit, die DORA verlangt.

Fazit

Viele Schweizer Institute haben mit Outsourcing- und Informationssicherheitsvorgaben bereits eine gute Basis. DORA fordert die Durchgängigkeit: ein zentrales Register statt verstreuter Listen, ein abgestimmter Testplan statt ad-hoc-Pen-Tests, vertraglich geregelte Aufsichts- und Auditrechte bei kritischen ICT-Dienstleistern. «Exit-Readiness» verbleibt nicht als Fussnote, sondern als konkretes Szenario. Damit steigen die Auditfähigkeit und die Reaktionsgeschwindigkeit im Ernstfall.

DORA ist kein Selbstzweck. Wer die Anforderungen als Designprinzip nutzt, gewinnt nicht nur Compliance, sondern robuste Abläufe, kürzere Ausfallzeiten und vertrauenswürdige Partnerschaften. Für Schweizer Organisationen ist 2025 auch das Jahr, in dem sich Resilienz messen und trainieren lässt: mit einem sauberen Register, klaren Rollen, harten Tests und gelebter Zusammenarbeit.