RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPÄISCHES BANKING & FINANZMÄRKTE

Wenn heute Nacht ein schwerer ICT-Incident beginnt: Wer entscheidet in der ersten Stunde?

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

Reza Monshizadeh · Monshizadeh.com · 9 Min. Lesezeit

01 SITUATION

EIN HYPOTHETISCHES BOARD-SZENARIO

Ein kritischer Service fällt aus. Die Ursache ist unklar. Die Uhr läuft bereits.

NEHMEN WIR FOLGENDE SITUATION AN

Ein kritischer ICT-Service wird spät am Abend instabil. Online-Banking, Zahlungen, Risk Reporting, Trading Support, Client Service, Identity Access oder ein cloud-gehosteter Workflow ist betroffen.

- **Der Provider untersucht noch.**
- **Interne Updates sind unvollständig.**
- **Kunden können bereits betroffen sein.**

Dieses Szenario ist generisch und hypothetisch. Es beschreibt kein konkretes Institut.

DIE ANSCHLIESSENDE FRAGE

- **Wer entscheidet?**
- **Wer eskaliert?**
- **Wer kommuniziert?**
- **Wer klassifiziert den Incident, bevor Root Cause bekannt ist?**

02 MANAGEMENT SUMMARY

Drei Orientierungspunkte für den Vorstand.

01

ICT Incidents sind Board-Level Resilience Events

DORA verlangt Detection, Klassifizierung, Eskalation, Kommunikation, Management-Body-Information und regulatorisches Reporting.

02

Die Incident-Landschaft ist materiell

Der erste jährliche DORA-Überblick berichtete **3.383 major ICT-related incidents** im Jahr 2025. Direkte Auswirkungen auf Kunden und Transaktionen waren generell begrenzt; Systemausfälle und externe Ereignisse waren die Haupttreiber.

03

First-Hour Decisions zählen

Der Initial Report muss so früh wie möglich eingereicht werden, innerhalb von **vier Stunden** ab Klassifizierung als major und spätestens **24 Stunden** ab Awareness.

Eine starke Antwort lautet nicht *„Wir haben einen Incident Plan.“* Eine starke Antwort zeigt, wer entscheidet, bevor die Fakten vollständig sind.

03 KALIBRIERUNG DER ANTWORTQUALITÄT

Decision Capability, nicht Incident-Plan-Status.

GRÜN — ENTSCHEIDUNGSFÄHIG

Incident-Klassifizierungskriterien sind getestet.

First-Hour Decision Matrix existiert.

Incident Commander ist je Szenario benannt.

Business Impact Ownership ist zugewiesen.

DORA Reporting Trigger sind eingebettet.

Management-Body-Schwellen sind definiert.

War-Room-Entscheidungen und Annahmen sind geloggt.

Fallback-Kommunikationskanäle sind getestet.

GELB — TEILWEISE BELEGT

Incident-Prozess existiert, aber First-Hour Decision Rights sind nicht vollständig getestet.

Technische Eskalation ist klar, aber Business Impact Ownership ist uneinheitlich.

DORA-Kriterien sind dokumentiert, aber nicht in Live Decisioning eingebettet.

Board Notification hängt während des Events von situativer Beurteilung ab.

Templates existieren, aber Fallback-Kanäle sind nicht getestet.

ROT — NICHT ENTSCHEIDUNGSFÄHIG

„IT kümmert sich darum.“

„Wir warten auf Root Cause.“

„Der Provider untersucht noch.“

„Wir informieren den Vorstand, sobald es als major bestätigt ist.“

„Der Incident Plan ist dokumentiert.“

„Der Service Owner wird wissen, was zu tun ist.“

„Der Regulator wird informiert, falls erforderlich.“

„Kunden werden informiert, nachdem wir die Auswirkung verstanden haben.“

GRÜN ist kein Incident-Plan-Status. GRÜN ist ein getesteter Decision-Capability-Status.

04 THE FIRST-HOUR DECISION CHAIN

Detect → Classify → Escalate → Communicate → Recover

01 DETECT

BOARD-TEST

Können wir zeigen, wie das erste Signal zu einer accountable Incident Decision wird?

02 CLASSIFY

BOARD-TEST

Können wir Severity, Criticality und DORA-Relevanz klassifizieren, bevor Root Cause bekannt ist?

03 ESCALATE

BOARD-TEST

Wer wird informiert, bis wann und auf Basis welcher Schwelle?

04 COMMUNICATE

BOARD-TEST

Wer genehmigt interne, Kunden-, Provider-, Regulator- und Medienkommunikation während der ersten Stunde?

05 RECOVER

BOARD-TEST

Welcher Service muss zuerst wiederhergestellt werden, warum und unter wessen Autorität?

Ein Incident Plan beschreibt, was passieren sollte. **Incident Decision Capability beweist, dass das Institut handeln kann, wenn Fakten unvollständig sind.**

05 WER ANTWORTEN MUSS

Technology kann den Service wiederherstellen. Das Management Body verantwortet die Resilience Expectation.

CIO / CTO	ICT Response Capability, Plattformauswirkung, technische Recovery, Tooling und Monitoring.
COO	Business Service Continuity, Operational Impact und cross-funktionale Recovery Execution.
CISO / Cybersecurity	Cyber Triage, Containment, Threat Assessment und Cyber-Eskalation.
CRO / Operational Risk	Severity, Operational Risk Impact, Tolerance Alignment und Challenge der Response-Qualität.
Business Owner	Business Impact, Critical Function Relevance, Client Impact und Recovery-Priorisierung.
Compliance / Regulatory Reporting	DORA Reporting Interpretation, Competent-Authority Notification und Evidence.
Legal	Regulatorische Verteidigungsfähigkeit, Client-Impact-Implikationen und Review externer Kommunikation.
Communications / Client Office	Interne Kommunikation, Client Messaging, Media Coordination und Konsistenz.
Third-Party Risk / Vendor Management	Provider-Eskalation, vertragliche Incident-Pflichten und Dependency Evidence.
Internal Audit	Unabhängige Prüfung von Klassifizierung, Eskalation, Evidenz, Kommunikation und Learning.

06 EVIDENZ, DIE DER VORSTAND ANFORDERN SOLLTE

Zehn Artefakte, die First-Hour Decisioning überprüfbar machen.

01 First-Hour Decision Matrix
Wer über Severity, Klassifizierung, Eskalation, Kommunikation und Notification entscheidet.

02 DORA Classification Path
Wie Kriterien für Kunden, Downtime, Data Impact, Criticality und Economic Impact angewendet werden.

03 Incident Command Record
Wer führte, wer nahm teil, welche Annahmen galten und welche Entscheidungen wurden getroffen.

04 War-Room Timeline
Zeitgestempelte Detection, Klassifizierung, Eskalation, Entscheidungen, Kommunikation und Recovery.

05 Business Impact Assessment
Betroffene Services, kritische Funktionen, Client Impact, Transaction Impact und Dependency Chains.

06 Management-Body Notification Trigger
Wann das Management Body informiert wird und wie Follow-up Decisions getrackt werden.

07 Regulator Notification Evidence
Ob der Incident reportable ist und wie die Reporting Clock gesteuert wird.

08 Client & External Communication Protocol
Wer Kunden-, Gegenparteien-, Medien- und öffentliche Kommunikation genehmigt.

09 Provider Escalation & Dependency Log
Provider Status, vertragliche Pflichten, Response Times und ungelöste Fragen.

10 Post-Incident Review Pack
Root Cause, Decision Quality, Kommunikationswirksamkeit, Control Gaps und Remediation Owner.

07 GOVERNANCE CHECK

WARNSIGNALE DER ANTWORTQUALITÄT

Diese Antworten können beruhigend klingen. Sie sind aber noch nicht entscheidungsfähig.

⚠ ***„IT kümmert sich darum.“***
IT kann den Service wiederherstellen. Sie verantwortet aber nicht allein Business Impact, Kundenkommunikation, regulatorische Klassifizierung oder Board-Eskalation.

⚠ ***„Wir warten auf Root Cause.“***
Root Cause kann später kommen. Klassifizierung, Eskalation und Kommunikation können früher nötig sein.

⚠ ***„Der Provider untersucht noch.“***
Provider-Untersuchung pausiert nicht die Verantwortung des Instituts.

⚠ ***„Kunden werden informiert, nachdem wir die Auswirkung verstanden haben.“***
Kommunikationsplanung muss beginnen, bevor das finale Impact-Bild vollständig ist.

⚠ ***„Wir informieren den Vorstand, sobald es als major bestätigt ist.“***
Das Management Body kann frühe Sichtbarkeit brauchen, bevor die finale Klassifizierung feststeht.

⚠ ***„Der Incident Plan ist dokumentiert.“***
Ein Plan ist nur nützlich, wenn Rollen, Schwellen, Entscheidungsrechte und Evidence Capture getestet wurden.

⚠ ***„Der Regulator wird informiert, falls erforderlich.“***
Das Institut muss zeigen, wer die Pflicht bestimmt und wann die Reporting-Uhr startet.

Keine dieser Aussagen ist notwendigerweise falsch. **Sie sind nur keine ausreichende Evidenz für Board-Level Reliance.**

08 PATH TO GREEN

Sechs Bedingungen für getestete Incident Decision Capability.

01 Decision Rights definiert

Wer in der ersten Stunde klassifizieren, eskalieren, kommunizieren, melden, containen und priorisieren kann.

02 Impact Path sichtbar

Business Impact, Client Impact, Critical Function Impact, Provider Dependency und geografische Ausbreitung können früh bewertet werden.

03 DORA Clock kontrolliert

Klassifizierungs- und Reporting-Fristen sind operationalisiert, owned und belegt.

04 Kommunikation gesteuert

Interne, Kunden-, Regulator-, Provider- und Medienkommunikation folgen genehmigten Entscheidungswegen.

05 Evidenz gesichert

First-Hour Timeline, Annahmen, Entscheidungen und Kommunikation können rekonstruiert werden.

06 Lessons eingebettet

Post-Incident Review verbessert Decision Quality, Eskalation, Kommunikation und Recovery.

NÄCHSTE FRAGE FÜR DEN VORSTAND

Welcher kritische oder wichtige Service würde den größten First-Hour Decision Pressure erzeugen, wenn er heute Nacht ausfällt — und können wir belegen, wer entscheidet, bevor Root Cause bekannt ist?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Ein Incident Plan beschreibt, was passieren sollte. Incident Decision Capability beweist, dass das Institut handeln kann, wenn die Fakten unvollständig sind.

Disciplined uncertainty ist der echte Test operativer Resilienz.

AUSGEWÄHLTE QUELLEN

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