IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ISM/2025/4625925/
Vol. 2025 (29), Article ID 4625925

Criteria For Classifying ICT-Related Incidents And Cyber Threats And The Procedure For Reporting Them By Financial Entities : A European Perspective*

Monika Szaraniec

Krakow University of Economics, Poland

Correspondence should be addressed to: Monika Szaraniec, szaranim@uek.krakow.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The rapid development of information and communication technologies necessitates the implementation of national legal frameworks that take into account cybersecurity standards, in particular in accordance with European Union legislation. Cybersecurity in financial entities forms the basis for legal and economic transactions and protects public interests. This article analyses the new regulatory obligations resulting from the implementation of the Digital Operational Resilience Act (DORA) and the NIS2 Directive, focusing on the identification and classification of incidents related to information and communication technologies (ICT). The author presents a comprehensive framework for classifying ICT incidents, introducing an eight-criteria model that assesses incidents based on: significance and impact, reputational consequences, duration, geographical scope, data loss, service criticality, and side effects. Particular attention is paid to the materiality threshold set out in Implementing Regulation 2024/1772, which is a key mechanism for determining whether an incident is material. The article presents a three-step procedural model that financial institutions should follow when an incident occurs.

The analysis shows that the new incident classification methodology goes beyond mere reporting requirements – it is an integral part of ICT management and macroprudential supervision systems in the financial sector. The standardisation of reporting procedures, including the elimination of duplicate notifications that were previously required under PSD2, enables more effective use of this tool in improving the efficiency of cyber monitoring at the international level.

Keywords: Innovations in information and communication technologies, financial entities, risk management, serious incidents, cyber attacks.

Introduction

Innovations in the field of information and communication technologies set the direction for the creation of various cybersecurity rules. With technological progress, national regulations should be systematically adapted to international standards, in particular to European Union legislation on combating cybercrime and ensuring an adequate level of protection in cyberspace. The cybersecurity of financial institutions, which are considered entities of public trust, is crucial for the stability of legal and economic transactions and for the protection of citizens' rights. Recent changes in EU legislation, such as the introduction of DORA and NIS2, have led to the adoption of specific legal standards for the financial sector. The article describes the new obligations of financial entities regarding the classification and reporting of incidents related to information and communication technologies (ICT) following the entry into force of the DORA Regulation. It discusses the definition of an ICT incident, the eight-criteria model for their classification, and the materiality thresholds set out in Implementing Regulation 2024/1772. The author points to the identification of incidents considered serious and to the three-

Cite this Article as: Monika Szaraniec, Vol. 2025 (29) "Criteria for Classifying ICT-Related Incidents and Cyber Threats and the Procedure for Reporting Them by Financial Entities: A European Perspective " Communications of International Proceedings, Vol. 2025 (29), Article ID 4625925,
https://doi.org/10.5171/2025.4625925

stage model for their reporting procedure. The article also outlines a methodology for classifying incidents, which not only serve a reporting function but are also an important element of ICT risk management and macroprudential supervision.

Definition of an ICT incident

On 14 December 2022, DORA was adopted with the aim of consolidating updates to regulations on ICT risk management, information sharing, testing and monitoring of risks from external ICT service providers. Digital operational resilience is understood as the ability of a financial institution to build, guarantee and verify its operational integrity from a technological point of view by ensuring, directly or indirectly (using the services of external ICT service providers), the full range of ICT capabilities necessary to ensure the security of the networks and information systems used by the financial institution and which support the continuous provision of financial services and their quality, including during disruptions.

DORA is the first regulation to comprehensively define the most important concepts related to the operational digital resilience of a financial entity. The scope of the DORA Regulation covers financial institutions such as: credit, payment and e-money institutions, investment firms, crypto-asset service providers (CASPs), Markets in Crypto-Assets Regulation (MiCA), issuers of asset-referenced tokens, central securities depositories (CSDs), central counterparties (CCPs), trading venues, trade repositories, alternative investment fund managers (AIFMs), management companies, data reporting service providers (AIS), insurance and reinsurance undertakings, insurance and reinsurance undertakings, insurance and reinsurance undertakings, insurance and reinsurance undertakings, insurance and reinsurance undert (CSDs), central counterparties – CCPs, trading venues, trade repositories, alternative investment fund managers – AIFMs), management companies, data reporting service providers – AIS, insurance and reinsurance undertakings, insurance and reinsurance intermediaries, institutions for occupational retirement pensions, credit rating agencies, statutory audit and audit firms, administrators of critical benchmarks, crowdfunding service providers, securitisation repositories, ICT third-party service providers. These include, in particular, concepts such as: IT networks and systems, obsolete ICT systems, IT network and system security, ICT-related risks, information resources, ICT resources, ICT-related incidents, serious ICT-related incidents and cyber attacks. According to Article 3(8) of DORA, an ICT-related incident is any unexpected event that has a negative impact on IT networks or systems, resulting in a breach of their availability, confidentiality, integrity or authenticity. This definition covers both technical failures (e.g. service interruptions) and cyber attacks (e.g. phishing). DORA adopts a broad concept of an incident, focusing not on its source but on its impact on the functioning of institutions and market stability. Article 3(10) of DORA defines and narrows down the concept of a serious incident. Such an incident is characterised by a significant negative impact on the networks and IT systems that support the critical or important functions of a financial entity. A cyberattack is defined in Article 3(14) of DORA and means a malicious ICT-related incident caused by an attempt to destroy, disclose, alteration, deactivation, theft or unauthorised access to or use of an asset by any aggressor, i.e. the involvement of third parties. All these definitions are crucial for the classification of ICT-related incydent (Byrski, Kurek-Sobieraj, 2025).

New criteria for classifying ICT-related incidents and cyber threats

Pursuant to Article 118(D) of DORA, financial entities are required to classify ICT incidents based on eight criteria. Detailed guidelines for classifying ICT incidents are set out in the supplementary Regulation 2024/1772 (materiality thresholds). The criteria set out in the DORA Regulation are as follows:

1) Criterion of the number or importance of customers or financial counterparties. Its assessment is based on the number and importance of these entities. Customers are all those who will be unable to use the services during the incident or who will suffer negative consequences as a result of difficulties in accessing the service functions. This includes both natural and legal persons, regardless of the organisational form or nature of the customer (professional/non-professional);

2) The criterion of the amount or number of transactions. Transactions include various financial activities and services, including payments, exchange of financial instruments, crypto-assets, commodities or other assets. The criterion takes into account all transactions where at least one part is carried out in the EU, including both-legs and one-legs transactions. In the absence of accurate data, the entity may estimate the number/amount of transactions based on data from comparable periods.

3) Criterion of impact on reputation. The financial entity assesses whether at least one of the following conditions is met: the incident has been reported in the media, there are repeated complaints from customers/contractors, it is impossible to meet regulatory requirements, there is a loss of customers/contractors affecting operations; the assessment should take into account the level of visibility of the incident from the perspective of third parties;

4) Criterion of the duration of the incident. The criterion of the duration of the incident includes an interruption in the provision of services by the financial entity. The duration of the incident should be measured from its occurrence to its resolution, and if it is not possible to determine the moment of occurrence, from the moment of its detection. If the incident occurred before detection, the time is counted from its registration in the network log, system log or other available sources;

5) The geographical scope criterion relates to the cross-border reach of an ICT incident, focusing on its impact in other Member States and not just in a single jurisdiction. Financial entities should therefore assess whether the incident affected: customers/contractors in other EU Member States in relation to the entity's headquarters, branches or entities from the same capital group operating in the EU, market infrastructure or suppliers whose activities may affect other entities in the EU;

6) Data loss criteria. This refers to the loss of data due to a breach of its availability, authenticity, integrity or confidentiality. The financial entity should assess whether: the data has become temporarily or permanently unavailable, i.e. its availability, whether the reliability of the data source has decreased, i.e. its authenticity, whether unauthorised modification of the data has occurred (integrity), whether the data has been disclosed or made available to unauthorised persons (confidentiality);

7) Criticality of services criterion. The impact on critical services should be assessed and the incident should be classified as serious. In this case, the financial entity should assess whether the incident: affected systems supporting critical functions, affected regulated financial services, constituted effective, malicious and unauthorised access to ICT systems;

8) Economic impact criterion. The economic impact of the incident is taken into account here, including losses and costs incurred by the financial entity, such as: lost assets, costs of replacing software, hardware and infrastructure, personnel costs, contractual breach fees (excluding uncertain contractual damages), customer claims and compensation payments, lost revenue, emergency communication costs, external consulting costs (legal, technical; Makowiec, 2025).

„Incident" and „serious incydent"

According to the Digital Operational Resilience Act (DORA), an 'ICT-related incident' is defined as: a single event or a series of related events, unplanned by a given financial entity, which threaten the security of networks and information systems and have a negative impact on the availability, authenticity, integrity or confidentiality of data or on the services provided by that financial entity."

A 'serious ICT-related incident'2 is defined as: 'an ICT-related incident with a significant negative impact on the networks and information systems that support the critical or important functions of a financial entity.'

These two definitions also use other terms (IT networks and systems, security of IT networks and systems, or critical or important function), which are also defined in the DORA Regulation and cover events including cyber attacks and operational incidents, meaning that such events may also include system failures and other technological disruptions.

The DORA Regulation provides for a number of criteria for classifying serious ICT-related incidents, including:

- the number or importance of customers or financial counterparties and (where applicable) the amount or number of transactions affected by the ICT-related incident, and whether such an incident has had reputational consequences,
- the criticality of the services affected by the ICT incident, including the transactions and operations of the financial entity,
- the duration of the ICT incident, including the interruption in the provision of services,
- the loss of data as a result of the ICT incident in terms of the availability, authenticity, integrity or confidentiality of data,
- the economic impact of the ICT incident, in particular direct and indirect costs and losses,
- the geographical scope of the ICT incident, in particular if it affects more than two Member States.

In addition, Article 18(3)(a) of the DORA Regulation provides that the clarification of the above criteria, including the determination of materiality thresholds for the purpose of determining serious ICT incidents, shall be carried out by means of regulatory technical standards as an implementing act to the DORA Regulation.

Therefore, the classification of ICT-related incidents, and in particular the assessment of the occurrence of a serious ICT-related incident, should be based on the definition of a 'serious ICT-related incident' and the application of classification criteria and materiality thresholds specified in the regulatory technical standards.

Reporting serious ICT incidents and significant cyber threats

This means that supervised entities, which have so far been subject to incident reporting requirements under PSD2, will be required to report serious operational incidents or serious security incidents related to payments in accordance with the DORA Regulation. This is intended to reduce the administrative burden and eliminate duplicate incident reporting obligations for certain financial entities (those providing payment services). This solution is also correlated with the amendments to PSD2 made under Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 with regard to the operational digital resilience of the financial sector. Reporting incidents is crucial for the long-term process of building security and resilience to cyber attacks, especially in the financial sector. This enables rapid action to be taken, which can often help to minimise the negative impact of an incident on the organisation and its customers. Information about incidents also allows for the analysis of causes and patterns of threats, which contributes to the development of better protection strategies in the future and provides the opportunity to preventively secure institutions potentially vulnerable to the same or similar attacks.

Summary

Under DORA, financial entities must maintain an ICT risk management framework, implement incident reporting procedures (including the use of specific templates) and manage third-party ICT risk through contractual and supervisory arrangements.

The literature particularly emphasises the supervisory and coordination tasks of authorities to ensure compliance with reporting and cross-border information exchange. This applies to:

- Risk management – financial entities must establish and apply an ICT risk management framework and internal procedures to identify, classify and report reportable incidents (Bierecki, 2024),

- Incident reporting procedures – financial entities are required to implement operational processes that generate standard notification content and trigger notification of the relevant authorities/supervisory bodies in the event of a reportable incydent (Clausmeier, 2022).

- Third-party contractual controls The DORA system includes mandatory contractual/supervisory provisions for external ICT service providers (including priority clauses applicable in the event of insolvency or cessation of services by providers), and competent supervisors play a role in coordinating third-party risks after notification (Duggan, 2024),

- Proportionality and exemptions The law is applied proportionally; smaller or less complex entities may apply simplified requirements if permitted by DORA and national options — the literature discusses these proportionality mechanisms and possible national exemptions.

- Supervision and sanctions Reporting and follow-up information enable supervisory authorities to monitor compliance; academic commentary highlights the challenges of supervisory coordination within the European system but does not mention specific levels of sanctions in the attached excerpts.

References

- Buttigieg C.P. and Zimmermann B.B., 'The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of the European Financial Supervisory Architecture', ERA Forum, 2024. doi: 10.1007/s12027-024-00793-w.
- Bierecki D., 'The principle of graphicality in the application of the regulation on the practical application of combating optical threats (Digital Operational Resilience Act – DORA)' 2024. doi: 10.52097/eppism.9272
- Komentarz , pod red. J. Byrski, J. Kurek-Sobieraj, Warszawa 2025, Legalis.
- Clausmeier D., 'Regulation of the European Parliament and of the Council on Digital Operational Resilience of the Financial Sector (DORA)', International Cybersecurity Law Review, 2022. doi: 10.1365/s43439-022-00076-5.
- Duggan D., 'The Impact of the Digital Operational Resilience Act on Financial Market Infrastructure in Europe', 2024. doi: 10.69554/khfm3582.

- K. Makowiec, ICT classifications and incidents after the implementation of DORA (in:) FinTech Financial Innovation Law) 2025, ed. J. Byrski, Legal Monitor Supplement 8/2025 C.H. Beck.
- Commentary, ed. J. Byrski, J. Kurek-Sobieraj, Warsaw 2025, Legalis.
- 'Supporting the digital operational resilience of the financial sector: the EU DORA Act on digital operational resilience', University of Piraeus (student analysis), available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/16273/DORA%20-%20MTE2109%20Karakasilioti.pdf?sequence=1 (accessed: September 2025).
- DORA (Digital Operational Resilience Act) – Regulation on the operational resilience of the digital financial sector, amending Regulation (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, OJ EU No L 333/1 of 27 December 2022. The Regulation will enter into force on 17 January 2025.
- NIS2 (Network and Information Systems Directive 2) – Directive (EU) 2022/25555 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, OJ L 333, 27.12.2022, p. 80.
- Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council (EU) 2022/2554 with regard to regulatory technical standards specifying the criteria for classifying ICT-related incidents and cyber threats, materiality thresholds and detailed information on the reporting of serious incidents, OJ L of 2024, p. 1772.