Getting ready for DORA: ICT-related incident management, classification and reporting

In short *This is the fourth edition in a series of AFM publications on the Digital Operational Resilience Act (DORA). This series is intended for all firms that will have to comply with this European regulation from 2025. This edition focuses on ICT-related incidents. In this way, firms can analyse their current status in this regard and what actions they may need to take to ensure compliance with the Regulation.*

1. ICT-related incidents in DORA

DORA aims to ensure that financial firms have better control of ICT risks and are thus more resilient to cyber threats and ICT disruptions. To that effect, the Regulation details several requirements in the area of ICT, including with regard to ICT-related incidents. Firms are already able to analyse their compliance with the DORA requirements in this respect and take action, if needed. They are advised that it is necessary to be in the process of implementation right now in order to be DORA-compliant by 17 January 2025.

To mitigate the impact of ICT-related incidents, it is important that they are adequately detected and handled. The requirements for the management of ICT incidents and cyber threats are set out in Article 17 (Chapter III) of the Regulation. In addition, some of the requirements with regard to ICT-related incident detection and response are elaborated in Chapter III (Articles 23 and 24) of the *Regulatory Technical Standard* (RTS) on ICT Risk Management.[1]

As part of the management process, firms must classify their ICT incidents in a consistent manner so that they can be followed up and handled with due diligence. Article 18 of the Regulation describes how firms should classify ICT-related incidents and what criteria they can use as a basis for determining their impact. These criteria are further explained in the RTS.[2] In addition, this RTS sets out the conditions and circumstances under which ICT-related incidents or cyber threats are classified as major or significant.

Firms should furthermore ensure that all ICT-related incidents that have occurred are recorded. This allows them to review incidents and perform analyses in order to identify the root cause of the incident. DORA requires major ICT-related incidents to be reported to the supervisory authority (this is already mandatory for incidents that pose a serious threat to sound business operations).[3] The Regulation includes general requirements for this reporting. Article 19, for example, explains which reports must be submitted to the supervisory authority and when clients of the financial entity should be informed

1 https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf

2 https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf

3 For investment firms and firms that manage collective investment companies, see also for reference https://www.afm.nl/nl-nl/sector/actueel/2023/mei/deep-dive-incidenten-bo

AFM

of an incident. The RTS and Implementing Technical Standard (ITS)[4] describe in detail what information firms must include in the reports. They also include a template that can be used for reporting major incidents. This edition in our series of publications is based on the RTS/ITS as published at the time of writing. Since the content of these RTS/ITS has yet to be finalised, it is possible that certain changes might yet be made to their wording, although it is common for a text to remain broadly the same.

In the following sections we will address the management and classification of ICT-related incidents and cyber threats and the areas that entities can already start working on in order to meet the DORA requirements. We will also briefly discuss how firms can report ICT-related incidents and cyber threats to the AFM.

Table 1

Further elaborations	Subject	Completed
RTS for Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	Already submitted to EC
RTS for Article 18(3)	Classification of ICT-related incidents and cyber threats	Already submitted to EC
RTS for Article 20(a)	Reporting content and templates	No later than 17 July 2024
ITS for Article 20(b)	ITS to establish the reporting details for major ICT-related incidents	No later than 17 July 2024

4 JC_2023_70_-_CP_on_draft_RTS_and_ITS_on_major_incident_reporting_under_DORA.pdf (europa.eu)

2. Getting started on ICT incidents

ICT-related incident management

Firms can already start working on:
- Establishing and implementing an ICT-related incident management process.

Article 17 of the Regulation sets out the requirements for the ICT-related incident management process. The management process helps firms to adequately detect, report and handle ICT-related incidents. Firms should establish and implement appropriate policies and procedures to minimise the impact of these incidents. Chapter III (Articles 22 and 23) of the RTS on ICT Risk Management provides further information on what firms should include in their ICT-related incident management policy and what mechanisms they should implement to detect and respond to incidents.

The ICT-related incident policy should enable firms to implement technical, organisational and operational mechanisms to support the ICT-related incident management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours. In addition, firms should establish a list of persons with internal functions and external stakeholders that are directly involved in ICT operations' security in the ICT-related incident policy. This should include the persons responsible for detecting and monitoring cyber threats, detecting anomalous activities and vulnerability management. Firms should establish and implement processes and methods to analyse significant or recurring ICT-related incidents.

The ICT-related incident management policy ensures the recording and consistent monitoring, handling and follow-up of all ICT-related incidents, to ensure that root causes are identified, documented and addressed. By establishing and implementing an effective policy in this area, firms can minimise the likelihood of incidents recurring.

Another aim of the management policy is to put in place plans for communication towards internal staff, external stakeholders and the media, in accordance with the communication policy (see also Article 14 of the Regulation), and to ensure that major ICT-related incidents are reported to the relevant management staff.

To ensure an effective detection of and response to ICT-related incidents and anomalies, it is important that the roles and responsibilities in this area are clearly defined and communicated within the organisation. In addition, firms should implement detection mechanisms that enable them to:
- collect, monitor and analyse internal and external factors, including system log information;
- collect, monitor and analyse potential internal and external cyber threats, including frequent scenarios;
- collect, monitor and analyse information about third-party ICT-related incidents;
- identify anomalous activities and behaviours and put in place tools for generating alerts for anomalies;
- record, analyse and review relevant information on all anomalous activities.

As the incident reports contain important (and often confidential) information, it is crucial that this and other relevant information about the incident are stored securely and protected from unauthorised access and alteration. In addition, key information about the incident, such as the date and time the anomaly occurred and the type of incident, must be recorded in a log file. Finally, the ICT-related incident procedure must be initiated where there are indications of unauthorised activity on an ICT system or network or where there are indications that an ICT system or network is no longer secure. Other instances in which the ICT-related incident procedure should be followed are in case of loss of data and system or network outage. In this regard, due account must be taken of the criticality of the services affected.

Classification of ICT-related incidents

Firms can already start working on:
- Establishing - and implementing - procedures describing how incidents are classified.

A proper system of classification of ICT-related incidents and cyber threats is essential to ensure an effective management process. This helps firms to determine the resources needed to address and resolve the incident. It also helps in communicating the status and expectations to stakeholders within the organisation. Firms may determine their own incident classification criteria, provided that they enable a distinction to be made between major incidents, cyber threats and all other incidents (low impact, medium impact, etc.).

For the purpose of classifying ICT-related incidents, firms should use various criteria that help determine the impact of the incident on the organisation and external stakeholders. These criteria are:
- The number and relevance of clients affected by the incident. The clients concerned are those who use the firm's services or the financial counterparts with whom the firm has a contractual arrangement. In addition, firms should determine the extent to which the impact of the incident affecting clients also affects the firm's own business objective. Finally, the relevance of a client is determined by considering the client's impact on the firm's ability to achieve its objectives;
- The data losses that the ICT-related incident entails. For this purpose, firms need to determine whether data are still accessible (availability), whether the data are inaccurate or incomplete (integrity) and whether the data have been accessed or disclosed by unauthorised users (confidentiality);
- The criticality of the services affected for the firm's operations. This is the case if the incident affected ICT services that support important or critical business functions;
- The reputational impact caused by the incident. Firms determine the reputational impact by considering how much market attention the incident received. This may include, among other things, investigating whether the incident received media coverage, whether complaints were received from clients or whether the firm is unable to comply with legal requirements as a result of the incident;
- The duration of the incident. The firm determines this by measuring the time that elapsed between the occurrence and the resolution of the incident. If the precise moment of occurrence cannot be determined, the firm can instead take the moment when the incident was established or the time it was recorded in log files or other data sources. If the precise time of resolution is unknown, firms may make an estimate to determine when the incident will be resolved;
- The geographical spread with regard to the areas affected by the incident. In order to determine the geographical spread, among other things firms assess the impact of the incident on the clients, other offices or institutions within the group in at least two EU Member States;
- The economic impact of the incident in absolute and relative terms, in particular direct and indirect costs and losses stemming from the incident.

If one or more of the criteria cannot be determined with certainty, an estimate should be made using the available data.

To determine whether the ICT-related incident should be classified as a major incident, the firm should consider the criteria on which the incident had a material impact. The first step is to determine whether the incident affected the firm's critical services. If this is not the case, there is no major incident. If critical services are affected, the incident should be classified as a major incident in case of successful, malicious, and unauthorize access to network and information systems, which may result to data losses. In addition, an incident will be classified as a major incident if it has had a material impact on two or more of the criteria mentioned above. Detailed explanations regarding material impact are provided for each criterion in the RTS[5]. Recurring ICT-related incidents, even if not individually classified as major, can still be classified as major if they occur more frequently within a three-month period. For this to be the case, the incident must occur more than twice, have the

5 https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf

same cause and have a similar impact. Cyber threats are classified as significant when the threat has an impact on the critical or important business functions of the firm, other financial institutions, third parties or clients. In addition, the likelihood of the cyber threat actually materialising should be considerable. Finally, the cyberthreat must have a material impact on the criteria in the list above, in the event that the threat materialises. If the cyber threat meets all the conditions, it must be classified as significant.

Table 2

Further elaborations	Description	Completed
RTS for Article 18(3)	Classification of ICT-related incidents and cyber threats	Already submitted to EC

Reporting of major ICT-related incidents and notification of significant cyber threats

Firms can already start working on:
- Making preparations for reporting on major ICT-related incidents in a timely manner

An ICT-related incident that is classified as major must be reported to the supervisory authority. Based on the report, the supervisory authority can implement the appropriate follow-up actions and measures and prevent the incident from having an adverse impact on the remainder of the sector. Where the incident also has an impact on the financial interests of their clients, firms must inform them about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of the incident. In addition to mandatory ICT-related incident reporting, firms may also, on a voluntary basis, notify significant cyber threats to the supervisory authority when they deem the threat to be of relevance to the remainder of the financial sector, financial service users or their clients. The requirements for reporting ICT-related incidents and notifying cyber threats are set out in Article 19 of the Regulation and Articles 20(a) and 20(b) of the RTS/ITS for incident reporting. They also specify what firms should include in the incident report.

Initial notification

Once a firm determines (based on the criteria in the previous section) that a major ICT-related incident has occurred, it must submit an initial notification to the supervisory authority. The time limit for doing so is 4 hours from the moment the incident is classified as major, and a maximum of 24 hours after the incident is first detected. When submitting the initial notification, firms shall provide the general information about the incident, such as the description of the incident, the date and time of detection of the incident and the classification of the incident (including the assessment of the aforementioned criteria). Furthermore, it is important that the firm provides information on how the incident was discovered, whether the incident is recurring as well as information about the source (cause) of the incident. If possible, firms should also provide an indication whether a business continuity plan has been activated as a result of the incident and whether the incident has had an impact on other financial institutions and third parties.

Intermediate report

Following the initial notification, firms should also submit an intermediate report to the supervisory authority in the event of major ICT-related incidents. The intermediate report must be submitted within 72 hours of the classification of the incident or as soon as regular activities have been recovered to levels as they were prior to the incident. As with the initial notification, firms should include in the intermediate report information about the date and time of detection of the incident and the criteria that were used to determine that it concerned a major incident. The firm should also describe the type of incident and provide information about affected functional areas, such as business processes and infrastructure components supporting business processes. The intermediate report should additionally include an indication whether a communication about the incident to clients has taken place as well as information about temporary measures and actions taken by the firm to recover from the incident. Finally, it is important that firms provide information about the consequences of the incident. For this, firms must examine

whether vulnerabilities have been exploited and whether there are any indications that IT systems or the IT infrastructure can no longer be used securely.

Final report

No later than one month after the classification of the incident, the firm should submit a final report to the supervisory authority. If the incident has not been resolved by that time, the final report should be submitted no later than one day after the incident is finally resolved. The final report should include the date and time when the incident was resolved, information about the root cause of the incident and information about the firm's inability to comply with legal requirements and contractual arrangements/SLAs (where applicable). The final report should also include information on the measures and actions taken by the firm for the resolution of the incident and, together with additional controls, to prevent similar incidents in the future. It is also important for the firm to provide information about direct and indirect costs stemming from the incident.

Notification of significant cyber threats

In addition to (mandatory) major ICT-related incident reporting, firms may also, on a voluntary basis, notify significant cyber threats to the supervisory authority. If they choose to make a notification, it is important that key information about the cyber threat is shared with the supervisory authority. This information consists of the date and time of detection of the significant cyber threat, a description of the cyber threat and the status of the cyber threat. In addition, it is important that the firm provides information about the potential impact of the cyber threat on the entity and a description of the actions taken to prevent the materialisation of the threat. Where clients have potentially been affected by the cyber threat, firms have an obligation to inform them of appropriate protection measures and actions they can take.

The AFM is currently developing an online environment where firms can report their ICT-related incidents and identified cyber threats. This online environment will be part of the AFM Portal[6] (which supervised entities can access). Entities that will fall under the scope of DORA and are subject to supervision by the AFM will be able to upload reports and notifications on outsourcing, significant ICT-related incidents and cyber threats to the AFM Portal from 17 January 2025. Entities can submit the initial notification with regard to ICT-related incidents to the AFM via the Portal. Upon submission of the initial notification, the incident will appear in the overview with all previous reports from the same entity. The intermediate report and the final report will be automatically linked to the incident upon submission of the necessary documents by the entity. Finally, the Portal will display an overview of outstanding actions. The entity will be informed in the event that additional documents have to be submitted.

Table 3

Further elaborations	Description	Completed
RTS for Article 20(a)	Reporting content and templates	No later than 17 July 2024
ITS for Article 20(b)	ITS to establish the reporting details for major ICT-related incidents	No later than 17 July 2024

6 https://portaal.afm.nl/

3. Outlook

At this time, the first as well as the second batch of RTSs and ITSs have both been published. The first batch (including that for Article 18(1)) has already been submitted to the European Commission for assessment and decision-making; the European Commission's decision is expected in July 2024. The second batch was submitted by the ESAs to firms in the financial sector for consultation. This batch will probably be submitted to the European Commission in the third quarter of 2024.

In the meantime, the AFM will continue its preparations for conducting DORA supervision. The next publication in this series will consider the testing of digital operational resilience. The next edition will be published in the third quarter of 2024.

For further elaboration on ICT-related incidents in DORA, the following pages can be consulted: https://www.afm.nl/en/sector/themas/belangrijke-europese-wet--en-regelgeving/dora/rts-en-formulieren and https://www.afm.nl/en/sector/themas/belangrijke-europese-wet--en-regelgeving/dora/melden

If you have any further questions, please contact the AFM Business Desk.