RM | REZA MONSHIZADEH

AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT

BANCA EUROPEA & MERCADOS FINANCIEROS

Si un incidente ICT mayor empieza esta noche, ¿quién decide en la primera hora?

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

Reza Monshizadeh · Monshizadeh.com · 9 min de lectura

01 SITUATION

UN ESCENARIO HIPOTÉTICO PARA EL BOARD

Un servicio crítico falla. El root cause es desconocido. El reloj ya ha empezado.

SUPONGAMOS LA SIGUIENTE SITUACIÓN

Un servicio ICT crítico se vuelve inestable tarde por la noche. Online banking, pagos, risk reporting, trading support, client service, identity access o un workflow cloud-hosted está afectado.

- El provider está investigando.
- Los updates internos son incompletos.
- Los clientes pueden estar ya afectados.

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

LA PREGUNTA QUE SIGUE

- ¿Quién decide?
- ¿Quién escala?
- ¿Quién comunica?
- ¿Quién clasifica el incidente antes de que se conozca el root cause?

02 MANAGEMENT SUMMARY

Tres puntos de orientación para el board.

01

Los ICT Incidents son eventos de resiliencia board-level

DORA exige detection, classification, escalation, communication, management-body information y regulatory reporting.

02

El paisaje de incidents es material

El primer annual overview DORA reportó **3.383 major ICT-related incidents** en 2025. El impacto directo en clientes y transacciones fue generalmente limitado; system failures y external events fueron los principales drivers.

03

Las first-hour decisions importan

El initial report debe presentarse lo antes posible, dentro de **cuatro horas** desde la classification as major y no más tarde de **24 horas** desde awareness.

Una respuesta fuerte no es *« we have an incident plan. »* Una respuesta fuerte muestra quién decide antes de que los facts estén completos.

03 CALIBRACIÓN DE LA CALIDAD DE RESPUESTA

Decision Capability, no Incident-Plan Status.

GREEN — DECISION-GRADE

Los criterios de classification están probados.

Existe una first-hour decision matrix.

El Incident Commander está nombrado por escenario.

La business impact ownership está asignada.

Los DORA reporting triggers están embedded.

Los thresholds management-body están definidos.

War-room decisions y assumptions están logged.

Los fallback communication channels están probados.

AMBER — PARCIALMENTE DEMOSTRADO

El proceso incident existe, pero los first-hour decision rights no están completamente probados.

La technical escalation es clara, pero la business impact ownership es inconsistente.

Los criterios DORA están documentados, pero no embedded en live decisioning.

La board notification depende del judgement durante el evento.

Los templates existen, pero los fallback channels no están probados.

RED — NO DECISION-GRADE

“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

¿Podemos mostrar cómo la primera señal se convierte en una accountable incident decision?

02 CLASSIFY

TEST BOARD

¿Podemos clasificar severity, criticality y relevancia DORA antes de que se conozca el root cause?

03 ESCALATE

TEST BOARD

¿Quién es informado, cuándo y sobre la base de qué threshold?

04 COMMUNICATE

TEST BOARD

¿Quién aprueba comunicación interna, client, provider, regulator y media durante la primera hora?

05 RECOVER

TEST BOARD

¿Qué servicio debe recover primero, por qué y bajo qué autoridad?

Un incident plan describe lo que debería ocurrir. **Incident decision capability demuestra que la institución puede actuar cuando los facts son incompletos.**

05 WHO SHOULD ANSWER

Technology may restore the service. The management body owns the resilience expectation.

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

06 EVIDENCE THE BOARD SHOULD REQUEST

Ten artefacts that make first-hour decisioning verifiable.

01 First-Hour Decision Matrix
Who decides severity, classification, escalation, communication and notification.

02 DORA Classification Path
How criteria for clients, downtime, data impact, criticality and economic impact are applied.

03 Incident Command Record
Who led, who attended, what assumptions were used and what decisions were taken.

04 War-Room Timeline
Timestamped detection, classification, escalation, decisions, communication and recovery.

05 Business Impact Assessment
Affected services, critical functions, client impact, transaction impact and dependency chains.

06 Management-Body Notification Trigger
When the management body is informed and how follow-up decisions are tracked.

07 Regulator Notification Evidence
Whether the incident is reportable and how the reporting clock is managed.

08 Client & External Communication Protocol
Who approves client, counterparty, media and public communication.

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

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

07 GOVERNANCE CHECK

WARNING SIGNALS

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

⚠ ***"IT is handling it."***
IT may restore the service. It does not alone own business impact, client communication, regulatory classification or board escalation.

⚠ ***"We are waiting for root cause."***
Root cause may come later. Classification, escalation and communication decisions may be needed earlier.

⚠ ***"The provider is still investigating."***
Provider investigation does not pause the institution's own responsibility.

⚠ ***"Clients will be informed after we understand the impact."***
Communication planning must start before the final impact picture is complete.

⚠ ***"We will inform the board once confirmed as major."***
The management body may need early visibility before final classification.

⚠ ***"The incident plan is documented."***
A plan is useful only if roles, thresholds, decision rights and evidence capture have been tested.

⚠ ***"The regulator will be notified if required."***
The institution must show who determines the requirement and when the reporting clock starts.

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

08 PATH TO GREEN

Six conditions for tested incident decision capability.

01 Decision Rights Defined

Who can classify, escalate, communicate, notify, contain and prioritise during the first hour.

02 Impact Path Visible

Business, client, critical-function impact, provider dependency and geographic spread can be assessed early.

03 DORA Clock Controlled

Classification and reporting time limits are operationalised, owned and evidenced.

04 Communication Governed

Internal, client, regulator, provider and media communication follow approved decision paths.

05 Evidence Retained

The first-hour timeline, assumptions, decisions and communications can be reconstructed.

06 Lessons Embedded

Post-incident review improves decision quality, escalation, communication and recovery.

SUGGESTED NEXT QUESTION

Which critical or important service would create the greatest first-hour decision pressure if it failed tonight — and can we evidence who decides before root cause is known?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

An incident plan describes what should happen. Incident decision capability proves the institution can act when the facts are incomplete.

Disciplined uncertainty is the real test of operational resilience.

SELECTED SOURCES

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