RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANCA EUROPEA & MERCADOS FINANCIEROS

Si su proveedor ICT crítico falla mañana: ¿qué se detiene — y durante cuánto tiempo?

Un Board Briefing Report sobre DORA, riesgo de terceros ICT, capacidad de exit y resiliencia operativa.

Reza Monshizadeh · Monshizadeh.com · 7 min de lectura

01 SITUATION

UN ESCENARIO HIPOTÉTICO PARA EL BOARD

La cuestión ya no es solo el proveedor. La cuestión es la cadena de continuidad.

SUPONGAMOS LA SIGUIENTE SITUACIÓN

Un proveedor tercero ICT crítico deja de estar disponible. Soporta una plataforma, un servicio de datos, un entorno cloud, un workflow engine, una capa de reporting o un proceso AI-enabled utilizado por la institución.

En cuestión de horas, la pregunta ya no es si el proveedor tiene una obligación contractual de restaurar el servicio.

Este escenario es genérico e hipotético. No describe ninguna institución específica.

LA PREGUNTA QUE SIGUE

¿Qué se detiene dentro del banco?

- ¿Qué funciones críticas o importantes se ven afectadas?
- ¿Qué cadenas de clientes, riesgo, operativas o decisionales dependen del proveedor?
- ¿Cuál es el tiempo de recovery realmente probado?

02 MANAGEMENT SUMMARY

Tres puntos de orientación para el board.

01

DORA convierte el riesgo de terceros ICT en board-level

Las entidades financieras siguen siendo responsables de la compliance incluso cuando los servicios ICT son prestados por terceros. DORA exige gestión del riesgo de terceros ICT, un Register of Information y estrategias de exit para servicios ICT que soportan funciones críticas o importantes.

02

Los proveedores críticos son ahora una realidad supervisada

Las Autoridades Europeas de Supervisión publicaron el 18 de noviembre de 2025 la primera lista de **19 proveedores terceros ICT críticos designados** bajo DORA.

03

La calidad de la respuesta importa

Una respuesta fuerte no es “we have an exit policy”. Una respuesta fuerte muestra qué se detiene, cuánto tarda el recovery, dónde convergen las dependencias y qué exit path ha sido probado.

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

03 CALIBRACIÓN DE LA CALIDAD DE RESPUESTA

Estado de continuidad, no estado contractual.

GREEN — DECISION-GRADE

El Register of Information actual refleja las dependencias ICT reales.

Las funciones críticas están mapeadas a proveedores y servicios.

La concentración de proveedores y las fourth-party chains están evaluadas.

RTO, RPO y máxima interrupción tolerable están definidos por función.

Los exit y substitution paths están documentados, probados y revisados.

El board reporting muestra riesgo residual de concentración y acciones abiertas.

AMBER — PARCIALMENTE DEMOSTRADO

El registro existe, pero no está completamente reconciliado con la realidad operativa.

El business service mapping es incompleto.

El exit plan está documentado, pero no probado para funciones críticas.

Los RTO están definidos, pero no probados mediante ejercicios de recovery.

La concentración de proveedores se reporta, pero no se traduce en decisiones del board.

El ownership existe en Procurement o IT, pero no end-to-end.

RED — NO 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 QUIÉN DEBE RESPONDER

Procurement puede poseer el contrato. Technology puede poseer la plataforma. El Business posee el impacto.

CIO / CTO	Arquitectura, plataformas, dependencias técnicas, recovery routes y portabilidad de datos.
COO	Continuidad operativa, impacto en business services, ejecución del recovery y contingency arrangements.
CRO / Operational Risk	Clasificación de criticidad, riesgo residual de concentración, tolerancia a la interrupción y risk acceptance.
CISO / ICT Risk	Security, resiliencia, incident response, recovery técnico y entorno de control de terceros.
Procurement / Vendor Management	Arrangements contractuales, cláusulas de exit, derechos de auditoría, SLAs, transition support y visibilidad sobre subcontracting.
Business Owner	Ownership de función crítica, decision impact, tolerancia del servicio y priorización durante la interrupción.
Internal Audit	Revisión independiente de la dependency map, capacidad de exit probada y evidence retenida para board reliance.

05 EVIDENCIA QUE EL BOARD DEBERÍA SOLICITAR

Diez artefactos que hacen verificable una respuesta.

01 **Register of Information**
Todos los arrangements contractuales ICT, incluidos los servicios que soportan funciones críticas o importantes.

02 **Critical Function Mapping**
Qué funciones, servicios, procesos y cadenas decisionales dependen de cada proveedor ICT.

03 **Provider Criticality Classification**
Qué proveedores y servicios son materiales para continuidad, impacto cliente y obligaciones regulatorias.

04 **Concentration Risk Assessment**
Dónde múltiples servicios críticos dependen de un único proveedor o de proveedores estrechamente conectados.

05 **Fourth-Party Dependency Map**
Subcontractors, capas de infraestructura, data centres, dependencias cloud y puntos de fallo compartidos.

06 **RTO / RPO / MTPD View**
Recovery time, recovery point y máxima interrupción tolerable por función crítica.

07 **Tested Exit Strategy**
Si exit o substitution han sido ejercitados, no solo documentados.

08 **Contractual Exit & Transition Evidence**
Acceso, auditoría, recovery, devolución, transition support y derechos de termination.

09 **Incident & Recovery Exercise Log**
Qué fue probado, qué falló, qué permaneció abierto y quién owns la remediation.

10 **Board Resilience Dashboard**
Provider exposure, recovery probado, riesgo residual de concentración, open issues y risk acceptance formal.

06 GOVERNANCE CHECK

SEÑALES DE ALERTA SOBRE LA CALIDAD DE RESPUESTA

Estas respuestas pueden sonar tranquilizadoras en una reunión del board. Todavía no son decision-grade.

"We have an exit policy."

Una policy marca dirección. No muestra que el exit sea operacionalmente posible dentro del tiempo requerido.

"The provider is directly overseen under DORA."

La supervisión CTPP fortalece el sistema. No transfiere la responsabilidad propia de la institución por la resiliencia.

"This is handled by Procurement."

Procurement puede gestionar el contrato. No owns el impacto sobre el business service.

"The exit plan is documented."

Un exit plan documentado todavía no es una capacidad de exit probada.

"The provider has strong SLAs."

Un SLA no es un recovery test. El board necesita saber qué ocurre cuando el SLA no se cumple.

"We use multiple providers."

La diversificación solo ayuda cuando la fourth-party chain es genuinamente independiente.

"The service is not client-facing."

Un servicio no client-facing puede seguir soportando reporting, risk control, settlement, decisioning u obligaciones regulatorias.

"We could exit if necessary."

Un exit creíble necesita portabilidad de datos, transition support, derechos contractuales, pasos probados y accountable owners.

Ninguna de estas afirmaciones es necesariamente falsa. **Simplemente no constituyen evidence suficiente para board-level reliance.**

07 PATH TO GREEN

Seis condiciones para un estado de continuidad probado.

01

Dependencias visibles

El Register of Information y el service mapping muestran qué proveedores soportan qué funciones críticas o importantes.

02

Criticidad clasificada

La institución puede explicar qué dependencias importan más, por qué importan y qué business services se verían afectados.

03

Concentración entendida

Los riesgos de concentración de proveedor, grupo, cloud, datos, subcontracting y fourth-party se evalúan antes del compromiso y se monitorizan tras onboarding.

04

Recovery medido

RTO, RPO y máxima interrupción tolerable están definidos y probados para funciones críticas, no solo estimados.

05

Exit habilitado

Los contratos incluyen los derechos, períodos de transition y recovery arrangements necesarios para soportar exit, migration o insourcing.

06

Riesgo residual gobernado

El board puede ver qué permanece concentrado, qué no puede sustituirse de forma realista, qué ha sido aceptado y cuándo será revisada esa aceptación.

08 SIGUIENTE PREGUNTA & FUENTES

SIGUIENTE PREGUNTA PARA EL BOARD

¿Qué función crítica o importante crearía la mayor disruption si su proveedor ICT fallara mañana — y podemos demostrar el recovery path probado?

FUENTES SELECCIONADAS

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 proveedor supervisado no es lo mismo que una institución resiliente.

La resiliencia empieza cuando el board puede hacer la pregunta — y recibir una respuesta mapeada, probada y gobernable.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com