# ICT Incident Management and Reporting

Nikos Kontizas, Counsel | Giannis Koutsoumpinas, Associate | Apostolos Solias, Trainee

01 July 2025

The Digital Operational Resilience Act (DORA)[1] introduces a harmonized regulatory framework across the EU for digital operational risk management by financial entities (FEs). One of its key pillars is the management and reporting of major ICT-related incidents and significant cyber threats.

## Regulatory and Implementing Technical Standards

The EU Commission has further adopted relevant Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS). Specifically, RTS have been adopted on the classification criteria for ICT-related incidents and cyber threats (RTS on classification)[2] and on the content and time limits for the notification procedure (RTS on time limits)[3]. ITS have also been adopted on standard templates for the notification procedure (ITS on templates)[4].

## DORA and PSD2

In order to reduce the administrative burden and potentially duplicative reporting obligations for certain FEs, Article 23 of DORA stipulates that the incident reporting framework laid down in DORA and its RTS/ITS applies to FEs covered by PSD2 [5], such as payment institutions, e-money institutions and account information service providers, for all operational or security payment-related incidents, whether ICT-related or not.

## ICT-related Incident Management Requirements

Under Article 17 of DORA, FEs are required to establish and implement robust policies and procedures for the identification, handling, and mitigation of ICT-related incidents and cyber threats. The ICT-related incident management process must cover the following:

- Detection & Classification: FEs should put in place early warning indicators and categorize incidents based on their priority, severity, and service impact.
- Roles & Communication: Responsibilities for different incident types must be defined, and communication plans must be established.
- Reporting & Escalation: Major incidents must be reported to senior management with impact assessments and response measures.
- Response & Recovery: Procedures to mitigate impacts and restore services securely and efficiently must be developed.

## Incident Classification Requirements

Article 18 of DORA requires FEs to classify all ICT-related incidents in accordance with certain qualitative and quantitative criteria. The RTS on classification further expand on the classification criteria, which include the following:

---

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[2] Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents.

[3] Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats.

[4] Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. The Directive has been transposed by Law 4537/2018.

- Client and Transactions Impact: Number and relevance of affected clients (or counterparts) and transactions.
- Data Loss: Impact on data availability, integrity, and confidentiality.
- Critical Services: Whether critical or important business functions were disrupted.
- Reputational Damage: Market perception, media coverage and client complaints.
- Duration: Time elapsed from incident occurrence to resolution.
- Geographical Spread: Cross-border effects in other EU Member States.
- Economic Impact: Direct and indirect costs and losses.

An incident is classified as major if it impacts critical services and materially affects two or more of the above criteria. Recurring (individually non-major) incidents sharing the same root cause over a 6-month period may collectively be considered major. The RTS on classification set out the specific materiality thresholds for classifying an incident as major.

In a similar fashion, FEs are required to classify cyber threats, in accordance with a more restrained number of criteria. A cyber threat qualifies as significant if it could impact critical functions, other FEs, third-party providers or clients, has a high probability of materializing based on risks and vulnerabilities, threat actor capabilities, and persistence, and meets materiality thresholds related to services affected, clients, or geographical spread.

**Reporting Requirements**

FEs must notify the competent authority of major ICT-related incidents, in accordance with Article 19 of DORA. The reporting process envisaged in the RTS on time limits is structured into three main stages, as outlined below.

**A. Initial Notification**

Time limit. Initial notification of major ICT-related incidents must be made within a tight timeframe: within 4 hours from the classification of the incident as major and no later than 24 hours from the moment the FE became aware of the incident.

Content. Initial notification reporting should cover specific information that is provided in the RTS: a description of the incident, the time and method of detection, its classification and relevant impact criteria, the possible activation of a business continuity plan and affected EU Member States. This information offers the competent authority a first, concise overview of the notified incident.

**B. Intermediate Report**

Time limit. Intermediate reports are submitted within 72 hours from the submission of the initial notification or upon recovery of regular activities. Updated intermediate reports are submitted without undue delay.

Content. Apart from the general information, intermediate reports must contain specific information that draws a more detailed description of the reported incident: the threat and techniques used by the threat actor, affected business areas and supporting infrastructure, impact on clients and measures for recovery, as well as whether affected activities have been recovered.

**C. Final Report**

Time limit. The final reports are submitted within 1 month after the submission of the intermediate report (or the latest updated intermediate report). It should be noted that root cause analysis must be completed within this timeframe.

Content. The final report contains information on the root causes of the ICT-related incident, the direct and indirect costs and losses stemming from it, the measures for recovery and mitigation of root causes and, if this is the case, information on recurring ICT-related incidents.

**D. General Remarks**

If FEs are unable to submit in time the initial notification and the intermediate or final reports, they shall inform the competent authority of their inability and the reasons thereof, within the applicable time limits.

For all stages of the notification procedure, the standard templates laid down in the ITS on templates apply.

If the time limits fall on a weekend day or a bank holiday, they are extended until noon of the next working day; this exception does not apply to credit institutions, CCPs, and other FEs classified as essential or important under the NIS2 Directive [6].

FEs must also inform their clients of the major ICT-related incident and the mitigating measures taken, if the incident affects their financial interests.

**Voluntary Reporting of Significant Cyber Threats**

While not mandatory, entities are encouraged to voluntarily notify significant cyber threats if these threats have the potential to disrupt the financial sector or client services. The reports must include:

- Date and time of detection.
- Threat description and hypothetical classification, had it been materialized.
- Preventive measures; and
- Potential or actual impact and indicators of compromise, where applicable.

**Competent Authorities- Law 5193/2025**

Law 5193/2025[7] introduces measures for the implementation of DORA, including the designation of national competent authorities for the supervision of compliance with DORA.

These tasks are divided between the Bank of Greece (BoG) and the Hellenic Capital Market Commission (HCMC), and consequently, incident reports are addressed to each of the two authorities based on the type of the FE making the notification:

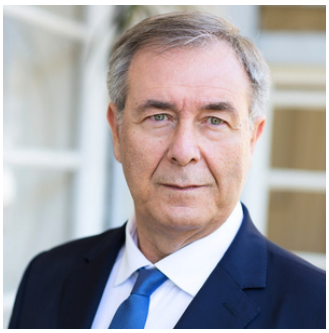
BoG is responsible for credit institutions, payment institutions, e-money institutions, account information service providers, and (re)insurance undertakings.

HCMC is responsible for investment firms, central securities depositories, central counterparties, trading venues, alternative investment fund managers and management companies.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. The Directive has been transposed by Law 5160/2020 (Government Gazette A' 195/27.11.2024).

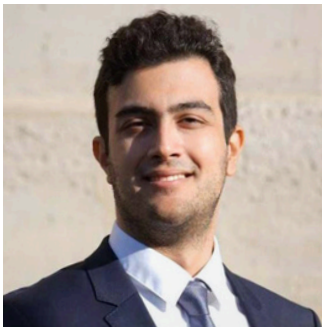
[7] Strengthening of the Capital Market and Other Provisions, Government Gazette, A' 56/11.4.2025.

## Key contacts



**Dr. Dimitris Tsibanoulis**
Senior & Managing Partner
d.tsibanoulis@tsibanoulis.gr

**Nikos Kontizas**
Counsel
n.kontizas@tsibanoulis.gr



**Giannis Koutsoumpinas**
Associate
g.koutsoumpinas@tsibanoulis.gr

**Tsibanoulis & Partners Law Firm**
18 Omirou St.
106 72 Athens | Greece
**T:** +30 210 3675 100
**W:** tsibanoulis.gr