RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPÄISCHES BANKING & FINANZMÄRKTE

Wenn Ihr kritischer ICT-Provider morgen ausfällt: Was steht still — und wie lange?

Ein Board Briefing Report zu DORA, ICT-Drittparteienrisiko, Exit-Fähigkeit und operativer Resilienz.

Reza Monshizadeh · Monshizadeh.com · 7 Min. Lesezeit

01 SITUATION

EIN HYPOTHETISCHES BOARD-SZENARIO

Es geht nicht mehr nur um den Provider. Es geht um die Kontinuitätskette.

NEHMEN WIR FOLGENDE SITUATION AN

Ein kritischer ICT-Drittanbieter fällt aus. Er unterstützt eine Plattform, einen Datendienst, eine Cloud-Umgebung, eine Workflow Engine, eine Reporting-Schicht oder einen KI-gestützten Prozess des Instituts.

Innerhalb weniger Stunden lautet die Frage nicht mehr, ob der Provider vertraglich verpflichtet ist, den Service wiederherzustellen.

Dieses Szenario ist generisch und hypothetisch. Es beschreibt kein konkretes Institut.

DIE ANSCHLIESSENDE FRAGE

Was steht innerhalb der Bank still?

- Welche kritischen oder wichtigen Funktionen sind betroffen?
- Welche Kunden-, Risiko-, operativen oder entscheidungsbezogenen Ketten hängen vom Provider ab?
- Welche Wiederherstellungszeit wurde tatsächlich getestet?

02 MANAGEMENT SUMMARY

Drei Orientierungspunkte für den Vorstand.

01

DORA macht ICT-Drittparteienrisiko board-relevant

Finanzunternehmen bleiben für Compliance verantwortlich, auch wenn ICT-Services von Drittanbietern erbracht werden. DORA verlangt ICT-Drittparteienrisikomanagement, ein Register of Information und Exit-Strategien für ICT-Services, die kritische oder wichtige Funktionen unterstützen.

02

Kritische Provider sind jetzt eine beaufsichtigte Realität

Die Europäischen Aufsichtsbehörden veröffentlichten am 18. November 2025 die erste Liste von **19 designierten kritischen ICT-Drittanbietern** unter DORA.

03

Antwortqualität zählt

Eine starke Antwort lautet nicht „Wir haben eine Exit-Policy.“ Eine starke Antwort zeigt, was stillsteht, wie lange Recovery dauert, wo Abhängigkeiten zusammenlaufen und welcher Exit-Pfad getestet wurde.

Quelle: DORA-Verordnung (EU) 2022/2554; ESAs CTPP-Designation, 18. November 2025.

03 KALIBRIERUNG DER ANTWORTQUALITÄT

Kontinuitätsstatus, nicht Vertragsstatus.

GRÜN — ENTSCHEIDUNGSFÄHIG

Das aktuelle Register of Information spiegelt tatsächliche ICT-Abhängigkeiten wider.

Kritische Funktionen sind Providern und Services zugeordnet.

Provider-Konzentration und Fourth-Party Chains sind bewertet.

RTO, RPO und maximal tolerierbare Unterbrechung sind je Funktion definiert.

Exit- und Substitutionspfade sind dokumentiert, getestet und überprüft.

Board Reporting zeigt verbleibendes Konzentrationsrisiko und offene Maßnahmen.

GELB — TEILWEISE BELEGT

Ein Register existiert, ist aber nicht vollständig mit der operativen Realität abgeglichen.

Das Mapping auf Business Services ist unvollständig.

Der Exit-Plan ist dokumentiert, aber für kritische Funktionen nicht getestet.

RTOs sind definiert, aber nicht durch Recovery-Übungen nachgewiesen.

Provider-Konzentration wird berichtet, aber nicht in Board-Entscheidungen übersetzt.

Ownership liegt in Procurement oder IT, aber nicht end-to-end.

ROT — NICHT ENTSCHEIDUNGSFÄHIG

„Wir haben eine Exit-Policy.“

„Der Provider wird jetzt direkt unter DORA beaufsichtigt.“

„Das wird von Procurement gesteuert.“

„Der Cloud-Provider hat eigene Resilienzpläne.“

„Der Vertrag enthält SLAs.“

„Wir könnten aussteigen, wenn wir müssten.“

GRÜN ist kein Vertragsstatus. GRÜN ist ein getesteter Kontinuitätsstatus.

04 WER ANTWORTEN MUSS

Procurement kann den Vertrag verantworten. Technology kann die Plattform verantworten. Das Business verantwortet die Auswirkung.

CIO / CTO	Architektur, Plattformen, technische Abhängigkeiten, Recovery Routes und Datenportabilität.
COO	Operative Kontinuität, Business-Service-Auswirkung, Recovery Execution und Contingency Arrangements.
CRO / Operational Risk	Kritikalitätsklassifizierung, verbleibendes Konzentrationsrisiko, Toleranz für Unterbrechung und Risk Acceptance.
CISO / ICT Risk	Security, Resilienz, Incident Response, technische Recovery und Third-Party-Control-Umfeld.
Procurement / Vendor Management	Vertragliche Arrangements, Exit-Klauseln, Audit-Rechte, SLAs, Transition Support und Subcontracting-Transparenz.
Business Owner	Ownership für kritische Funktionen, Entscheidungswirkung, Service-Toleranz und Priorisierung während einer Unterbrechung.
Internal Audit	Unabhängige Prüfung der Abhängigkeitskarte, getesteter Exit-Fähigkeit und Evidenz für Board Reliance.

05 EVIDENZ, DIE DER VORSTAND ANFORDERN SOLLTE

Zehn Artefakte, die eine Antwort überprüfbar machen.

01 **Register of Information**
Zeigt alle ICT-Vertragsarrangements, einschließlich Services, die kritische oder wichtige Funktionen unterstützen.

02 **Critical Function Mapping**
Zeigt, welche Funktionen, Services, Prozesse und Entscheidungsketten von welchem ICT-Provider abhängen.

03 **Provider Criticality Classification**
Zeigt, welche Provider und Services für Kontinuität, Kundenauswirkung und regulatorische Pflichten materiell sind.

04 **Concentration Risk Assessment**
Zeigt, wo mehrere kritische Services von einem Provider oder eng verbundenen Providern abhängen.

05 **Fourth-Party Dependency Map**
Zeigt Subcontractors, Infrastrukturschichten, Rechenzentren, Cloud-Abhängigkeiten und gemeinsame Ausfallpunkte.

06 **RTO / RPO / MTPD View**
Zeigt Recovery Time, Recovery Point und maximal tolerierbare Unterbrechung je kritischer Funktion.

07 **Tested Exit Strategy**
Zeigt, ob Exit oder Substitution geübt wurde — nicht nur dokumentiert.

08 **Contractual Exit & Transition Evidence**
Zeigt Zugang, Audit, Recovery, Rückgabe, Transition Support und Kündigungsrechte.

09 **Incident & Recovery Exercise Log**
Zeigt, was getestet wurde, was fehlgeschlagen ist, was offen blieb und wer Remediation verantwortet.

10 **Board Resilience Dashboard**
Zeigt Provider Exposure, getestete Recovery, verbleibendes Konzentrationsrisiko, offene Issues und formale Risk Acceptance.

06 GOVERNANCE CHECK

WARNSIGNALE DER ANTWORTQUALITÄT

Diese Antworten können in einer Vorstandssitzung beruhigend klingen. Sie sind aber noch nicht entscheidungsfähig.

„Wir haben eine Exit-Policy.“

Eine Policy gibt Richtung vor. Sie zeigt nicht, dass Exit innerhalb der erforderlichen Zeit operativ möglich ist.

„Der Provider wird direkt unter DORA beaufsichtigt.“

CTPP-Oversight stärkt das System. Es überträgt nicht die eigene Verantwortung des Instituts für Resilienz.

„Das wird von Procurement gesteuert.“

Procurement kann den Vertrag managen. Es verantwortet nicht die Auswirkung auf den Business Service.

„Der Exit-Plan ist dokumentiert.“

Ein dokumentierter Exit-Plan ist noch keine getestete Exit-Fähigkeit.

„Der Provider hat starke SLAs.“

Ein SLA ist kein Recovery-Test. Das Board muss wissen, was passiert, wenn das SLA nicht eingehalten wird.

„Wir nutzen mehrere Provider.“

Diversifikation hilft nur dort, wo die Fourth-Party Chain wirklich unabhängig ist.

„Der Service ist nicht kundennah.“

Ein nicht kundennaher Service kann trotzdem Reporting, Risk Control, Settlement, Decisioning oder regulatorische Pflichten unterstützen.

„Wir könnten aussteigen, wenn es notwendig wäre.“

Ein glaubwürdiger Exit braucht Datenportabilität, Transition Support, vertragliche Rechte, getestete Schritte und accountable Owner.

Keine dieser Aussagen ist notwendigerweise falsch. **Sie sind nur keine ausreichende Evidenz für Board-Level Reliance.**

07 PATH TO GREEN

Sechs Bedingungen für einen getesteten Kontinuitätsstatus.

01

Abhängigkeiten sichtbar

Das Register of Information und Service Mapping zeigen, welche Provider welche kritischen oder wichtigen Funktionen unterstützen.

02

Kritikalität klassifiziert

Das Institut kann erklären, welche Abhängigkeiten am wichtigsten sind, warum sie wichtig sind und welche Business Services betroffen wären.

03

Konzentration verstanden

Provider-, Gruppen-, Cloud-, Daten-, Subcontracting- und Fourth-Party-Konzentrationsrisiken werden vor Vertragsabschluss bewertet und nach Onboarding überwacht.

04

Recovery gemessen

RTO, RPO und maximal tolerierbare Unterbrechung sind für kritische Funktionen definiert und getestet, nicht nur geschätzt.

05

Exit ermöglicht

Verträge enthalten Rechte, Übergangsfristen und Recovery Arrangements, die Exit, Migration oder Insourcing unterstützen.

06

Residual Risk gesteuert

Das Board kann sehen, was konzentriert bleibt, was realistisch nicht substituiert werden kann, was akzeptiert wurde und wann diese Akzeptanz überprüft wird.

08 NÄCHSTE FRAGE & QUELLEN

NÄCHSTE FRAGE FÜR DEN VORSTAND

Welche kritische oder wichtige Funktion würde die größte Störung erzeugen, wenn ihr ICT-Provider morgen ausfällt — und können wir den getesteten Recovery-Pfad belegen?

AUSGEWÄHLTE QUELLEN

Regulation (EU) 2022/2554, Digital Operational Resilience Act, Articles 28, 29 and 30.

European Supervisory Authorities, designation of critical ICT third-party providers under DORA, 18 November 2025.

ECB Banking Supervision, Supervisory Priorities 2026–28.

BCBS, Principles for Operational Resilience, 2021.

FSB, Enhancing Third-Party Risk Management and Oversight, 2023.

RM | BOARD BRIEFINGS SERIES

EXECUTIVE QUESTIONS FOR
EUROPEAN BANKING & FINANCIAL MARKETS

Ein beaufsichtigter Provider ist nicht dasselbe wie ein resilientes Institut.

Resilienz beginnt, wenn das Board die Frage stellen kann — und eine Antwort erhält, die gemappt, getestet und steuerbar ist.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com