RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPEAN BANKING & FINANCIAL MARKETS

# If Your Critical ICT Provider Fails Tomorrow, What Stops — and for How Long?

A Board Briefing Report on DORA, ICT third-party risk, exit capability and operational resilience.

**Reza Monshizadeh** · Monshizadeh.com · 7 min read

# 01 SITUATION

A HYPOTHETICAL BOARD SCENARIO

## The question is no longer only the provider. It is the continuity chain.

ASSUME THE FOLLOWING

A critical ICT third-party provider becomes unavailable. It supports a platform, data service, cloud environment, workflow engine, reporting layer or AI-enabled process used by the institution.

Within hours, the question is no longer whether the provider has a contractual obligation to restore service.

This scenario is generic and hypothetical. It does not describe any specific institution.

THE QUESTION THAT FOLLOWS

### What stops inside the bank?

- Which critical or important functions are affected?
- Which client, risk, operational or decision chains depend on the provider?
- What is the tested recovery time?

# 02 MANAGEMENT SUMMARY

## Three orientating facts for the board.

01

### DORA makes ICT third-party risk board-level

Financial entities remain responsible for compliance even when ICT services are provided by third parties. DORA requires ICT third-party risk management, a Register of Information and exit strategies for ICT services supporting critical or important functions.

02

### Critical providers are now a supervised reality

The European Supervisory Authorities published the first list of **19 designated critical ICT third-party providers** under DORA on 18 November 2025.

03

### Answer quality matters

A strong answer is not “we have an exit policy”. A strong answer shows what stops, how long recovery takes, which dependencies converge and which exit path has been tested.

Source: DORA Regulation (EU) 2022/2554; ESAs CTPP designation, 18 November 2025.

# 03 ANSWER QUALITY CALIBRATION

## Continuity status, not contract status.

### GREEN — DECISION-GRADE

Current Register of Information reflects actual ICT dependencies.

Critical functions are mapped to providers and services.

Provider concentration and fourth-party chains are assessed.

RTO, RPO and maximum tolerable disruption are defined by function.

Exit and substitution paths are documented, tested and reviewed.

Board reporting shows residual concentration risk and open actions.

### AMBER — PARTIALLY EVIDENCED

Register exists but is not fully reconciled with operating reality.

Business service mapping is incomplete.

Exit plan is documented, but not tested for critical functions.

RTOs are defined, but not proven through recovery exercises.

Provider concentration is reported, but not translated into board decisions.

Ownership exists in Procurement or IT, but not end-to-end.

### RED — NOT DECISION-GRADE

*“We have an exit policy.”*

*“The provider is now directly overseen under DORA.”*

*“This is managed by Procurement.”*

*“The cloud provider has its own resilience plan.”*

*“The contract includes SLAs.”*

*“We could exit if we had to.”*

**GREEN is not a contract status. GREEN is a tested continuity status.**

# 04 WHO SHOULD ANSWER

**Procurement may own the contract. Technology may own the platform. The business owns the impact.**

| | |
|---|---|
| **CIO / CTO** | Architecture, platforms, technical dependencies, recovery routes and data portability. |
| **COO** | Operational continuity, business service impact, recovery execution and contingency arrangements. |
| **CRO / Operational Risk** | Criticality classification, residual concentration risk, tolerance for disruption and risk acceptance. |
| **CISO / ICT Risk** | Security, resilience, incident response, technical recovery and third-party control environment. |
| **Procurement / Vendor Mgmt** | Contractual arrangements, exit clauses, audit rights, SLAs, transition support and subcontracting visibility. |
| **Business Owner** | Critical function ownership, decision impact, service tolerance and prioritisation during disruption. |
| **Internal Audit** | Independent review of the dependency map, tested exit capability and evidence retained for board reliance. |

# 05 EVIDENCE THE BOARD SHOULD REQUEST

## Ten artefacts that make an answer verifiable.

01 **Register of Information**
All ICT contractual arrangements, including services supporting critical or important functions.

02 **Critical Function Mapping**
Which functions, services, processes and decision chains depend on each ICT provider.

03 **Provider Criticality Classification**
Which providers and services are material to continuity, client impact and regulatory obligations.

04 **Concentration Risk Assessment**
Where multiple critical services depend on one provider or closely connected providers.

05 **Fourth-Party Dependency Map**
Subcontractors, infrastructure layers, data centres, cloud dependencies and shared failure points.

06 **RTO / RPO / MTPD View**
Recovery time, recovery point and maximum tolerable disruption by critical function.

07 **Tested Exit Strategy**
Whether exit or substitution has been exercised, not merely documented.

08 **Contractual Exit & Transition Evidence**
Access, audit, recovery, return, transition support and termination rights.

09 **Incident & Recovery Exercise Log**
What was tested, what failed, what remained open and who owns remediation.

10 **Board Resilience Dashboard**
Provider exposure, tested recovery, residual concentration risk, open issues and formal risk acceptance.

## 06 GOVERNANCE CHECK

WARNING SIGNALS

These answers may sound reassuring in a board meeting. They are not yet decision-grade.

***"We have an exit policy."***

A policy sets direction. It does not show that exit is operationally possible within the required time.

***"The provider is directly overseen under DORA."***

CTPP oversight strengthens the system. It does not transfer the institution's own responsibility for resilience.

***"This is handled by Procurement."***

Procurement can manage the contract. It does not own the business service impact.

***"The exit plan is documented."***

A documented exit plan is not yet a tested exit capability.

***"The provider has strong SLAs."***

An SLA is not a recovery test. The board needs to know what happens when the SLA is missed.

***"We use multiple providers."***

Diversification only helps where the fourth-party chain is genuinely independent.

***"The service is not client-facing."***

It can still support reporting, risk control, settlement, decisioning or regulatory obligations.

***"We could exit if necessary."***

A credible exit needs data portability, transition support, contractual rights, tested steps and accountable owners.

None of these statements is necessarily wrong. **They are simply not sufficient evidence for board-level reliance.**

# 07 PATH TO GREEN

## Six conditions for a tested continuity status.

01

### Dependencies Visible

The Register of Information and service mapping show which providers support which critical or important functions.

02

### Criticality Classified

The institution can explain which dependencies matter most, why they matter and which business services would be affected.

03

### Concentration Understood

Provider, group, cloud, data, subcontracting and fourth-party concentration risks are assessed before commitment and monitored after onboarding.

04

### Recovery Measured

RTO, RPO and maximum tolerable disruption are defined and tested for critical functions, not merely estimated.

05

### Exit Enabled

Contracts include the rights, transition periods and recovery arrangements needed to support exit, migration or insourcing.

06

### Residual Risk Governed

The board can see what remains concentrated, what cannot realistically be substituted, what has been accepted and when that acceptance will be reviewed.

# 08 NEXT QUESTION & SOURCES

SUGGESTED NEXT QUESTION

## Which critical or important function would create the greatest disruption if its ICT provider failed tomorrow — and can we evidence the tested recovery path?

SELECTED SOURCES


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

# A supervised provider is not the same as a resilient institution.

Resilience starts when the board can ask the question — and receive an answer that is mapped, tested and governable.

**Reza Monshizadeh** · Senior Technology Executive · Frankfurt

www.monshizadeh.com