RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPÉEN & MARCHÉS FINANCIERS

Si votre fournisseur ICT critique tombe demain : qu’est-ce qui s’arrête — et pour combien de temps ?

Un Board Briefing Report sur DORA, le risque tiers ICT, la capacité d’exit et la résilience opérationnelle.

Reza Monshizadeh · Monshizadeh.com · 7 min de lecture

01 SITUATION

UN SCÉNARIO HYPOTHÉTIQUE DE BOARD

La question n’est plus seulement le fournisseur. La question est la chaîne de continuité.

SUPPOSONS LA SITUATION SUIVANTE

Un fournisseur tiers ICT critique devient indisponible. Il soutient une plateforme, un service de données, un environnement cloud, un moteur de workflow, une couche de reporting ou un processus assisté par IA utilisé par l’institution.

En quelques heures, la question n’est plus de savoir si le fournisseur a une obligation contractuelle de restaurer le service.

Ce scénario est générique et hypothétique. Il ne décrit aucune institution spécifique.

LA QUESTION QUI SUIT

Qu’est-ce qui s’arrête à l’intérieur de la banque ?

- Quelles fonctions critiques ou importantes sont affectées ?
- Quelles chaînes client, risque, opérationnelles ou décisionnelles dépendent du fournisseur ?
- Quel est le temps de récupération réellement testé ?

02 MANAGEMENT SUMMARY

Trois points d’orientation pour le board.

01

DORA rend le risque tiers ICT board-level

Les entités financières restent responsables de leur conformité même lorsque les services ICT sont fournis par des tiers. DORA exige une gestion du risque tiers ICT, un Register of Information et des stratégies d’exit pour les services ICT soutenant des fonctions critiques ou importantes.

02

Les fournisseurs critiques sont désormais une réalité supervisée

Les Autorités européennes de surveillance ont publié le 18 novembre 2025 la première liste de **19 fournisseurs tiers ICT critiques désignés** sous DORA.

03

La qualité de la réponse compte

Une réponse forte n’est pas « we have an exit policy ». Une réponse forte montre ce qui s’arrête, combien de temps dure la récupération, où les dépendances convergent et quel exit path a été testé.

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

03 CALIBRATION DE LA QUALITÉ DE RÉPONSE

Statut de continuité, pas statut contractuel.

GREEN — DÉCISIONNEL

Le Register of Information actuel reflète les dépendances ICT réelles.

Les fonctions critiques sont mappées aux fournisseurs et services.

La concentration fournisseur et les fourth-party chains sont évaluées.

RTO, RPO et interruption maximale tolérable sont définis par fonction.

Les exit et substitution paths sont documentés, testés et revus.

Le board reporting montre le risque résiduel de concentration et les actions ouvertes.

AMBER — PARTIELLEMENT DÉMONTRÉ

Le registre existe, mais n'est pas entièrement réconcilié avec la réalité opérationnelle.

Le business service mapping est incomplet.

Le plan d'exit est documenté, mais non testé pour les fonctions critiques.

Les RTO sont définis, mais non prouvés par des exercices de recovery.

La concentration fournisseur est reportée, mais non traduite en décisions du board.

L'ownership existe en Procurement ou IT, mais pas end-to-end.

RED — NON DÉCISIONNEL

« 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 QUI DOIT RÉPONDRE

Procurement peut détenir le contrat. Technology peut détenir la plateforme. Le Business détient l’impact.

CIO / CTO	Architecture, plateformes, dépendances techniques, recovery routes et portabilité des données.
COO	Continuité opérationnelle, impact sur les business services, exécution du recovery et arrangements de contingence.
CRO / Operational Risk	Classification de criticité, risque résiduel de concentration, tolérance à l’interruption et risk acceptance.
CISO / ICT Risk	Sécurité, résilience, incident response, recovery technique et environnement de contrôle tiers.
Procurement / Vendor Management	Arrangements contractuels, clauses d’exit, droits d’audit, SLAs, transition support et visibilité sur le subcontracting.
Business Owner	Ownership de fonction critique, impact décisionnel, tolérance du service et priorisation pendant une interruption.
Internal Audit	Revue indépendante de la dependency map, de la capacité d’exit testée et de l’evidence conservée pour la board reliance.

05 PREUVES QUE LE BOARD DEVRAIT DEMANDER

Dix artefacts qui rendent une réponse vérifiable.

01 **Register of Information**
Tous les arrangements contractuels ICT, y compris les services soutenant des fonctions critiques ou importantes.

02 **Critical Function Mapping**
Quelles fonctions, services, processus et chaînes décisionnelles dépendent de chaque fournisseur ICT.

03 **Provider Criticality Classification**
Quels fournisseurs et services sont matériels pour la continuité, l'impact client et les obligations réglementaires.

04 **Concentration Risk Assessment**
Où plusieurs services critiques dépendent d'un seul fournisseur ou de fournisseurs étroitement liés.

05 **Fourth-Party Dependency Map**
Subcontractors, couches d'infrastructure, data centres, dépendances cloud et points de défaillance partagés.

06 **RTO / RPO / MTPD View**
Recovery time, recovery point et interruption maximale tolérable par fonction critique.

07 **Tested Exit Strategy**
Si l'exit ou la substitution a été exercé, et pas seulement documenté.

08 **Contractual Exit & Transition Evidence**
Accès, audit, recovery, restitution, transition support et droits de résiliation.

09 **Incident & Recovery Exercise Log**
Ce qui a été testé, ce qui a échoué, ce qui est resté ouvert et qui détient la remediation.

10 **Board Resilience Dashboard**
Exposition fournisseur, recovery testé, risque résiduel de concentration, points ouverts et risk acceptance formelle.

06 GOVERNANCE CHECK

SIGNAUX D'ALERTE SUR LA QUALITÉ DE RÉPONSE

Ces réponses peuvent sembler rassurantes en réunion de board. Elles ne sont toutefois pas encore décisionnelles.

« We have an exit policy. »

Une policy donne une direction. Elle ne montre pas que l'exit est opérationnellement possible dans le délai requis.

« The provider is directly overseen under DORA. »

L'oversight CTPP renforce le système. Il ne transfère pas la responsabilité propre de l'institution en matière de résilience.

« This is handled by Procurement. »

Procurement peut gérer le contrat. Il ne détient pas l'impact sur le business service.

« The exit plan is documented. »

Un plan d'exit documenté n'est pas encore une capacité d'exit testée.

« The provider has strong SLAs. »

Un SLA n'est pas un recovery test. Le board doit savoir ce qui se passe lorsque le SLA n'est pas tenu.

« We use multiple providers. »

La diversification n'aide que lorsque la fourth-party chain est réellement indépendante.

« The service is not client-facing. »

Un service non client-facing peut tout de même soutenir reporting, risk control, settlement, decisioning ou obligations réglementaires.

« We could exit if necessary. »

Un exit crédible nécessite portabilité des données, transition support, droits contractuels, étapes testées et accountable owners.

Aucune de ces déclarations n'est nécessairement fausse. **Elles ne constituent simplement pas une evidence suffisante pour une board-level reliance.**

07 PATH TO GREEN

Six conditions pour un statut de continuité testé.

01

Dépendances visibles

Le Register of Information et le service mapping montrent quels fournisseurs soutiennent quelles fonctions critiques ou importantes.

02

Criticité classifiée

L'institution peut expliquer quelles dépendances comptent le plus, pourquoi elles comptent et quels business services seraient affectés.

03

Concentration comprise

Les risques de concentration fournisseur, groupe, cloud, données, subcontracting et fourth-party sont évalués avant engagement et monitorés après onboarding.

04

Recovery mesuré

RTO, RPO et interruption maximale tolérable sont définis et testés pour les fonctions critiques, pas seulement estimés.

05

Exit activé

Les contrats incluent les droits, périodes de transition et arrangements de recovery nécessaires pour soutenir exit, migration ou insourcing.

06

Risque résiduel gouverné

Le board peut voir ce qui reste concentré, ce qui ne peut pas être réalistiquement substitué, ce qui a été accepté et quand cette acceptation sera revue.

08 QUESTION SUIVANTE & SOURCES

QUESTION SUIVANTE POUR LE BOARD

Quelle fonction critique ou importante créerait la plus grande disruption si son fournisseur ICT tombait demain — et pouvons-nous démontrer le recovery path testé ?

SOURCES SÉLECTIONNÉES

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 supervisé n’est pas la même chose qu’une institution résiliente.

La résilience commence lorsque le board peut poser la question — et recevoir une réponse mappée, testée et gouvernable.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com