RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
BANKING EUROPEO & MERCATI FINANZIARI

Se un major ICT incident inizia stanotte, chi decide nella prima ora?

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

Reza Monshizadeh · Monshizadeh.com · 9 min di lettura

01 SITUATION

UNO SCENARIO IPOTETICO PER IL BOARD

Un servizio critico fallisce. Il root cause è sconosciuto. L’orologio è già partito.

ASSUMIAMO LA SEGUENTE SITUAZIONE

Un servizio ICT critico diventa instabile a tarda sera. Online banking, pagamenti, risk reporting, trading support, client service, identity access o un workflow cloud-hosted è impattato.

- **Il provider sta investigando.**
- **Gli update interni sono incompleti.**
- **I clienti potrebbero già essere impattati.**

Questo scenario è generico e ipotetico. Non descrive alcuna istituzione specifica.

LA DOMANDA CHE NE DERIVA

- **Chi decide?**
- **Chi escala?**
- **Chi comunica?**
- **Chi classifica l’incident prima che il root cause sia noto?**

02 MANAGEMENT SUMMARY

Tre punti di orientamento per il board.

01

Gli ICT Incidents sono eventi di resilienza board-level

DORA richiede detection, classification, escalation, communication, management-body information e regulatory reporting.

02

Il panorama degli incidents è materiale

Il primo overview annuale DORA ha riportato **3.383 major ICT-related incidents** nel 2025. L'impatto diretto su clienti e transazioni è stato generalmente limitato; system failures ed external events sono stati i principali driver.

03

Le first-hour decisions contano

L'initial report deve essere presentato il prima possibile, entro **quattro ore** dalla classification as major e non oltre **24 ore** dall'awareness.

Una risposta forte non è *« we have an incident plan. »* Una risposta forte mostra chi decide prima che i fatti siano completi.

03 CALIBRAZIONE DELLA QUALITÀ DELLA RISPOSTA

Decision Capability, non Incident-Plan Status.

GREEN — DECISIONALE

I criteri di classification sono testati.

Esiste una first-hour decision matrix.

L'Incident Commander è nominato per scenario.

La business impact ownership è assegnata.

I DORA reporting triggers sono embedded.

Le soglie management-body sono definite.

War-room decisions e assumptions sono loggati.

I fallback communication channels sono testati.

AMBER — PARZIALMENTE DIMOSTRATO

Il processo incident esiste, ma i first-hour decision rights non sono pienamente testati.

La technical escalation è chiara, ma la business impact ownership è incoerente.

I criteri DORA sono documentati, ma non embedded nel live decisioning.

La board notification dipende dal judgement durante l'evento.

I templates esistono, ma i fallback channels non sono testati.

RED — NON DECISIONALE

"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

Possiamo mostrare come il primo segnale diventa una accountable incident decision?

02 CLASSIFY

TEST BOARD

Possiamo classificare severity, criticality e rilevanza DORA prima che il root cause sia noto?

03 ESCALATE

TEST BOARD

Chi viene informato, entro quando e in base a quale threshold?

04 COMMUNICATE

TEST BOARD

Chi approva comunicazione interna, client, provider, regulator e media durante la prima ora?

05 RECOVER

TEST BOARD

Quale servizio deve recover per primo, perché e sotto quale autorità?

Un incident plan descrive cosa dovrebbe accadere. **Incident decision capability dimostra che l'istituzione può agire quando i fatti sono incompleti.**

05 CHI DEVE RISPONDERE

Technology può ripristinare il servizio. Il management body owns la resilience expectation.

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

06 EVIDENZE CHE IL BOARD DOVREBBE RICHIEDERE

Dieci artefatti che rendono verificabile il first-hour decisioning.

01 First-Hour Decision Matrix
Chi decide severity, classification, escalation, communication e notification.

02 DORA Classification Path
Come sono applicati i criteri per clients, downtime, data impact, criticality ed economic impact.

03 Incident Command Record
Chi ha guidato, chi ha partecipato, quali assumptions e quali decisions.

04 War-Room Timeline
Detection, classification, escalation, decisions, communication e recovery actions con timestamp.

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

06 Management-Body Notification Trigger
Quando il management body è informato e come sono tracciate le follow-up decisions.

07 Regulator Notification Evidence
Se l'incident è reportable e come viene gestito il reporting clock.

08 Client & External Communication Protocol
Chi approva client, counterparty, media e public communication.

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

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

07 GOVERNANCE CHECK

SEGNALI DI ALLERTA SULLA QUALITÀ DELLA RISPOSTA

Queste risposte possono sembrare rassicuranti. Non sono ancora decision-grade.

⚠ ***"IT is handling it."***
IT può ripristinare il servizio. Non owns da sola business impact, client communication, regulatory classification o board escalation.

⚠ ***"We are waiting for root cause."***
Il root cause può arrivare dopo. Classification, escalation e communication possono essere necessarie prima.

⚠ ***"The provider is still investigating."***
L'indagine del provider non sospende la responsabilità dell'istituzione.

⚠ ***"Clients will be informed after we understand the impact."***
La communication planning deve iniziare prima che l'immagine finale dell'impact sia completa.

⚠ ***"We will inform the board once confirmed as major."***
Il management body può avere bisogno di early visibility prima della classification finale.

⚠ ***"The incident plan is documented."***
Un piano è utile solo se roles, thresholds, decision rights ed evidence capture sono stati testati.

⚠ ***"The regulator will be notified if required."***
L'istituzione deve mostrare chi determina il requirement e quando parte il reporting clock.

Nessuna di queste affermazioni è necessariamente falsa. **Semplicemente, non costituiscono evidence sufficiente per board-level reliance.**

08 PATH TO GREEN

Sei condizioni per una incident decision capability testata.

01 Decision Rights definiti

Chi può classify, escalate, communicate, notify, contain e prioritise durante la prima ora.

02 Impact Path visibile

Business impact, client impact, critical function impact, provider dependency e geographic spread possono essere valutati presto.

03 DORA Clock controllato

Classification e reporting time limits sono operationalised, owned ed evidenced.

04 Communication governata

Internal, client, regulator, provider e media communication seguono approved decision paths.

05 Evidence conservata

La first-hour timeline, assumptions, decisions e communications possono essere ricostruite.

06 Lessons embedded

La post-incident review migliora decision quality, escalation, communication e recovery.

DOMANDA SUCCESSIVA PER IL BOARD

Quale servizio critico o importante creerebbe la maggiore first-hour decision pressure se fallisse stanotte — e possiamo dimostrare chi decide prima che il root cause sia noto?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Un incident plan descrive cosa dovrebbe accadere. Incident decision capability dimostra che l’istituzione può agire quando i fatti sono incompleti.

Disciplined uncertainty è il vero test dell’operational resilience.

FONTI SELEZIONATE

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