RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPEO & MERCATI FINANZIARI

Se il vostro provider ICT critico cade domani: cosa si ferma — e per quanto tempo?

Un Board Briefing Report su DORA, rischio terze parti ICT, capacità di exit e resilienza operativa.

Reza Monshizadeh · Monshizadeh.com · 7 min di lettura

01 SITUATION

UNO SCENARIO IPOTETICO PER IL BOARD

Il punto non è più solo il provider. Il punto è la catena della continuità.

ASSUMIAMO LA SEGUENTE SITUAZIONE

Un provider terzo ICT critico diventa indisponibile. Supporta una piattaforma, un servizio dati, un ambiente cloud, un workflow engine, un layer di reporting o un processo AI-enabled utilizzato dall'istituzione.

Nel giro di poche ore, la domanda non è più se il provider abbia un obbligo contrattuale di ripristinare il servizio.

Questo scenario è generico e ipotetico. Non descrive alcuna istituzione specifica.

LA DOMANDA CHE NE DERIVA

Cosa si ferma dentro la banca?

- Quali funzioni critiche o importanti sono impattate?
- Quali catene clienti, rischio, operative o decisionali dipendono dal provider?
- Qual è il tempo di recovery realmente testato?

02 MANAGEMENT SUMMARY

Tre punti di orientamento per il board.

01

DORA rende il rischio terze parti ICT board-level

Le entità finanziarie restano responsabili della compliance anche quando i servizi ICT sono forniti da terzi. DORA richiede ICT third-party risk management, un Register of Information e strategie di exit per servizi ICT che supportano funzioni critiche o importanti.

02

I provider critici sono ora una realtà supervisionata

Le Autorità europee di vigilanza hanno pubblicato il 18 novembre 2025 la prima lista di **19 provider terzi ICT critici designati** sotto DORA.

03

La qualità della risposta conta

Una risposta forte non è “we have an exit policy”. Una risposta forte mostra cosa si ferma, quanto dura il recovery, dove convergono le dipendenze e quale exit path è stato testato.

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

03 CALIBRAZIONE DELLA QUALITÀ DELLA RISPOSTA

Status di continuità, non status contrattuale.

GREEN — DECISIONALE

L’attuale Register of Information riflette le dipendenze ICT reali.

Le funzioni critiche sono mappate a provider e servizi.

La concentrazione dei provider e le fourth-party chains sono valutate.

RTO, RPO e interruzione massima tollerabile sono definiti per funzione.

Exit e substitution paths sono documentati, testati e revisionati.

Il board reporting mostra rischio residuo di concentrazione e open actions.

AMBER — PARZIALMENTE DIMOSTRATO

Il registro esiste, ma non è pienamente riconciliato con la realtà operativa.

Il business service mapping è incompleto.

Il piano di exit è documentato, ma non testato per funzioni critiche.

Gli RTO sono definiti, ma non provati attraverso esercizi di recovery.

La concentrazione provider è riportata, ma non tradotta in decisioni del board.

L’ownership esiste in Procurement o IT, ma non end-to-end.

RED — NON DECISIONALE

“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 CHI DEVE RISPONDERE

Procurement può detenere il contratto. Technology può detenere la piattaforma. Il Business detiene l’impatto.

CIO / CTO	Architettura, piattaforme, dipendenze tecniche, recovery routes e portabilità dei dati.
COO	Continuità operativa, impatto sui business services, esecuzione del recovery e contingency arrangements.
CRO / Operational Risk	Classificazione della criticità, rischio residuo di concentrazione, tolleranza all’interruzione e risk acceptance.
CISO / ICT Risk	Security, resilienza, incident response, recovery tecnico e ambiente di controllo terze parti.
Procurement / Vendor Management	Arrangements contrattuali, clausole di exit, diritti di audit, SLAs, transition support e visibilità sul subcontracting.
Business Owner	Ownership della funzione critica, decision impact, tolleranza del servizio e prioritizzazione durante la disruption.
Internal Audit	Revisione indipendente della dependency map, capacità di exit testata ed evidence mantenuta per board reliance.

05 EVIDENZE CHE IL BOARD DOVREBBE RICHIEDERE

Dieci artefatti che rendono una risposta verificabile.

01 **Register of Information**
Tutti gli arrangements contrattuali ICT, inclusi i servizi che supportano funzioni critiche o importanti.

02 **Critical Function Mapping**
Quali funzioni, servizi, processi e catene decisionali dipendono da ciascun provider ICT.

03 **Provider Criticality Classification**
Quali provider e servizi sono materiali per continuità, impatto cliente e obblighi regolamentari.

04 **Concentration Risk Assessment**
Dove più servizi critici dipendono da un unico provider o da provider strettamente collegati.

05 **Fourth-Party Dependency Map**
Subcontractors, layer infrastrutturali, data centres, dipendenze cloud e punti di failure condivisi.

06 **RTO / RPO / MTPD View**
Recovery time, recovery point e interruzione massima tollerabile per funzione critica.

07 **Tested Exit Strategy**
Se exit o substitution sono stati esercitati, non solo documentati.

08 **Contractual Exit & Transition Evidence**
Accesso, audit, recovery, restituzione, transition support e diritti di termination.

09 **Incident & Recovery Exercise Log**
Cosa è stato testato, cosa è fallito, cosa è rimasto aperto e chi owns la remediation.

10 **Board Resilience Dashboard**
Provider exposure, recovery testato, rischio residuo di concentrazione, open issues e risk acceptance formale.

06 GOVERNANCE CHECK

SEGNALI DI ALLERTA SULLA QUALITÀ DELLA RISPOSTA

Queste risposte possono sembrare rassicuranti in una riunione del board. Non sono ancora decision-grade.

"We have an exit policy."

Una policy dà direzione. Non mostra che l'exit sia operativamente possibile entro il tempo richiesto.

"The provider is directly overseen under DORA."

L'oversight CTPP rafforza il sistema. Non trasferisce la responsabilità dell'istituzione per la resilienza.

"This is handled by Procurement."

Procurement può gestire il contratto. Non owns l'impatto sul business service.

"The exit plan is documented."

Un exit plan documentato non è ancora una capacità di exit testata.

"The provider has strong SLAs."

Un SLA non è un recovery test. Il board deve sapere cosa succede quando lo SLA non viene rispettato.

"We use multiple providers."

La diversificazione aiuta solo dove la fourth-party chain è realmente indipendente.

"The service is not client-facing."

Un servizio non client-facing può comunque supportare reporting, risk control, settlement, decisioning o obblighi regolamentari.

"We could exit if necessary."

Un exit credibile richiede portabilità dei dati, transition support, diritti contrattuali, passaggi testati e accountable owners.

Nessuna di queste affermazioni è necessariamente falsa. **Semplicemente, non costituiscono evidence sufficiente per board-level reliance.**

07 PATH TO GREEN

Sei condizioni per uno status di continuità testato.

01

Dipendenze visibili

Il Register of Information e il service mapping mostrano quali provider supportano quali funzioni critiche o importanti.

02

Criticità classificata

L'istituzione può spiegare quali dipendenze contano di più, perché contano e quali business services sarebbero impattati.

03

Concentrazione compresa

I rischi di concentrazione provider, gruppo, cloud, dati, subcontracting e fourth-party sono valutati prima dell'impegno e monitorati dopo onboarding.

04

Recovery misurato

RTO, RPO e interruzione massima tollerabile sono definiti e testati per funzioni critiche, non solo stimati.

05

Exit abilitato

I contratti includono diritti, periodi di transition e recovery arrangements necessari per supportare exit, migration o insourcing.

06

Rischio residuo governato

Il board può vedere cosa resta concentrato, cosa non può realisticamente essere sostituito, cosa è stato accettato e quando tale accettazione sarà rivista.

08 DOMANDA SUCCESSIVA & FONTI

DOMANDA SUCCESSIVA PER IL BOARD

Quale funzione critica o importante creerebbe la maggiore disruption se il suo provider ICT cadesse domani — e possiamo dimostrare il recovery path testato?

FONTI SELEZIONATE

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

Un provider supervisionato non è la stessa cosa di un’istituzione resiliente.

La resilienza inizia quando il board può porre la domanda — e ricevere una risposta mappata, testata e governabile.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com