Official Journal
of the European Union

EN
L series

2024/1772

25.6.2024

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 ([1]), and in particular Article 18(4), third subparagraph, thereof,

Whereas:

(1) Regulation (EU) 2022/2554 aims to harmonise and streamline reporting requirements for ICT-related incidents and for operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions ('incidents'). Considering that the reporting requirements cover 20 different types of financial entities, the classification criteria and the materiality thresholds for determining major incidents and significant cyber threats should be specified in a simple, harmonised and consistent way that takes into account the specificities of the services and activities of all relevant financial entities.

(2) In order to ensure proportionality, the classification criteria and the materiality thresholds should reflect the size and overall risk profile, and the nature, scale and complexity of the services of all financial entities. Moreover, the criteria and materiality thresholds should be designed in such a way that they apply consistently to all financial entities, irrespective of their size and risk profile, and do not pose unproportional reporting burden to smaller financial entities. However, in order to address situations where a significant number of clients are affected by an incident which as such does not exceed the applicable threshold, an absolute threshold mainly targeted at larger financial entities should be set out.

(3) In relation to incident reporting frameworks, which have existed prior to the entry into force of Regulation (EU) 2022/2554, continuity for financial entities should be ensured. Therefore, the classification criteria and materiality thresholds should be aligned with and inspired by the EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 of the European Parliament and of the Council ([2]), the Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories, the ECB/SSM Cyber Incident Reporting Framework and other relevant guidance. The classification criteria and thresholds should also be suitable for the financial entities that have not been subject to incident reporting requirements prior to Regulation (EU) 2022/2554.

(4) With regard to the classification criterion 'amount and number of transactions affected', the notion of transactions is broad and covers different activities and services across the sectorial acts applicable to financial entities. For the purposes of that classification criterion, payment transactions and all forms of exchange of financial instruments, crypto-assets, commodities, or any other assets, also in form of margin, collateral or pledge, both against cash and against any other asset, should be covered. All transactions that involve assets whose value can be expressed in a monetary amount should be considered for classification purposes.

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

([2]) 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, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) The classification criteria should ensure that all relevant types of major incidents are captured. Cyber attacks related to intrusion into network or information systems may not necessarily be captured by many classification criteria. However, they are important since any intrusion in network and information systems may harm the financial entity. Accordingly, the classification criteria 'critical services affected' and 'data losses' should be specified in such a way as to capture these types of major incidents, in particular unauthorised intrusions which, even if the impacts are not immediately known, may lead to serious consequences, in particular data breaches and data leakages.

(6) Since credit institutions are subject both to the framework for classification of incidents under Article 18 of Regulation (EU) 2022/2554 and to the operational risk framework under Commission Delegated Regulation (EU) 2018/959 ([3]), the approach for assessing the economic impact of an incident based on the calculation of costs and losses should, to the greatest possible extent, be consistent across both frameworks to avoid introducing incompatible or contradicting requirements.

(7) The criterion in relation to the geographical spread of an incident set out in Article 18(1), point (c), of Regulation (EU) 2022/2554 should focus on the cross-border impact of the incident, since the impact of an incident on the activities of a financial entity within a single jurisdiction will be captured by the other criteria set out in that Article.

(8) Given that the classification criteria are interdependent and linked to each other, the approach for identifying major incidents which are to be reported in accordance with Article 19(1) of Regulation (EU) 2022/2554 should be based on a combination of criteria, where some criteria that are closely related to the definitions of an ICT-related incident and a major ICT-related incident set out in Article 3(8) and (10) of Regulation (EU) 2022/2554 should have more prominence in the classification of major incidents than other criteria.

(9) With a view to ensure that the reports on and notifications of major incidents received by competent authorities under Article 19(1) of Regulation (EU) 2022/2554 serve both for supervisory purposes and for the prevention of contagion across the financial sector, the materiality thresholds should make it possible to capture major incidents, by focusing, inter alia, on the impact on entity specific critical services, the specific absolute and relative thresholds of clients or financial counterparts, transactions that indicate a material impact on the financial entity, and the significance of the impact in other Member States.

(10) Incidents that affect ICT services or network and information systems that support critical or important functions, or financial services requiring authorisation or malicious unauthorised access to network and information systems that support critical or important functions, should be considered as incidents affecting critical services of the financial entities. Malicious, unauthorised access to network and information systems that support critical or important functions of financial entities poses serious risks to the financial entity and, as they may affect other financial entities, should always be considered as major incidents which are to be reported.

(11) Recurring incidents that are linked through a similar apparent root cause, which individually are not major incidents, can indicate significant deficiencies and weaknesses in the financial entity's incident and risk management procedures. Therefore, recurring incidents should be considered as major collectively where they occur repeatedly over a certain period of time.

(12) Considering that cyber threats can have a negative impact on the financial entity and sector, the significant cyber threats which financial entities may submit should indicate the probability of materialisation and the criticality of the potential impact. Accordingly, to ensure a clear and consistent assessment of the significance of cyber threats, the classification of a cyber threat as significant should be dependent on the likelihood that the classification criteria for major incidents and their threshold would be met if the threat had materialised, on the type of cyber threat and on the information available to the financial entity.

([3]) Commission Delegated Regulation (EU) 2018/959 of 14 March 2018 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council with regard to regulatory technical standards of the specification of the assessment methodology under which competent authorities permit institutions to use Advanced Measurement Approaches for operational risk (OJ L 169, 6.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Considering that competent authorities in other Member States are to be notified of incidents that impact financial entities and customers in their jurisdiction, the assessment of the impact in another jurisdiction in accordance with Article 19(7) of Regulation (EU) 2022/2554 should be based on the root cause of the incident, on potential contagion through third-party providers and on financial market infrastructures, as well as on the impact of the incident on significant groups of clients or financial counterparts.

(14) The reporting and notification processes referred to in Article 19(6) and (7) of Regulation (EU) 2022/2554 should allow the respective recipients to assess the impact of the incidents. Therefore, the transmitted information should cover all details contained in the incident reports submitted by the financial entity to the competent authority.

(15) Where an incident constitutes a personal data breach according to Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]) and Directive 2002/58/EC of the European Parliament and of the Council ([5]), this Regulation should not affect the recording and notification obligations for personal data breaches set out in those Union laws. The competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.

(16) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities, in consultation with the European Union Agency for Cybersecurity (ENISA) and the European Central bank (ECB).

(17) The Joint Committee of the European Supervisory Authorities referred to in Article 54 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([6]), in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([7]) and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([8]) has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential costs and benefits of the proposed standards and requested advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010, the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010, and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010,

([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [9] and delivered an opinion on 24 January 2024,

HAS ADOPTED THIS REGULATION:

CHAPTER I

CLASSIFICATION CRITERIA

Article 1

Clients, financial counterparts and transactions

1. The number of clients affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, shall reflect the number of all affected clients, whether natural or legal persons, that are or were unable to make use of the service provided by the financial entity during the incident or that were adversely impacted by the incident. That number shall also include third parties explicitly covered by the contractual agreement between the financial entity and the client as beneficiaries of the affected service.

2. The number of financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554 shall reflect the number of all affected financial counterparts that have concluded a contractual arrangement with the financial entity.

3. In relation to the relevance of clients and financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial entity shall take into account the extent to which the impact on a client or a financial counterpart will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency.

4. In relation to the amount or number of transactions affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial entity shall take into account all affected transactions involving a monetary amount where at least one part of the transaction is carried out in the Union.

5. Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estimate those numbers or amounts based on available data from comparable reference periods.

Article 2

Reputational impact

1. For the purposes of determining the reputational impact of the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, financial entities shall consider that a reputational impact has occurred where at least one of the following criteria is met:

(a) the incident has been reflected in the media;

(b) the incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships;

(c) the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident;

(d) the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the incident.

[9] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. When assessing the reputational impact of the incident, financial entities shall take into account the level of visibility that the incident has gained or is likely to gain in relation to each criterion listed in paragraph 1.

Article 3

Duration and service downtime

1. Financial entities shall measure the duration of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the incident occurs until the moment when it is resolved.

Where financial entities are unable to determine the moment when the incident occurred, they shall measure the duration of the incident from the moment it was detected. Where financial entities become aware that the incident occurred prior to its detection, they shall measure the duration from the moment the incident is recorded in network or system logs or other data sources.

Where financial entities do not yet know when the incident will be resolved or are unable to verify records in logs or other data sources, they shall apply estimates.

2. Financial entities shall measure the service downtime of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where the service downtime causes a delay in the provision of service after regular activities or operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is fully provided.

Where financial entities are unable to determine the moment when the service downtime started, they shall measure the service downtime from the moment it was detected.

Article 4

Geographical spread

For the purpose of determining the geographical spread with regard to the areas affected by the incident as referred to in Article 18(1), point (c), of Regulation (EU) 2022/2554, financial entities shall assess whether the incident has or had an impact in other Member States, and in particular the significance of the impact in relation to any of the following:

(a) clients and financial counterparts in other Member States;

(b) branches or other financial entities within the group carrying out activities in other Member States;

(c) financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services, to the extent such information is available.

Article 5

Data losses

For the purpose of determining the data losses that the incident entails as referred to in Article 18(1), point (d), of Regulation (EU) 2022/2554, financial entities shall take into account the following:

(a) in relation to the availability of data, whether the incident has rendered the data on demand by the financial entity, its clients or its counterparts temporarily or permanently inaccessible or unusable;

(b) in relation to the authenticity of data, whether the incident has compromised the trustworthiness of the source of data;

(c) in relation to the integrity of data, whether the incident has resulted in non-authorised modification of data that has rendered it inaccurate or incomplete;

(d) in relation to the confidentiality of data, whether the incident has resulted in data having been accessed by or disclosed to an unauthorised party or system.

Article 6

Criticality of services affected

For the purpose of determining the criticality of the services affected as referred to in Article 18(1), point (e), of Regulation (EU) 2022/2554, financial entities shall assess whether the incident:

(a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;

(b) affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities;

(c) constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity.

Article 7

Economic impact

1. For the purpose of determining the economic impact of the incident as referred to in Article 18(1), point (f), of Regulation (EU) 2022/2554, financial entities shall, without accounting for financial recoveries, take into account the following types of direct and indirect costs and losses which they have incurred as a result of the incident:

(a) expropriated funds or financial assets for which they are liable, including assets lost to theft;

(b) costs for replacement or relocation of software, hardware or infrastructure;

(c) staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills;

(d) fees due to non-compliance with contractual obligations;

(e) costs for redress and compensation to customers;

(f) losses due to forgone revenues;

(g) costs associated with internal and external communication;

(h) advisory costs, including costs associated with legal counselling, forensic services and remediation services.

2. Costs and losses referred to in paragraph 1 shall not include costs that are necessary for the day-to-day operation of the business, in particular the following:

(a) costs for general maintenance of infrastructure, equipment, hardware and software, and costs for keeping skills of staff up to date;

(b) internal or external costs to enhance the business after the incident, including upgrades, improvements and risk assessment initiatives;

(c) insurance premiums.

3. Financial entities shall calculate the amounts of costs and losses based on data available at the time of reporting. Where the actual amounts of costs and losses cannot be determined, financial entities shall estimate those amounts.

4. When assessing the economic impact of the incident, financial entities shall sum up the costs and losses referred to in paragraph 1.

CHAPTER II

MAJOR INCIDENTS AND MATERIALITY THRESHOLDS

Article 8

Major incidents

1. An incident shall be considered a major incident for the purposes of Article 19(1) of Regulation (EU) 2022/2554 where it has affected critical services as referred to in Article 6 and where either of the following conditions is fulfilled:

(a) the materiality threshold referred to in Article 9(5), point (b), is met;

(b) two or more of the other materiality thresholds referred to in Articles 9(1) to (6) are met.

2. Recurring incidents that individually are not considered a major incident in accordance with paragraph 1 shall be considered as one major incident where they meet all of the following conditions:

(a) they have occurred at least twice within 6 months;

(b) they have the same apparent root cause as referred to in Article 20, first subparagraph, point (b) of Regulation (EU) 2022/2554;

(c) they collectively fulfil the criteria for being considered a major incident set out in paragraph 1.

Financial entities shall assess the existence of recurring incidents on a monthly basis.

This paragraph does not apply to microenterprises and to financial entities listed in Article 16(1) of Regulation (EU) 2022/2554.

Article 9

Materiality thresholds for determining major incidents

1. The materiality threshold for the criterion 'clients, financial counterparts and transactions' is met where any of the following conditions are fulfilled:

(a) the number of affected clients is higher than 10 % of all clients using the affected service;

(b) the number of affected clients using the affected service is higher than 100 000;

(c) the number of affected financial counterparts is higher than 30 % of all financial counterparts carrying out activities related to the provision of the affected service;

(d) the number of affected transactions is higher than 10 % of the daily average number of transactions carried out by the financial entity related to the affected service;

(e) the amount of affected transactions is higher than 10 % of the daily average value of transactions carried out by the financial entity related to the affected service;

(f) clients or financial counterparts which have been identified as relevant in accordance with Article 1(3) have been affected.

Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estimate those numbers or amounts based on available data from comparable reference periods.

2. The materiality threshold for the criterion 'reputational impact' is met where any of the conditions set out in Article 2, points (a) to (d), are fulfilled.

3. The materiality threshold for the criterion 'duration and service downtime' is met where any of the following conditions are fulfilled:

(a) the duration of the incident is longer than 24 hours;

(b) the service downtime is longer than 2 hours for ICT services that support critical or important functions.

4. The materiality threshold for the criterion 'geographical spread' is met where the incident has an impact in two or more Member States in accordance with Article 4.

5. The materiality threshold for the criterion 'data losses' is met where any of the following conditions are fulfilled:

(a) any impact as referred to in Article 5 on the availability, authenticity, integrity or confidentiality of data has or will have an adverse impact on the implementation of the business objectives of the financial entity or on its ability to meet regulatory requirements;

(b) any successful, malicious and unauthorised access not covered by point (a) occurs to network and information systems, where such access may result in data losses.

6. The materiality threshold for the criterion 'economic impact' is met where the costs and losses incurred by the financial entity due to the incident have exceeded or are likely to exceed 100 000 euro.

CHAPTER III

SIGNIFICANT CYBER THREATS

Article 10

High materiality thresholds for determining significant cyber threats

For the purposes of Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be considered significant where all of the following conditions are fulfilled:

(a) the cyber threat, if materialised, could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third-party providers, clients or financial counterparts, based on information available to the financial entity;

(b) the cyber threat has a high probability of materialisation at the financial entity or at other financial entities, taking into account at least the following elements:

  (i) applicable risks related to the cyber threat referred to in point (a), including potential vulnerabilities of the systems of the financial entity that can be exploited;

  (ii) the capabilities and intent of threat actors to the extent known by the financial entity;

  (iii) the persistence of the threat and any accrued knowledge about incidents that have impacted the financial entity or its third-party provider, clients or financial counterparts;

(c) the cyber threat could, if materialised, meet any of the following:

  (i) the criterion regarding criticality of services set out in Article 18(1), point (e), of Regulation (EU) 2022/2554, as specified in Article 6 of this Regulation;

  (ii) the materiality threshold set out in Article 9(1);

  (iii) the materiality threshold set out in Article 9(4).

Where, depending on the type of cyber threat and available information, the financial entity concludes that the materiality thresholds set out in Article 9(2), (3), (5) and (6) could be met, those thresholds may also be considered.

CHAPTER IV

RELEVANCE OF MAJOR INCIDENTS TO COMPETENT AUTHORITIES IN OTHER MEMBER STATES AND DETAILS OF REPORTS TO BE SHARED WITH OTHER COMPETENT AUTHORITIES

Article 11

Relevance of major incidents to competent authorities in other Member States

The assessment of whether the major incident is relevant for competent authorities in other Member States as referred to in Article 19(7) of Regulation (EU) 2022/2554 shall be based on whether the incident has a root cause originating from another Member State or whether the incident has or has had a significant impact in another Member State in relation to any of the following:

(a) clients or financial counterparts;

(b) a branch of the financial entity or another financial entity within the group;

(c) a financial market infrastructure or a third-party provider which may affect financial entities to which they provide services.

Article 12

Details of major incidents to be shared with other competent authorities

The details of major incidents to be submitted by competent authorities to other competent authorities in accordance with Article 19(6) of Regulation (EU) 2022/2554 and the notifications to be submitted by EBA, ESMA or EIOPA and the ECB to the relevant competent authorities in other Member States in accordance with Article 19(7) of that Regulation shall contain the same level of information, without any anonymisation, as the notifications and reports of major incidents received from financial entities in accordance with Article 19(4) of Regulation (EU) 2022/2554.

CHAPTER V

FINAL PROVISIONS

Article 13

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 13 March 2024.

For the Commission
The President
Ursula VON DER LEYEN