JC 2026 16

03 June 2026

2025 Report on major ICT-related incidents

Joint-ESA report under Article 22 of DORA

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

List of Figures

Abbreviations

Abbreviation	Meaning
AISP	Account Information Service Provider
CA	Competent Authority
CI	Credit institution
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMI	Electronic Money Institution
ESA	European Supervisory Authorities
ESMA	European Securities and Markets Authority
FE	Financial entity as referred to in Article 2(1), points (a) to (t) of Regulation (EU) 2022/2554
ICT	Information and communication technology
TPP	Third-party service provider
MS	Member State
PI	Payment institution
PSD2	Payment Services Directive (Directive (EU) 2015/2366)
TARGET2	Trans-European Automated Real-time Gross settlement Express Transfer system
T2S	TARGET2-Securities
TIPS	TARGET Instant Payment Settlement

Executive Summary

This joint-ESA report provides an overview, on an anonymised and aggregated basis, of major ICT related incidents occurred in 2025, in accordance with Article 22(2) of the Digital Operational Resilience Act (DORA). Major ICT related incidents are ICT-incidents that have a high adverse impact on the network and information systems that support critical or important functions of financial entities[1]. Overall, 3,383 major incidents (corresponding to an average of 0.18 major ICT related incidents per financial entity subject to DORA) were reported in 2025 across all financial sectors in the EU, with the majority of them occurring in the credit and payments sectors[2]. Such a concentration reflects differences in market structure, the existence of similar reporting requirements prior to DORA, and the highly digital and customer facing nature of services provided in these sectors rather than sector-specific weaknesses.

In general, the number of major incidents should not be interpreted as a sign of structural weaknesses: the increased digitalisation, complexity and interconnection of the financial sector make operational incidents to some extent unavoidable. Instead of absolute numbers, the resilience of the financial sector is demonstrated by the ability shown by financial entities to promptly identify, manage and contain major incidents. Indeed, this report finds that despite their frequency and, in some cases, wide geographical reach, the impact of major incidents on clients, transactions and financial counterparties was limited: two thirds of major incidents resulted in no or minor disruption to clients and transactions, suggesting that in fact the timely detection, paired with effective incident response and containment measures were often successful in limiting operational harm and spillover effects.

The analysis also shows that ICT risks are increasingly borderless. Around one third of reported major incidents had a cross-border impact. This underlines the growing interconnectedness of financial entities through shared infrastructures, common ICT services and cross-border business models.

System failures and external events emerged as the predominant driver of major incidents. Almost one third of major incidents originated from failures attributable to third-parties (including ICT third-party providers, other financial entities, and infrastructure providers), highlighting the critical role of outsourced services, the interconnectedness of the financial system, and the importance of robust third-party risk management, oversight and coordination. At the same time, the relatively low number of major incidents categorised as cybersecurity-related seems to suggest that existing safeguards and detection mechanisms were generally effective in limiting the occurrence of such incidents. While this shows that the financial sector was able to withstand ICT-related threats, it is key that financial entities uphold to highest cybersecurity standards to be able to keep pace with the potential use of highly capable AI-driven tools.

From a supervisory perspective, divergent reporting practices across sectors and jurisdictions are still observed. These divergences reflect the early stage of implementation of the new major incident reporting framework introduced by DORA. The continued coordination and exchange between

[1] See Article 3(10) of DORA.
[2] The credit sector is composed of credit institutions, while the payments sector is composed of electronic money institutions (EMI) and exempted EMIs, payment institutions (PI) and exempted PIs, and account information service providers.

supervisors are expected to significantly enhance data quality, comparability and supervisory usability of the data reported.

Looking ahead, the ESAs will continue to monitor and analyse major incidents and provide additional guidance to competent authorities, supporting greater supervisory convergence and improved reporting practices.

1. Introduction

1. This report responds to the mandate set in Article 22(2) of the Digital Operational Resilience Act (DORA)[3] for the European Supervisory Authorities (ESAs) through the Joint Committee to report yearly on major ICT-related incidents on an anonymised and aggregated basis, setting out at least: (i) the number of major ICT-related incidents, (ii) their nature, (iii) their impact on the operations of financial entities or clients, (iv) remedial actions taken, and (v) the costs incurred.

2. Article 3(8) of DORA defines an 'ICT-related incident' as 'a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity'. Article 3(10) of DORA further defines a "major" ICT-related incident as 'an ICT-incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity'. Article 18(1) of DORA sets forth the criteria to classify ICT-related incidents while the relevant materiality thresholds to determine when an incident should be classified as "major" are specified in the Commission Delegated Regulation (EU) 2024/1772[4] (hereinafter, the RTS on classification criteria). For the purposes of this report, 'ICT-related incidents' and 'major ICT-related incidents' will be referred to, respectively, as 'incidents' and 'major incidents'.

3. Pursuant to Article 19 of DORA, financial entities (FEs) are required to report major incidents to the relevant Competent Authority (CA), through different subsequent notifications, each containing specific information as further defined in the Commission Delegated Regulation (EU) 2025/301[5] (hereinafter, the RTS on the content of major incident reports):

   (i) an initial notification, providing limited available information, to be submitted within four hours from the classification of the incident as major and no later than 24 hours from the moment the financial entity has become aware of it;

[3] 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 (OJ L 333, 27.12.2022, pp. 1–79, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[4] 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 (OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

[5] 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, (OJ L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

(ii) an intermediate report after the initial notification, containing more detailed information about the incident, to be submitted within 72 hours from the submission of the initial notification; and

(iii) a final report when the root cause analysis has been completed, including all the relevant information, to be submitted no later than one month after the submission of the intermediate report, or, where applicable, after the latest updated intermediate report.

4. The Commission Implementing Regulation (EU) 2025/302[6] (hereinafter, the ITS on templates and procedure to report major incidents) further details the format and the templates to be used by FEs to report major incidents to their CAs. Upon receipt of the major incident, CAs are required to provide the details of the major incident to the ESAs and the ECB so that, inter alia, they can notify other relevant CAs in case of relevance (Article 19(6) and (7) of DORA).

5. This report is intended to provide an overview of major incidents occurred in 2025 in the EU[7] and reported to CAs in accordance with Article 19 of DORA, while Section 2 delineates the methodology followed for the analysis as well as the identified limitations, while Section 3 provides an aggregated overview of key metrics per sector; it also includes a deep dive on selected major incidents that had a broad impact on the EU financial sector, e.g. in terms of number of entities and clients impacted, or due to a widespread news coverage.

2. Methodology

6. The analysis underpinning this report is based on quantitative and qualitative information included in the major incident reports submitted by FEs to CAs and forwarded to the ESAs in accordance with Article 19 of DORA. To avoid duplication and ensure accurate representation of data, the analysis is limited to major incidents occurred in 2025 for which a final report was submitted by the cutoff date of 5 February 2026. This cutoff date was chosen to ensure a better representation of incidents that occurred in December 2025, as FEs must submit the final report within one month from the last intermediate notification. This approach aims to ensure that all the relevant information is consistently captured, while preventing the inclusion of incidents that are still open and may later be reclassified as non-major. To this extent, it should be noted that a final report

[6] 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 (*OJ L, 2025/302, 20.2.2025,* ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj).

[7] It should be noted that DORA is also applicable to countries in the European Economic Area (EEA): it entered into force on 1 February 2025 in Liechtenstein and on 1 July 2025 in Norway. As to Iceland, DORA has entered into force on 1 January 2026, therefore the current analysis does not cover the entirety of the EEA.

was not received by the cutoff date for approximately 15% of the major incidents notified in 2025, which were therefore excluded from the analysis.

7. Furthermore, certain events may affect simultaneously multiple FEs in the same or different jurisdictions, as well as in the same or multiple sectors. When several FEs are affected by the same event, as long as it qualifies as a major incident at the level of single FE, each affected FE is required to notify it to the relevant CA and reflect the respective individual impact in the reporting template.

8. During the first reporting year under Article 19 of DORA, the ESAs ensured both data availability (i.e. ensuring the information flow between competent authorities, ESAs and other relevant authorities in a timely manner) and data confidentiality (i.e. ensuring that the transmission of information is done through secure channels). However, major incident reports were not yet subject to a full set of automated data quality rules. Therefore, a set of basic post-reporting checks was introduced. While these checks did not fully reflect the breadth of validation rules that could be derived from the reporting requirements, they were designed to address the key data quality issues during this transitional phase. Ultimately, nearly all submissions (~93%) were accepted and included in the database for the analysis.

9. To support the analysis and mitigate data quality constraints, a set of centralised quality assurance and data preparation steps was carried out, aimed to ensure a minimum and consistent level of data quality for the indicators presented in this report. These included, inter alia:

   (i) standardisation of formats, including removal of special characters, extra spaces and inconsistent delimiters;

   (ii) harmonisation of identifiers, country codes and permitted values to ensure consistency and validity;

   (iii) translation of certain fields written in languages other than English; and

   (iv) introduction of derived variables to further facilitate analysis, including flags identifying the latest version of major incident reports based on the type of submission[8].

3. Overview of major incidents in the EU

10. This section provides an overview of major incidents that occurred in the EU in 2025 and with a final report submitted by the cutoff date of 5 February 2026. The metrics presented in this section aim to illustrate key patterns and trends of major incidents relating to their frequency, classification criteria, underlying nature and observed impact on clients, transactions and financial

[8] For instance, in cases where a multiple initial, intermediate or final report were submitted, a flag was created to identify which report was the latest version.

entities. Where possible, results are also presented with a breakdown per sector, as defined in the Table below.

Overview of sectors and entities.

Sector	Type of entities subject to incident reporting under DORA
Credit	Credit institutions (CIs)
Payments	Payment Institutions (PIs) and exempted PIs
	Account Information Service Providers (AISPs)
	Electronic Money Institutions (EMIs) and exempted EMIs
Crypto	Issuers of Asset Referenced Tokens (ARTs)
	Crypto Asset Service Providers (CASPs)
Markets and intermediaries (M&I)	Investment firms
	Crowdfunding service providers
Asset management (AM)	Managers of alternative investment funds
	Management companies
Market infrastructures and post-trade (MI&PT)	Central securities depositories
	Central counterparties
	Trading venues
Market Transparency Infrastructure (MTI)	Trade repositories
	Data reporting service providers
	Securitisation repositories
Rating and benchmarks (R&B)	Credit rating agencies
	Administrators of critical benchmarks
Insurance	Insurance and reinsurance undertakings
	Insurance and reinsurance intermediaries and ancillary insurance intermediaries
Pensions	Institutions for occupational retirement provision

11. The indicators included in this section should be read in light of the scope, data quality limitations and reporting practices described in Section 2 and are intended to support a high-level understanding of ICT risk drivers rather than a granular assessment of individual incidents. Unless otherwise specified, all figures and charts in this section are based on data collected and processed by the ESAs from major incident reports and are presented on an anonymised and aggregated basis. Certain figures are based on fields allowing for multiple choices and therefore reflect the total number of occurrences reported which could be equal or higher than the number of individuals major incidents.

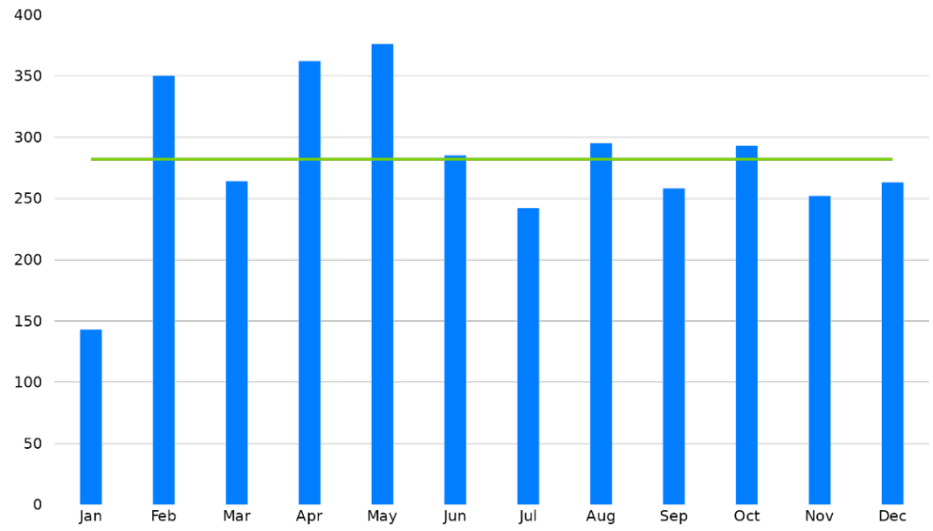
3.1 Number of ICT-related incidents

12. During 2025, FEs reported a total of 3,383 major incidents, with an average[9] of 282 major incidents per month (see Figure 1). When compared to the total number of FEs subject to DORA, this equals

[9] The lower total number in January can be explained with the fact that DORA entered into force on 17 January.

0.18 major incidents per FE, with a monthly average of 0.015 major incidents per FE. Spikes in the number of incidents reported in February, April and May can be explained by specific cross-border and/or cross-sectoral events, including: (i) the TARGET2 outage occurred in February 2025, which caused the suspension of securities settlement, payments, ancillary system processing and liquidity transfers for several hours; (ii) the energy blackout in the Iberian Peninsula occurred in April 2025, which disrupted normal operations across all sectors; and (iii) two separate events affecting multiple entities in May 2025 .

Figure 1. Total number of major incidents (blue bar) per month and annual average number of major incidents per month in 2025 (green line)



13. As shown in Figure 2, more than three quarters of all 2025 major incidents affected two sectors: more than 60% occurred within the credit sector (with an average of 0.57 major incidents per FE), while an additional 16% affected the payments sector (with an average of 0.23 major incidents per FE).

14. At this stage, it is not possible to draw definitive conclusions based on the number of incidents only, and the number of incidents per se is not a risk indicator. Differences across sectors may be attributed to a variety of factors, including:

    (i) the existence of similar reporting obligations prior to DORA: for instance, both the credit and the payments sector have been subject to major incident reporting since 2018 under the revised Payment Services Directive (PSD2)[10];

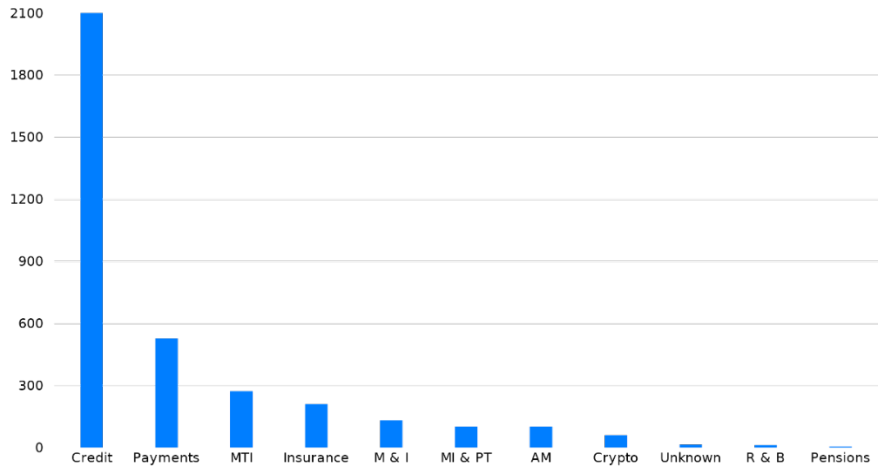
    (ii) the structure of the market: in the credit sector there are instances of many smaller entities belonging to the same group. These generally rely on the same shared infrastructure and are

[10] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market *amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC* (OJ L 337, 23.12.2015, pp. 35–127,ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

serviced by large TPPs for core banking, payment processing and connectivity, creating a multiplier effect: a single failure can generate dozens of related major incidents[11]; and

(iii) the nature of the services provided: CIs and PIs operate some of the most digitally intensive and consumer-facing services in the financial system, such as payments, online and mobile banking, and card processing, which are used at massive scale every day. This increases both the exposure surface and the likelihood that disturbances are quickly detected and reported.

Figure 2. Total number of major incidents occurred per sector in 2025[12]



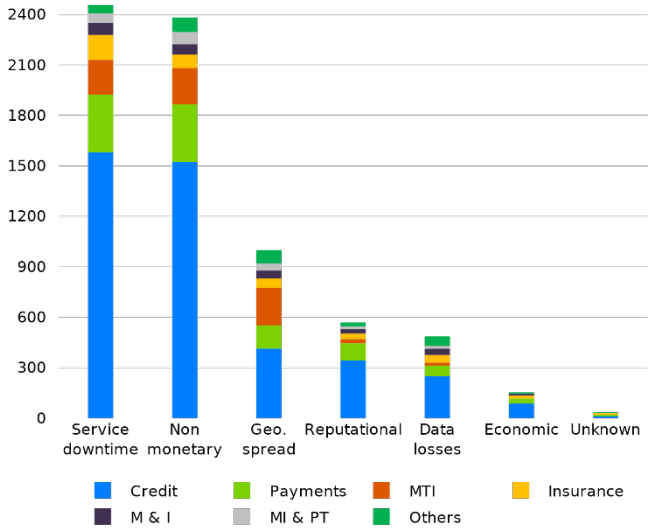
15. The RTS on classification criteria set out the rules for determining when incidents qualify as "major" based on their impact on critical services, clients, data, operations, geography, and economic losses; they also define quantitative and qualitative materiality thresholds that trigger the reporting obligation. Figure 3 shows the number of major incidents by each classification criteria with a breakdown per sector. It should be noted that each major incident can be triggered by multiple classification criteria, therefore the total number of incidents based on classification criteria appears higher than the total number of major incidents.

[11] In such cases, provided that certain conditions are met, Article 7 of the ITS on templates and procedure to report major incidents allows TPPs to provide aggregated information about a major incident impacting multiple FEs and submit the relevant notification/report to the CA on behalf of all impacted FEs.

[12] It should be noted that the number of incidents under market transparency infrastructure is higher due to the divergent application of classification criteria by one entity for a prolonged period in 2025.

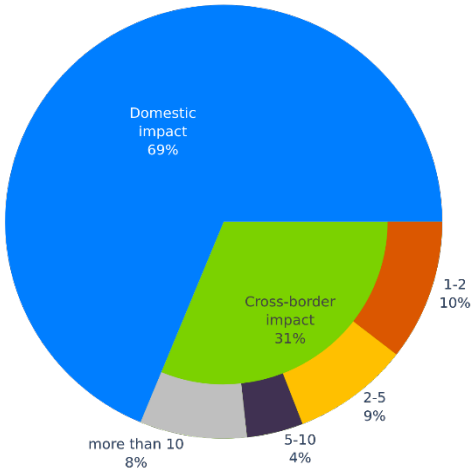
16. In 2025, the vast majority of incidents were classified as major due to mainly two classification criteria: (i) duration and service downtime, and (ii) clients, financial counterparts and transactions affected (labelled as "non-monetary" in Figure 3). Around 16% of major incidents were classified as major on the basis of a reputational impact, meaning they were reflected (or could potentially be reflected) in the media, resulted in repetitive complaints from different customers, caused the FE to (likely) not be able to meet regulatory requirements and/or caused the FE to (likely) lose customers with a material impact on its business.

Figure 3. Classification criteria that triggered incident reporting (breakdown by sector)



17. Moreover, a third of major incidents (i.e. 1,056 major incidents) had a cross-border impact, meaning their effects extended beyond the country in which it was reported to the relevant CA[13] (see Figure 4). Around one third of these cross-border major incidents affected one or two Member States. However, in about 8% of all major incidents, more than 10 countries were impacted, highlighting the interconnectedness of the financial sector and the borderless nature of ICT risks[14]. Indeed, such risks can be amplified by the interconnections both within individual sectors and across the broader financial system: as FEs increasingly rely on shared infrastructure, services, and third-party ICT service providers (ICT TPPs), disruptions, failures and other operational events can rapidly propagate across multiple sectors and jurisdictions.

Figure 4. Share of major incidents with a domestic or cross-border impact (with breakdown per number of members states affected).



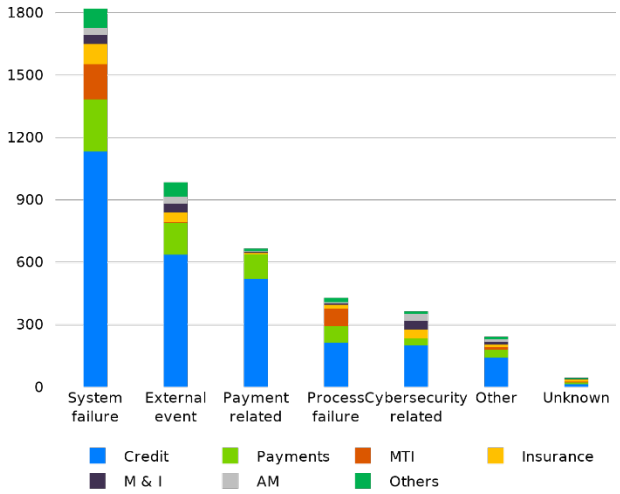
[13] Pursuant to Articles 4 and 9 of the RTS on incident classification, FEs are required to assess the cross-border impact of the major incident. To this end, FEs need to assess whether the major incident had an impact on other member states, an in particular in relation to: (i) clients and financial counterparts located in other member states; (ii) branches or other FEs within the group carrying out activities in other member states; and (iii) financial market infrastructures or third-party providers, which may affect FEs in other Member States to which they provide services.

[14] More than two thirds of these incidents are linked to system failures or process failures.

3.2 Nature of the major ICT-related incidents

18. In terms of type of incidents, system failures were reported for 51% of all major incidents, followed by external events (27%) and payment-related incidents (18%). However, these figures need to be interpreted carefully, potentially due to specific reporting practices[15]. While the nature of major incidents appears to be the same across most sectors, those reported by entities in the MTI sector were predominantly classified as system failure or process failure (see also Figure 5), as expected due to the nature of the services provided (i.e. data and reporting services). Overall, the high number of system failures across all sectors may be caused by the complexity of the digital infrastructure which exposes FEs to more software issues. On the other hand, Cybersecurity-related incidents accounted for 10% of the total. As already evidenced in the EBA Autumn 2025 Risk Assessment Report[16], the relatively low number of cybersecurity incidents seems to show that safeguards and security measures in place are effective in limiting the occurrence of such incidents.

Figure 5. Classification of major incidents by type with breakdown by sector



Text box: Analysis of cybersecurity incidents

In cases of cybersecurity incidents, FEs are required to indicate the threats and techniques used by the threat actor[17]. In 2025, the majority of attacks were concentrated in two categories: Distributed Denial of Service (DDoS) attacks[18] (33%), and data exfiltration and manipulation, including identity theft (31%). As highlighted in Figure 6, these two types of attacks appear to occur significantly more frequently in the credit sector. This could be explained by a combination of factors: the scale of their digital services, the concentration of sensitive data, and their role in processing payments. In addition, the relatively mature monitoring and incident-detection frameworks in place at many credit institutions may lead to earlier identification and more consistent reporting of cybersecurity incidents. In contrast, the remaining techniques are more evenly distributed across sectors, with the

[15] The high number of incidents observed at credit institutions, paired with CAs' own assessment, may point to potential underreporting of payment-related incidents. This may be caused, for instance, to diverging reporting practices, with FEs not selecting all applicable options.

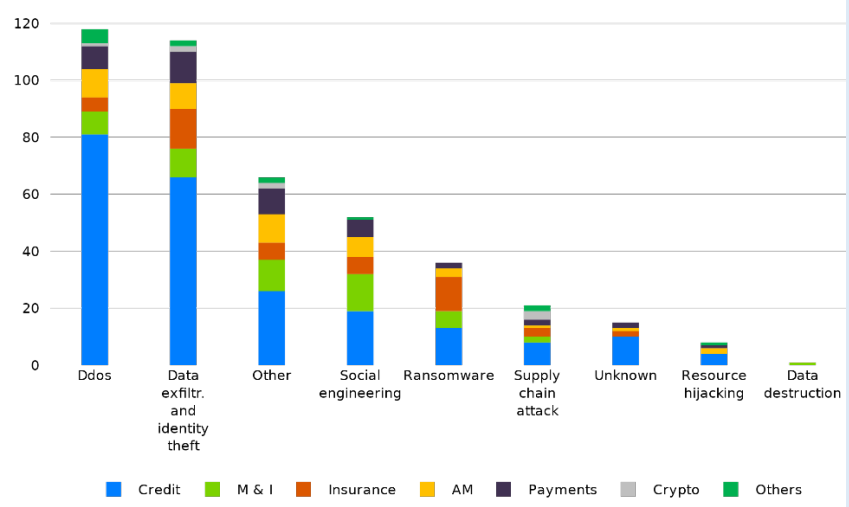
[16] "Amid a decreasing volume and frequency of cyber-attacks, the share of responding banks having faced at least one successful attack which resulted in an actual major ICT-related incident decreased to 28%, from 35% in the last iteration of the RAQ, and after a steady increase since 2023. These figures might indicate that cyber threats may have levelled, albeit staying overall high". See Risk Assessment Report Autumn 2025.

[17] Field 3.25 - Threats and techniques used by the threat actor.

[18] A Distributed Denial of Service (DDoS) is a cyber-attack that floods a website or online service with traffic from many devices at once, overwhelming its resources and making it slow or unavailable for legitimate users.

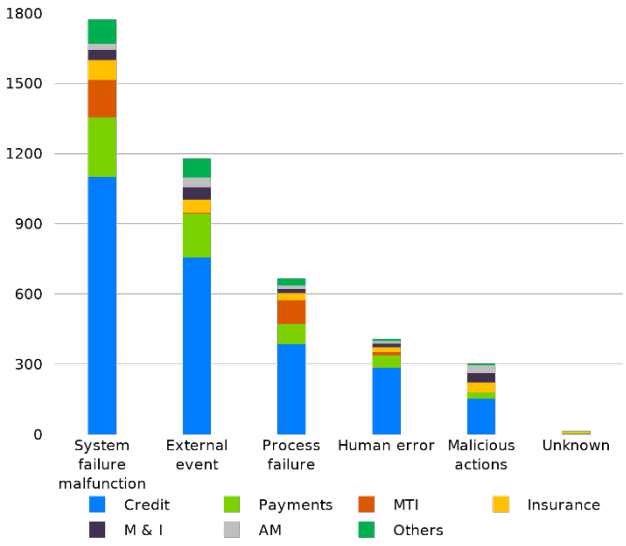
exception of ransomware attacks[19], which appear to target especially the insurance sector. This may be explained by the fact that insurance companies hold large volumes of sensitive health and financial data.

Figure 6. Threats and techniques used by the threat actor, only applicable to cybersecurity incidents with breakdown by sector.



19. Irrespective of their nature, each major incident can be caused by a few different reasons. Therefore, FEs are required to analyse the root cause(s) of each major incident and to indicate it in the final report. This information is provided by selecting one or more of the following pre-defined high-level categories: (i) malicious actions; (ii) process failure; (iii) system failure/malfunction; (iv) human error; and (v) external event. Figure 7 provides an overview of the high-level root causes with a breakdown per sector. In 2025, half of major incidents were caused by a system failure/malfunction. External events and process failures accounted for 32% and 19% of total major incidents respectively, and the share of incidents reported to be caused by external events is indeed consistent with the finding that 29% of all major incidents are caused by a failure attributable to a TPP (see text box: third-party dependency).

Figure 7. Breakdown per sector of high-level root causes triggering a major incident

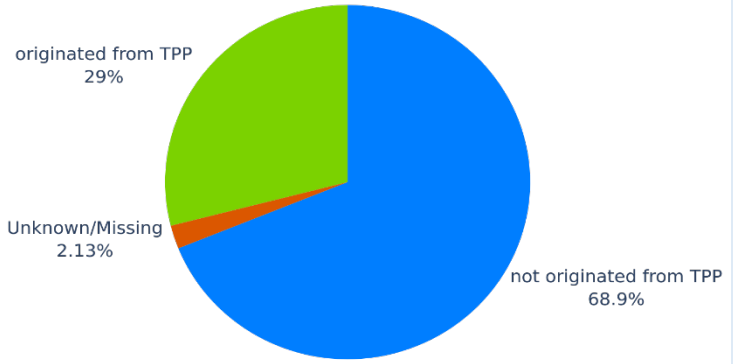


[19] A ransomware is a malicious software attack that locks or encrypts data until a ransom is paid for their release.

Text box: Third party dependency

Almost one third of major incidents originated by a failure on the side of a TPP (see Figure 8). This indicates that dependencies on TPPs, even those non designated as critical, constitute an area of supervisory attention and underscores the need for FEs to further strengthen their third-party- risk management frameworks.

Figure 8. Share of major incidents originating from ICT third-party service providers



20. Human errors caused 12% of major incidents, mainly concentrated in the credit sector, while no major incidents caused by human error were reported in the ratings & benchmarks and pensions sectors. Process failures and system failures/malfunction occurred in all sectors.

3.3 Impact on clients, transactions and financial counterparties

21. In addition to having a direct impact on FEs, major incidents can also affect clients, transactions and other financial counterparts. If this is the case, FEs are required to indicate in the intermediate report: (i) the number and percentage of clients affected; (ii) the number and percentage of financial counterparts affected, and (iii) the number and the percentage of transactions affected[20].

22. In the vast majority of cases (i.e. almost 60%), the impact on clients is either absent or minor, with less than 1,000 clients affected (see Figure 9). On the other hand, a few incidents have affected more than 1 million clients: some of these occurred in the credit and payment sectors, and a lower number in the insurance and the asset management sector. In general, major incidents with a heavier impact on clients are those affecting the credit and the payment sector, potentially due to the higher customer base making use of these services on a daily basis, and sometimes multiple

[20] In this data fields some data quality issues could not be addressed and therefore less information than for the remaining of the report was used.

times a day, including overnight. From the incidents affecting clients in the crypto sector, only one third had an impact on more than 1,000 clients.

23. As to transactions affected, two thirds of major incidents did not affect any transactions (32%) or affected less than 1,000 transactions (26%) (see Figure 10). On the other hand, only 30 major incidents (i.e. 1%) affected more than a million transactions, mainly impacting the credit and payments sector.

Figure 9. Sectoral breakdown of major incidents by number of clients affected (in buckets)

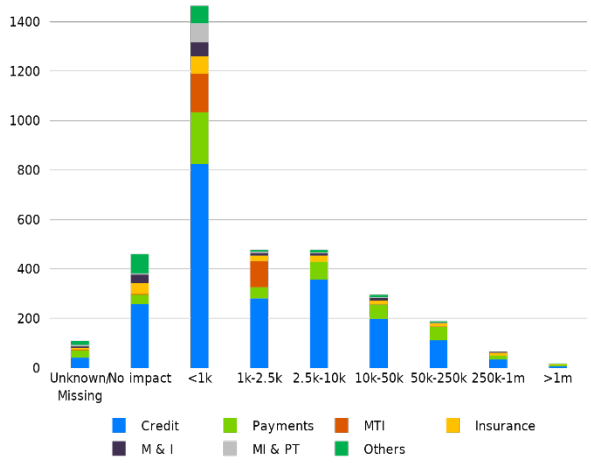
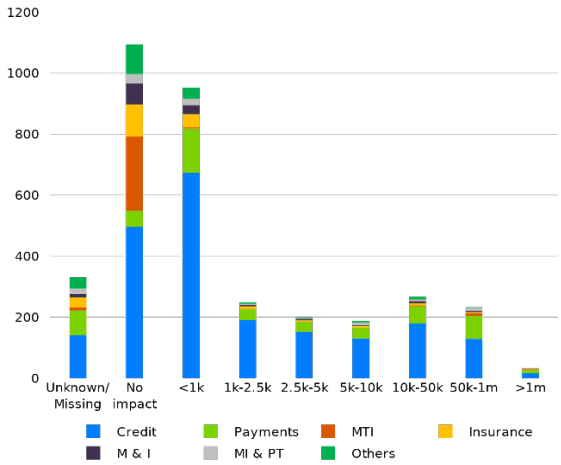


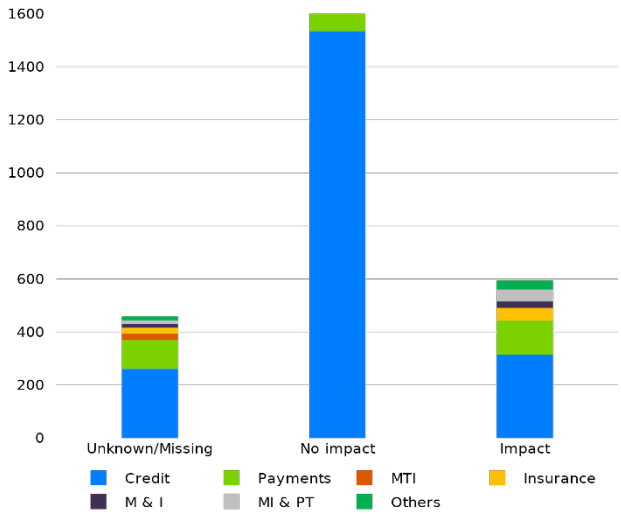
Figure 10. Sectoral breakdown of major incidents by number of transactions affected (in buckets)



24. The implications of major incidents for financial counterparts are also limited: less than 18% of major incidents affected other financial counterparts (see Figure 11, far-right bar). More than two-thirds of these cases occurred in the credit and payments sectors, potentially due to the specificities of the services and products offered by CIs, EMIs and PIs.

25. Overall, the impact of major incidents on clients, transactions and financial counterparties appears rather limited in the vast majority of cases. In practical terms, most incidents either did not affect clients, transactions or counterparties at all, or affected them only to a relatively small extent. Especially the very limited impact on financial counterparties may appear counterintuitive given the high degree of interconnectedness within the financial system. However, such an outcome may be explained by different factors. Firstly, the timely detection of incidents and the relatively swift implementation of remedial actions may have helped contain their effects

Figure 11. Sectoral breakdown of major incidents having or not an impact on financial counterparts



before they escalated into more widespread disruptions, allowing FEs to deploy countermeasures and containment actions in a timely manner. Secondly, the safeguards put in place by FEs may have been effective in mitigating spillover effects, even in an environment characterised by strong interdependencies.

3.4 Remedial actions

26. In the final report, FEs are required to include a summary of the remedial actions undertaken. The assessment revealed consistent operational patterns: most incidents, regardless of the entity type, are initially stabilised through rapid technical interventions. Such actions are commonly used to restore service continuity during the initial phase of incident management.

27. Following the initial recovery, FEs typically introduce longer-term corrective measures aimed at reducing the likelihood of recurrence. These measures range from enhancements in monitoring and alerting, improvements to testing and change-management procedures, adjustments to system configurations and the correction or reconstruction of affected data. Coordination with external service providers to agree and implement follow-up safeguards is also observed, especially when the major incident is caused by a TPP.

28. Overall, the remedial actions seem to reflect a balanced combination of short-term service stabilisation and subsequent structural improvements, consistent with established incident-handling practices. Remedial actions seem also to be correlated with the classification criteria that triggered the major incident reporting.

3.5 Costs incurred

29. FEs are required to specify in the final report the gross direct and indirect costs and losses caused by major incidents, including foregone revenues, costs linked to the replacement of software and remuneration of overtime for staff, amounts due for compensation to customers and for non-compliance with contractual obligations[21]. In addition, the final report must indicate the total amount of financial recoveries, if any[22].

30. Based on the available information, it seems that major incidents had a very limited monetary impact: half of them did not report any direct or indirect costs[23] (almost 40%) or indicated to have suffered a negligible monetary impact, with direct and indirect costs amounting to less than EUR 1,000 (around 10%). An additional 15% did not fill the relevant field.

[21] To estimate costs and losses, FEs should take into consideration the Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34).
[22] In this data fields some data quality issues could not be addressed and therefore less information than for the remaining of the report was used.
[23] It should be noted that according to Q&A 2025_7439, the working time of staff "clearly allocated to the handling of the incident, should count towards staff costs. This consideration also applies where the resources have been earmarked or planned for incident handling in general". Therefore, such results may point to incorrect reporting practices.

31. Similarly, about two thirds of FEs indicated the absence of financial recoveries, while another third provided entries with different reporting logic that could not be reconciled for analytical use[24]. Only a very small share of major incidents, around 3% of the total, reported a positive amount of recoveries.

3.6 Deep dive on selected events

32. By introducing new EU-wide, cross-sectoral requirements for major incident reporting and information sharing across CAs, DORA ensures a better overview of major incidents both at sector and aggregated level. In 2025, two major cross-border events created visible peaks in the reported incidents as highlighted in Section 3.1.

TARGET2 incident (February 2025)

33. On 27 February 2025, TARGET Services experienced a major incident that made T2 and T2S unavailable for approximately 10 and 8 hours respectively and caused around 1 hour of partial disruption in TARGET Instant Payment Settlement (TIPS), with the consequent suspension of securities settlement, payments, ancillary system processing and liquidity transfers for several hours[25].

34. The root cause was found to be the faulty behaviour of a core component of the storage system, an extremely rare hardware malfunction not previously observed worldwide in similar systems. To restore services, the Eurosystem performed a failover to the secondary site and conducted comprehensive integrity checks before resuming operations. The incident resulted in significant delays to T2's operating day, a drop in T2S settlement efficiency, temporary slowdowns in instant payments via TIPS, and some delays to salary and pension payments in certain communities.

35. The event mainly affected the credit and payments sector and the market infrastructures and post-trade sector

Blackout on the Iberian Peninsula (April 2025)

36. On 28 April 2025, at 12.30 CEST, the Spanish electrical grid experienced a total blackout that also impacted Portugal for approximately 10 hours. During this time, while the data centers of major banks and insurance undertakings were able to operate continuously thanks to backup power generators, the volume of operations was significantly lower throughout the day due to disruption at branches and in telecommunication providers.

37. The event mainly impacted the credit and payments sectors, primarily due to the disruption of communication channels. Widespread internet outages impaired clients' ability to access banking services via mobile applications or web platforms (even if they were available and functional), while many branches were left without power or connectivity. In addition, point-of-sale terminals

[24] For instance, some FEs indicated dates (i.e., DD/MM/YYY) instead of monetary amounts.
[25] More details are available here: TARGET Services incident of 27th February 2025.

either ran out of battery or suffered connectivity issues, preventing customers from carrying out day-to-day purchases and payments. Given the widespread impact on branches and telecommunication providers, the overall volume of operations was significantly lower during the day. Electricity supply was largely restored overnight, and by the following day most FEs were operating normally, with only a limited number of branches still affected by residual power or connectivity issues, while online services continued to operate normally throughout the incident.

4. Conclusions

38. This report provides a comprehensive overview of the 3,383 major incidents reported across the EU financial sector in 2025. While improvements in data quality are expected as reporting practices are further consolidated, some conclusions can already be drawn.

39. First, operational disruptions are increasingly borderless and cross-sectoral, reflecting the high level of interconnectedness across sectors and jurisdictions, driven by shared infrastructures, common service providers and cross-border business models.

40. Second, system failures and external events (originating by ICT third-party providers, other financial entities, and infrastructure providers) are the main drivers of major incidents, highlighting the need for robust third-party risk management, effective oversight of outsourced services and close coordination with service providers during incident response and remediation. The presence of system and process-related failures also highlights the importance of robust ICT governance, change management, testing and resilience arrangements.

41. Third, the low frequency of cybersecurity incidents may suggest that existing security safeguards and detection mechanisms were effective in preventing cyber incidents from escalating into major events.

42. Fourth, despite the wide geographical reach of some incidents, the direct impact on clients and transactions was limited in most cases, possibly suggesting that timely detection and effective incident response were generally effective in containing operational harm. Taken together, these findings illustrate both the growing systemic dimension of ICT risk and the importance of continued improvements in resilience, supervision and data quality to strengthen the financial sector's ability to prevent, absorb and recover from future incidents.

43. Finally, the analysis shows that a harmonised framework for major incident reporting is a key element in ensuring timely supervisory awareness of ICT risks, supporting effective coordination among CAs, and strengthening the overall resilience and stability of the EU financial system. Looking ahead, the introduction of a new IT tool in 2026 for the CAs reporting of major incidents to the ESAs, together with automated validation checks and feedback mechanisms, is expected to

significantly improve data quality, collection and processing. In addition, the DORA Register of Information, which centralises ICT contractual arrangements for EU FEs and underpins the designation of critical ICT TPPs[26], will further support additional analysis in conjunction with major incidents reported by FEs to their CAs. Strengthening this linkage will especially support the identification of major incidents originating at the level of critical ICT TPPs and enhance supervisory understanding of systemic ICT risk concentrations across the financial sector.

44. In 2026, the ESAs will continue monitoring and analysing major incidents. Further guidance to CAs will be offered, with a view to support supervisory convergence among CAs on major incident reporting and on the supervision of ICT third-party risk management. Moreover, the ESAs will focus on 'open' incidents, inter alia by supporting CAs in the identification of overdue cases, fostering CAs' follow up actions with FEs, with a view to ensuring the incidents were properly followed up and enhancing compliance with reporting requirements.

[26] See The ESAs designate critical ICT third-party providers.