RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPÉEN & MARCHÉS FINANCIERS

Si un incident ICT majeur commence ce soir, qui décide dans la première heure ?

DORA · Major ICT Incidents · Escalation · Reporting · Operational Resilience

Reza Monshizadeh · Monshizadeh.com · 9 min de lecture

01 SITUATION

UN SCÉNARIO HYPOTHÉTIQUE DE BOARD

Un service critique tombe. La cause est inconnue. L’horloge a déjà commencé.

SUPPOSONS LA SITUATION SUIVANTE

Un service ICT critique devient instable tard dans la soirée. Online banking, paiements, risk reporting, trading support, client service, identity access ou un workflow cloud-hosted est affecté.

- **Le provider enquête.**
- **Les updates internes sont incomplets.**
- **Les clients peuvent déjà être affectés.**

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

LA QUESTION QUI SUIT

- **Qui décide ?**
- **Qui escalade ?**
- **Qui communique ?**
- **Qui classifie l’incident avant que le root cause soit connu ?**

02 MANAGEMENT SUMMARY

Trois points d’orientation pour le board.

01

Les ICT Incidents sont des événements de résilience board-level

DORA exige detection, classification, escalation, communication, information du management body et regulatory reporting.

02

Le paysage des incidents est matériel

Le premier aperçu annuel DORA a reporté **3 383 major ICT-related incidents** en 2025. L’impact direct sur clients et transactions était généralement limité; system failures et external events étaient les principaux drivers.

03

Les décisions de première heure comptent

Le rapport initial doit être soumis aussi tôt que possible, dans les **quatre heures** suivant la classification comme major et au plus tard **24 heures** après awareness.

Une réponse forte n’est pas *« we have an incident plan. »* Une réponse forte montre qui décide avant que les faits soient complets.

03 CALIBRATION DE LA QUALITÉ DE RÉPONSE

Decision Capability, pas Incident-Plan Status.

GREEN — DÉCISIONNEL

Les critères de classification sont testés.

Une first-hour decision matrix existe.

L'Incident Commander est nommé par scénario.

La business impact ownership est assignée.

Les DORA reporting triggers sont intégrés.

Les seuils management-body sont définis.

Décisions et hypothèses de war-room sont loggées.

Les fallback communication channels sont testés.

AMBER — PARTIELLEMENT DÉMONTRÉ

Le processus incident existe, mais les first-hour decision rights ne sont pas entièrement testés.

L'escalade technique est claire, mais la business impact ownership est incohérente.

Les critères DORA sont documentés, mais pas intégrés au live decisioning.

La board notification dépend du jugement pendant l'événement.

Les templates existent, mais les fallback channels ne sont pas testés.

RED — NON DÉCISIONNEL

"IT is handling it."

"We are waiting for root cause."

"The provider is still investigating."

"We will inform the board once confirmed as major."

"The incident plan is documented."

"The service owner will know what to do."

"The regulator will be notified if required."

"Clients will be informed after we understand the impact."

GREEN is not an incident-plan status. GREEN is a tested decision-capability status.

04 THE FIRST-HOUR DECISION CHAIN

Detect → Classify → Escalate → Communicate → Recover

01 DETECT

TEST BOARD

Pouvons-nous montrer comment le premier signal devient une accountable incident decision ?

02 CLASSIFY

TEST BOARD

Pouvons-nous classifier severity, criticality et pertinence DORA avant que le root cause soit connu ?

03 ESCALATE

TEST BOARD

Qui est informé, quand, et sur la base de quel seuil ?

04 COMMUNICATE

TEST BOARD

Qui approuve la communication interne, client, provider, regulator et media pendant la première heure ?

05 RECOVER

TEST BOARD

Quel service doit recover en premier, pourquoi, et sous quelle autorité ?

Un incident plan décrit ce qui devrait se passer. **Incident decision capability prouve que l'institution peut agir lorsque les faits sont incomplets.**

05 QUI DOIT RÉPONDRE

Technology peut restaurer le service. Le management body owns l’exigence de résilience.

CIO / CTO	ICT response capability, impact plateforme, technical recovery, tooling et monitoring.
COO	Business service continuity, operational impact et cross-functional recovery execution.
CISO / Cybersecurity	Cyber triage, containment, threat assessment et cyber escalation.
CRO / Operational Risk	Severity, operational risk impact, tolerance alignment et challenge de la response quality.
Business Owner	Business impact, critical function relevance, client impact et recovery prioritisation.
Compliance / Regulatory Reporting	DORA reporting interpretation, competent-authority notification et evidence.
Legal	Regulatory defensibility, client-impact implications et external communication review.
Communications / Client Office	Internal communication, client messaging, media coordination et consistency.
Third-Party Risk / Vendor Mgmt	Provider escalation, contractual incident obligations et dependency evidence.
Internal Audit	Independent review de classification, escalation, evidence, communication et learning.

06 PREUVES QUE LE BOARD DEVRAIT DEMANDER

Dix artefacts qui rendent le first-hour decisioning vérifiable.

01 First-Hour Decision Matrix
Qui décide severity, classification, escalation, communication et notification.

02 DORA Classification Path
Comment les critères clients, downtime, data impact, criticality et economic impact sont appliqués.

03 Incident Command Record
Qui a dirigé, qui a participé, quelles hypothèses et quelles décisions.

04 War-Room Timeline
Detection, classification, escalation, decisions, communication et recovery actions horodatées.

05 Business Impact Assessment
Services affectés, fonctions critiques, client impact, transaction impact et dependency chains.

06 Management-Body Notification Trigger
Quand le management body est informé et comment les follow-up decisions sont suivies.

07 Regulator Notification Evidence
Si l'incident est reportable et comment l'horloge de reporting est gérée.

08 Client & External Communication Protocol
Qui approuve client, counterparty, media et public communication.

09 Provider Escalation & Dependency Log
Provider status, contractual obligations, response times et unresolved questions.

10 Post-Incident Review Pack
Root cause, decision quality, communication effectiveness, control gaps et remediation owners.

07 GOVERNANCE CHECK

SIGNAUX D'ALERTE SUR LA QUALITÉ DE RÉPONSE

Ces réponses peuvent sembler rassurantes. Elles ne sont pas encore décisionnelles.

⚠ ***"IT is handling it."***
IT peut restaurer le service. IT n'owns pas seul business impact, client communication, regulatory classification ou board escalation.

⚠ ***"We are waiting for root cause."***
Le root cause peut arriver plus tard. Classification, escalation et communication peuvent être nécessaires plus tôt.

⚠ ***"The provider is still investigating."***
L'enquête provider ne suspend pas la responsabilité de l'institution.

⚠ ***"Clients will be informed after we understand the impact."***
La communication planning doit commencer avant que l'image finale de l'impact soit complète.

⚠ ***"We will inform the board once confirmed as major."***
Le management body peut avoir besoin d'une early visibility avant la classification finale.

⚠ ***"The incident plan is documented."***
Un plan n'est utile que si rôles, seuils, decision rights et evidence capture ont été testés.

⚠ ***"The regulator will be notified if required."***
L'institution doit montrer qui détermine l'obligation et quand l'horloge de reporting démarre.

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

08 PATH TO GREEN

Six conditions pour une incident decision capability testée.

01 Decision Rights définis

Qui peut classifier, escalader, communiquer, notifier, contain et prioriser pendant la première heure.

02 Impact Path visible

Business impact, client impact, critical function impact, provider dependency et geographic spread peuvent être évalués tôt.

03 DORA Clock contrôlée

Les délais de classification et reporting sont operationalised, owned et evidenced.

04 Communication gouvernée

Internal, client, regulator, provider et media communication suivent des approved decision paths.

05 Evidence conservée

La first-hour timeline, les hypothèses, décisions et communications peuvent être reconstruites.

06 Lessons intégrées

La post-incident review améliore decision quality, escalation, communication et recovery.

QUESTION SUIVANTE POUR LE BOARD

Quel service critique ou important créerait la plus grande pression décisionnelle dans la première heure s'il tombait ce soir — et pouvons-nous démontrer qui décide avant que le root cause soit connu ?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Un incident plan décrit ce qui devrait se passer. Incident decision capability prouve que l’institution peut agir lorsque les faits sont incomplets.

Disciplined uncertainty est le vrai test de l’operational resilience.

SOURCES SÉLECTIONNÉES

DORA — Regulation (EU) 2022/2554.

Commission Delegated Regulation (EU) 2024/1772.

Commission Delegated Regulation (EU) 2025/301.

ESAs — 2025 Report on Major ICT-Related Incidents under DORA.

ECB Banking Supervision — Supervisory Priorities 2026–28.

BCBS — Principles for Operational Resilience.

FSB — Cyber Incident Reporting.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com