RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPEAN BANKING & FINANCIAL MARKETS

If a Major ICT Incident Starts Tonight, Who Decides in the First Hour?

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

Reza Monshizadeh · Monshizadeh.com · 9 min read

01 SITUATION

A HYPOTHETICAL BOARD SCENARIO

A critical service fails. The root cause is unknown. The clock has already started.

ASSUME THE FOLLOWING

A critical ICT service becomes unstable late in the evening. Online banking, payments, risk reporting, trading support, client service, identity access or a cloud-hosted workflow is affected.

- The provider is investigating.
- Internal updates are incomplete.
- Clients may already be affected.

This scenario is generic and hypothetical. It does not describe any specific institution.

THE QUESTION THAT FOLLOWS

- Who decides?
- Who escalates?
- Who communicates?
- Who classifies the incident before root cause is known?

02 MANAGEMENT SUMMARY

Three orientating facts for the board.

01

ICT incidents are now board-level resilience events

DORA requires incident detection, classification, escalation, communication, management-body information and regulatory reporting.

02

The incident landscape is material

The first DORA annual overview reported **3,383 major ICT-related incidents** in 2025. Direct client and transaction impact was generally limited, while system failures and external events were the main drivers.

03

First-hour decisions matter

The initial report must be submitted as early as possible, within **four hours** from classification as major and no later than **24 hours** from awareness.

A strong answer is not *"we have an incident plan."* A strong answer shows who decides before the facts are complete.

03 ANSWER QUALITY CALIBRATION

Decision capability, not incident-plan status.

GREEN — DECISION-GRADE

- Incident classification criteria are tested.
- First-hour decision matrix exists.
- Incident Commander is named by scenario.
- Business impact ownership is assigned.
- DORA reporting triggers are embedded.
- Management-body thresholds are defined.
- War-room decisions and assumptions are logged.
- Fallback communication channels are tested.

AMBER — PARTIALLY EVIDENCED

- Incident process exists, but first-hour decision rights are not fully tested.
- Technical escalation is clear, but business impact ownership is inconsistent.
- DORA criteria are documented, but not embedded in live decisioning.
- Board notification thresholds depend on judgement during the event.
- Communication templates exist, but fallback channels are not tested.

RED — NOT 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

BOARD TEST

Can we show how the first signal becomes an accountable incident decision?

02 CLASSIFY

BOARD TEST

Can we classify severity, criticality and DORA relevance before root cause is known?

03 ESCALATE

BOARD TEST

Who is informed, by when, and based on which threshold?

04 COMMUNICATE

BOARD TEST

Who approves internal, client, provider, regulator and media communication in the first hour?

05 RECOVER

BOARD TEST

Which service must recover first, why, and under whose authority?

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

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