January 2025

DORA Incident Management Guide

rootly × 

rootly

#Contents

Abbreviations

CA	Competent authority
CTPP	Critical third-party provder
DORA	Digital Operatinal Resiliece Act (Regulation EU 2022/2554)
ESAs	European Supervisory Authorities
EU	European Union
FE	Financial entity
ITS	Implementing Technical Standards
NIS2	Network and Information Security (Directive EU 2022/2555)
RTS	Regulatory Technical Standards
TPP	Third-party provider

1. Purpose of this guide

Whether you're a financial entity in the midst of preparing for DORA or a critical third-party provider, there will be something in this guide for you. The core focus of this guide will be on incident management in relation to DORA. This guide will cover the key details for incident reporting, management and classification. It will equip you with the knowledge necessary for your DORA compliance journey and provide practical solutions on how to integrate DORA into your existing incident management process.

2. What's DORA and why should I care?

The Digital Operational Resilience Act (DORA) is an EU regulation that came into force on the 17th January 2025. For financial entities with operations in the EU, DORA should already be on the radar as the regulation came into force in 2023. For those unfamiliar with the regulation, we will provide a short overview of what DORA entails and why it's needed.

Fig 1: DORA timeline

What's the aim of DORA?

DORA aims to ensure that the financial sector within the EU is resilient and can weather severe operational digital disruption. The regulation will contribute to regulatory harmonisation, strengthen security and improve information sharing within the financial services sector and between the ESAs.

Why is DORA needed?

Major disruption to FEs not only impacts the financial sector but can have knock on effects on the rest of the economy. Increasingly, the financial sector is relying on external TPPs to provide tools and services that are critical to their operations and product offerings. This poses a risk as TPPs are not subjected to the same regulation or oversight as FEs. In addition to introducing obligations on financial entities and CTPPs, DORA also introduces obligations on the supervisory competent authorities with respect to risk.

DORA in a nutshell

The key pillars of DORA provides a simple overview of the regulation (EU) 2022/2554:

1. **ICT Risk Management** (Articles 5 -16)
2. **ICT Related Incident Management, Classification and Reporting** (Articles 17-23)
3. **Digital Operational Resilience Testing** (Articles 24-27)
4. **Managing of ICT Third Party Risk** (Articles 28-44)
    a. Oversight of critical third-party providers
5. **Information Sharing Agreements** (Articles 45-49)

Fig 2: DORA Key Pillars

If you want to know more about the key pillars of DORA - refer to this blog post.

Who is in scope for DORA?

DORA applies to 20 different types of financial entities, ranging from crypto-asset service providers to investment firms. DORA also applies to the critical third-party providers to these financial entity types. A comprehensive list of financial entities types in scope of DORA can be found here.

Some financial entity types will be excluded from the scope of DORA e.g. micro/small insurance intermediaries. Take a moment to check whether DORA directly applies to your organisation or whether you are classed as a CTPP.

Key DORA Players

Competent Authorities

The competent authorities are responsible for regulating and supervising the financial entities in each EU member state.

You can find the full list of CAs here.

European Supervisory Authorities

The ESA is made up of three supervisory bodies:

- European Banking Authority (EBA)
- European Securities and Markets Authority (ESMA)
- European Insurance and Occupational Pensions Authority (EIOPA)

And a board that monitors systemic risk:

- European Systemic Risk Board (ESRB)

Financial Entities

Organisation that operate in the financial sector that are regulated by the CAs.

You can find the full list of FEs types that are in scope of DORA here.

Critical Third Party Providers

Companies that provide services that support critical or important functions in FEs.

Implications for non-compliance

It shouldn't come as a surprise that there are implications under DORA for non-compliance. The enforcement of penalties, including fines, will be at the discretion of the competent authorities. There is currently no maximum penalty defined in the regulation - Article 50 states that "penalties and measures shall be effective, proportionate and dissuasive". If you are a non-compliant CTPP, you could be subjected to a periodic penalty payment up to 1 % of the average daily worldwide turnover[3].

Another implication to consider is the suspension (temporarily or completely) of the use of a CTPP until any risks identified by the CA have been addressed. In some cases, FEs will be required to terminate contracts with their CTPPs. This could result in disruption to your operations if alternative solutions to a CTPPs service are unavailable. If you are a CTPP, contract terminations could negatively impact your revenue and business model if your primary client base are FEs.

Non-compliance can lead to reputational damage for CTPPs and FEs alike. The CAs will publish on their official websites who they decide to impose a penalty on. This can lead to damaging business relationships and market confidence.

3. Incident Management under DORA

The drive to make the European financial sector more resilient has been an ongoing priority for the EU. In order for financial services to provide continued service and maintain the trust of consumers and the market, FEs need to demonstrate that they can recover quickly from cyber breaches and incidents.

DORA is looking to establish harmonisation across the sector for the reporting of major ICT-related incidents and significant cyber threats. It's aiming to:

- **Provide FEs with an understanding of the landscape of threats and incidents that they may encounter**
- **Provide CAs with the information required to respond to the risks and threats impacting the financial sector**

Aside from the regulatory text, there are a number of documents published by the ESAs that contain more information about the technical and implementation details regarding incident management. Highlighted below are some of the key DORA and incident management documents.

DORA Level 1 Regulation and Directive

- Directive (EU) 2022/2556: this is the legislative act that outlines the goal that EU countries need to achieve[4].
- Regulation (EU) 2022/2554: this is the binding legislative act that is implemented across the EU[4]. The key articles for incident management, classification and reporting are covered in Chapter 3 - Articles 17 - 23.

DORA Level 2 Text for Incident Management

The delegated regulation EU 2024/1772 supplements DORA regulation 2022/2554, here you will find more of the nitty gritty details for incident management, reporting and classification. For

those tasked with implementing DORA incident management protocols in their organisations, the level 2 text should be considered mandatory reading.

- Commission Delegated Regulation (EU) 2024/1772: this covers the criteria for the classification of incidents and cyber threats.

The draft RTS and ITS will be the document that provides you with detailed information about the contents of each of the reports that are required to be submitted:

- DRAFT Regulatory Technical Standards (RTS) and Implementing Technical standards (ITS)
    - The RTS outlines what the content of the initial notification and reports should be for major incidents and significant cyber threats. It also covers the reporting time lines.
    - The ITS provides the standard forms, templates and procedures for reporting major incidents and notification of significant cyber threats.

For a deeper understanding of how to categorise major incidents under DORA, refer to:

- DRAFT Regulatory Technical Standards (RTS) specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under DORA

What is classified as a major incident under DORA?

The ESAs have specified the criteria for classifying major incidents under DORA in the delegated regulation EU 2024/1772. This should be your reference for a detailed breakdown of the classification criteria and materiality thresholds. In the following section we will provide a brief overview of how to classify a major incident under DORA.

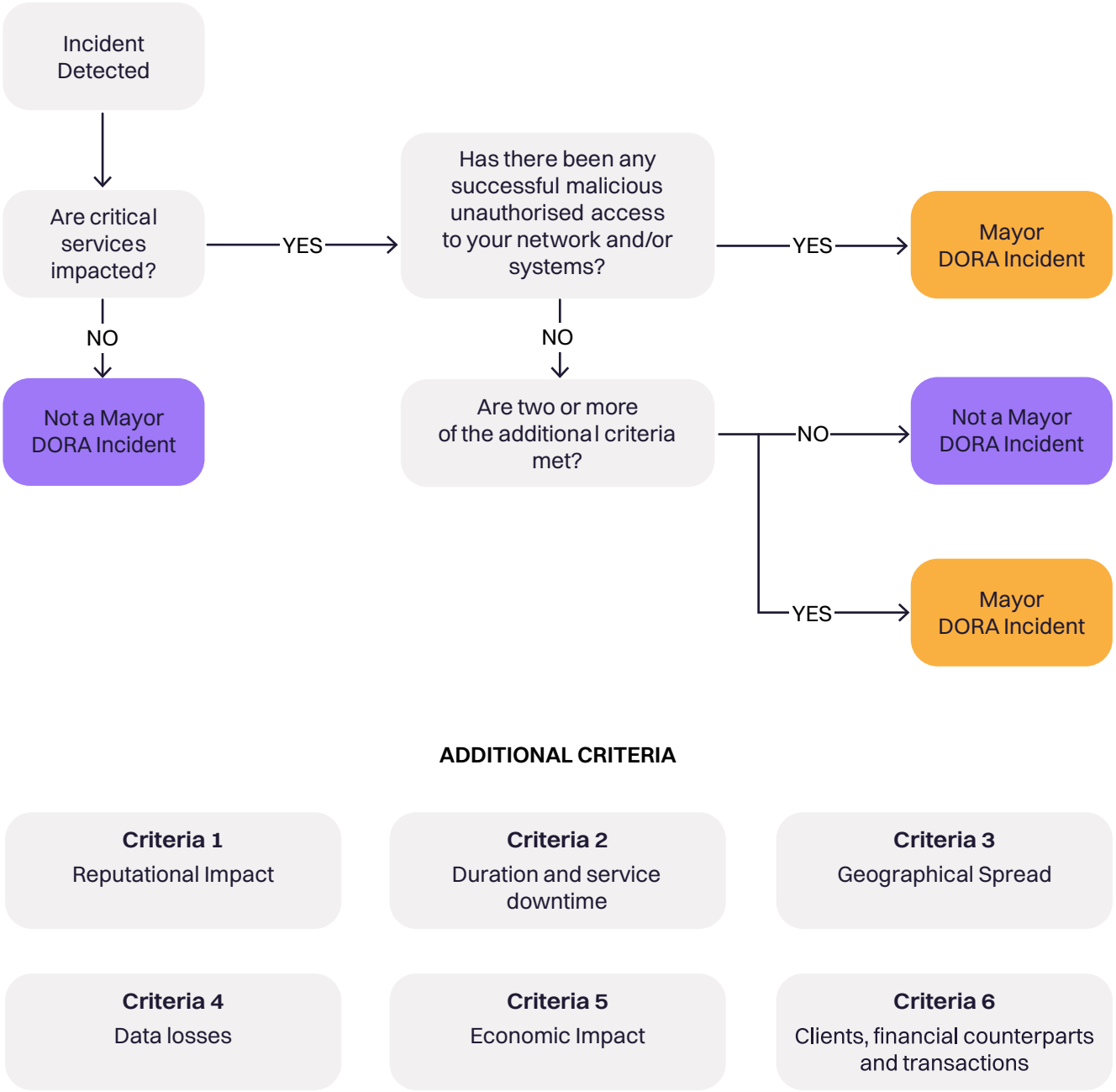

Fig 3: DORA major incident classification flow chart

For an incident to be classified under DORA as major, it needs to fulfil either one of the mandatory conditions and potentially additional criteria.

The mandatory conditions are:

- If your network or critical services are successfully accessed by unauthorised and malicious actors then the incident is classified as major.
- If critical services are impacted but not because of unauthorised access, two or more of the additional criteria needs to be met. The six additional criteria are as follows:

1. Reputational Impact

(Article 2, Delegated Regulation (EU) 2024/1772)

At least **one** of the following criteria has to be met:

- You are unable or unlikely to meet regulatory requirements as a result of the incident
- You are likely going to lose clients as a result of the incident which could have a material impact on your business
- The incident has been in the media
- The incident has resulted in repetitive complaints about your services by different clients or industry peers

ⓘ *When evaluating whether the criteria for reputational impact has been met, consider the level of visibility the incident has already gained or will gain.*

2. Duration and service downtime

(Article 3, Delegated Regulation (EU) 2024/1772)

This criteria will be met when (Article 11, Delegated Regulation (EU) 2024/1772):

- The incident **duration exceeds 24 hours**; or
- The critical service or function is **down** for **more than 2 hours**

ⓘ *If an incident occurs outside of business hours - do you have out-of-hours support to recover your critical services?*

The incident duration is measured from when the incident occurs until the moment the incident has been resolved. If you don't know when the incident occurred, measure the duration from when the incident has been detected.

The service downtime is measured from when the service becomes partially or completely unavailable to your clients until the service has been fully restored to its pre-incident state.

Rootly captures critical incident metrics like service level objective (SLO) and service recovery time (SRT). Benefit from an integrated status page to surface real-time service downtime information internally and externally, ensuring transparency with customers and stakeholders.

3. Geographical Spread

(Article 4, Delegated Regulation (EU) 2024/1772)

The criteria for geographical spread (Article 12, Delegated Regulation (EU) 2024/1772) is met if at least two EU member states are impacted by the incident.

Do you operate in more than one EU member state and do your branches share critical services? If so, have you considered isolating your critical services so that if they fail the repercussions are localised and don't progate across borders?

4. Data Losses

(Article 5, Delegated Regulation (EU) 2024/1772)

The criteria will be met if either of the below occur (Article 13):

- If the incident impacts the availability, authenticity, integrity or confidentiality of data that will have or has negatively affected the financial entities business or the ability for the entity to meet regulatory requirements
- If the incident results in data losses due to unauthorised access to network systems or services

Consider the following:

- *Does your business continuity plan cover large scale data loss?*
- *Do you have the appropiate backups in place?*
- *What is classified as critical data for your organisation?*
- *How will you recover any critical data?*
- *Have you tested your data recovery protocols?*
- *Do you know how long it will take you to recover your data?*
- *Would you know who has had unauthorised access to your data, when they have had access and what they accessed?*

5. Economic Impact

(Article 7, Delegated Regulation (EU) 2024/1772)

The criteria will be met if the incident will incur costs and losses that are anticipated to be greater than €100,000 (Article 14, Delegated Regulation (EU) 2024/1772).

An example of a cost incurred would be if you have to replace any hardware infrastructure as a result of the incident. For the full list of costs and losses that need to be taken into account refer to Article 7 of Delegated Regulation (EU) 2024/1772.

6. Clients, financial counterparts and transactions

(Article 1, Delegated Regulation (EU) 2024/1772)

The criteria will be met if any of the following circumstances are satisfied (Article 9, Delegated Regulation (EU) 2024/1772):

- The number of impacted clients using the affected service is **>10%** of all clients or exceeds **100,000 impacted clients**
- The number of impacted financial counterparts is **>30%** of all the financial counterparts dependent on the affected service
- The number of impacted transactions is **>10%** of your daily average number transactions or daily average value of transactions*

*at least one part of the transaction has to have been carried out in the EU!

Can you use your existing monitoring tools to track whether criteria 6 has been met? Do you have alerting in place to notify your teams when you exceed the thresholds?

Incident reporting obligations

Financial entities and critical third party suppliers are expected to submit three reports for ICT-related incidents that have been classified as major. DORA clearly outlines the reporting timelines for each report and FEs are expected to be ready to meet these reporting obligations from 17th January 2025.

The reports will inform whether the ESAs need to coordinate response at an EU level. Your CA will conduct the initial assessment, taking into account whether the incident will impact multiple financial entities, consumers or the wider financial sector. They may then engage with the ESAs to inform them of the severity and impact of the incident. Depending on the nature of the incident they may inform other authorities to co-ordinate a national or EU wide response.

Unlike the reporting of major incidents, the notification of significant cyber threats is voluntary under DORA. Any information that is provided will inform supervisory response. Financial entities can also choose to report cyber threats to their country specific cyber security and incident response centres (like the National Cyber Response Centre in Germany) rather than via the DORA route.

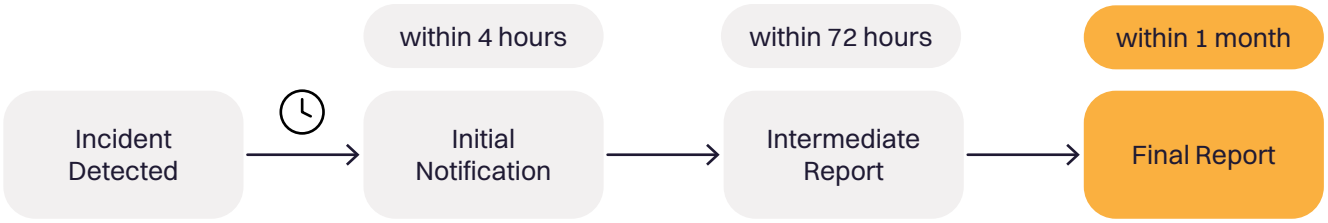

Fig 4: Reporting timeline

1. Initial Notification - within 4 hours[5]

The initial notification should be submitted as early as possible and no later than 24 hours after you know about the incident. The expectation is that the report will be submitted within 4 hours from the time the incident has been classified as major.

Gain granular visibility into each incident with a comprehensive timeline of events. Precisely track and analyze the exact moment an incident was classified as major, enabling data-driven insights and improved incident response strategies.

2. Intermediate report - within 72 hours[5]

The intermediate report should be submitted no later than 72 hours from when the initial notification has been submitted. Even if there is no status change or updates since the submission of the initial notification, within 72 hours, you are expected to submit the intermediate report. When the incident has been resolved, you are expected to submit an updated intermediate report.

3. Final report - within 1 month[5]

The final report should be submitted within 1 month from the submission of the latest updated intermediate report.

If the time limit for submission of any of the reports falls on a weekend or public holiday (in the country of the reporting entity), you have an extension and can submit the reports by 12 (midday) of the next working day.

However, there are some exceptions as the time limits set out above won't apply to to the following FE types[6]:

- Credit institutions
- Central counterparties
- Operators of trading venues
- Any financial entity that has been identified as essential
- Any important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555
- Any financial entity that is classified as significant or systemic by their CA

If you fall into any of the above FE types, you are expected to comply with the standard reporting time limits even on the weekend and public holidays.

Do you require out-of-hours support to cover your critical services on weekends and public holidays?

Incident re-classification

DORA caters for cases of incident re-classification as what might start as a minor incident could evolve into a major one and vice versa. Further investigation during an incident's lifecycle can provide us with a better understanding of the scale and impact of the incident, which can in turn inform the classification.

If an incident classification changes and becomes major during its life cycle, the financial entity is required to submit the initial notification within the 4 hour time frame after the re-classification. The submission of the following reports follow the standard timelines and deadlines. If an incident is classified as major but re-classified as non-major at a later date, the financial entity is expected to inform the competent authority.

Rootly provides a complete audit trail of incident modifications. Easily view the history of reclassifications, including the responsible user and timestamp, ensuring accountability and facilitating comprehensive post-incident analysis.

Incident reporting scope

All the reports include a selection of mandatory and non-mandatory fields with the detail of information required increasing with each report. The ESAs have provided templates for the major incident and cyber threat reports. The content of the reports have been streamlined after the ESAs public consultation of the draft RTS and ITS concerning incident management.

Initial Notification

The initial notification is the shortest report. The aim is to gather the minimum amount of information required so that the CA can assess whether the incident will result in wider impact, while not hindering the incident response. You will be expected to provide basic information, such as:

- a short description of the incident
- when the incident was detected and classified as major

- what criteria resulted in the incident being classified as major

You will be expected to indicate whether the incident was caused by the FE or a TPP.

Leverage Rootly's incident workflow design to automate data capture from initial incident declaration. Minimize manual input and maximize data accuracy for comprehensive reporting and analysis.

Intermediate Report

The intermediate report is more involved as it's expected that you will have more information at hand when you are further along the incident lifecycle. You will be expected to provide information about the impact of the incident such as how many clients were impacted, the number of transactions affected etc. If you don't have the exact numbers at this point in time, estimates are acceptable. If the incident has been resolved at this point, you will be asked for the incident duration and to describe the actions that have been taken to recover from the incident.

Final Report

The contents of the final report is focused on understanding the root cause of the incident and resolution. If you have already conducted a post-incident review, you should have the relevant information readily at hand. If there have been costs and losses as a result of the incident, you will be required to provide further details in this report.

ⓘ *Arrange your post-incident reviews right after the incident. This has many benefits:*

The incident is fresh in people's minds and your team will remember the details of the incident. The resulting post-incident report is likely to be richer in detail and more exact.

Understanding the root cause is prioritised by your teams and any follow up actions are mitigated early on to reduce the risk of recurring incidents.

Bonus - you can reuse the relevant information captured in the post-incident review in the final report.

For more details with regards to the reporting scope and requirements refer to the ITS[7]

Rootly integrates seamlessly with platforms like Notion and Confluence, enabling post-incident report management within your preferred environment. Utilize customizable templates and AI-powered assistance to streamline reporting and accelerate learning from incidents.

Incident reporting process

DORA incident reports are required to be submitted within the time limits stated in the above section on reporting obligations. You can submit two or all the reports together if you have resolved the incident and conducted the root cause analysis within the timelines outlined[8].

Notifications requirements

The reports need to be submitted to your CA in the member state that you are operating in. Your CA should inform you about how to submit your reports using 'secure electronic channels'. If you are unclear about what the secure channels are, reach out to your competent authority to find out more.

ⓘ *Example: The Central Bank of Ireland has a portal for submissions - the Central Bank Portal. This portal is already in use for regulatory reporting and will be used for DORA reporting[11].*

If you are an FE and decide to outsource your incident reporting to a third-party you will need to let your CA know and provide them with some information about the third-party - name, contact information and identification code. You should inform your CA before the TPP raises any reports on your behalf and when you decide to no longer outsource your reporting to them[5].

If you are a CTPP submitting reports on behalf of an FE and don't have a pre-existing relationship with the CA, reach out to them to understand how to submit reports.

Recurring incidents

An incident is usually classed as recurring if it has the same root cause and occurs more than once. Recurring incidents often indicate that the underlying problem that results in the incident

has not been mitigated. Under DORA, incidents need to meet the below criteria to be classed as recurring:

- Occurred twice within 6 months
- Have the same root cause

If both criteria are met, the incidents collectively are categorised as a major incident under DORA and you will be required to report on them[10].

ⓘ *There are some financial entities (e.g. microenterprises) that will be excluded from reporting recurring incidents so please check whether this will apply to your financial entity type!*

Utilize Rootly's custom tagging to categorize incidents effectively. Improve identification of recurring issues, enabling targeted remediation efforts and proactive prevention strategies

Aggregated reporting

Aggregate reporting aims to reduce the reporting burden and duplication of reports for major incidents. Aggregate reports will be practical for incidents that are caused by third-parties and impact many financial entities. If you are a FE and most of your incidents originate from your third-party providers, you may be sighing with relief - but don't let your guard down as there are some conditions that need to be met before your third-party can submit reports on your behalf.

So, what is aggregating reporting? Aggregated reporting allows third-parties, that have reporting obligations outsourced to by FEs, to submit a single set of reports for major incidents to the CA that impact numerous entities. The major incident must originate or be caused by the TPP in order for them to submit reports for all the impacted entities.

ⓘ *Bear in mind your CA can request that you submit an independent report so don't be complacent even if a major incident has been caused by a TPP!*

The conditions that need to be met for aggregate reporting to take place are as follows[12]:

- **Every FE** included in the aggregated report independently classifies the incident as **major**
- The incident **originates** or is caused by a **TPP**
- The **CA** has been **notified** of reporting obligations outsourced to the TPP by the FE

- The CA has **explicitly granted** the FE permission for aggregate reporting
- The incident impacts FEs in a **single EU member state** and the entities are supervised by the **same CA**
- The third-party provider provides its services to **multiple financial entities** (or group) in one EU member state

If you are a third-party provider, submitting an aggregated report will require collaboration and good communication with the FEs that you work with so that you can gather any required information in a timely manner.

If an incident's geographical spread is across more than one EU member state, you will need to file an aggregate report to each CA and be approved to do so by each CA. Plan ahead accordingly if you want to use aggregate reporting for DORA incident management.

If you are one of the below FE types, you will be expected to submit an independent set of reports to the CA, even if an outsourced third party is submitting an aggregated report[12]:

- Significant credit institution
- Central counterparties
- Operators of trading venues

Applying incident management best practices to DORA

DORA expects that the FEs establish incident management processes so that they can record major incidents and cyber threats. The CAs expect that FEs engage with them in an open and transparent manner in order to assess whether there are extensive systemic risks. The expectations are relatively standard and you may be already implementing many of these processes. Here is what is expected of FEs [13] :

- Monitoring in place to detect and identify incidents when they occur.
- Processes in place to record and classify an incident when detected
- Incident roles and responsibilities assigned during an incident.
- Communications plans in place should you need to notify customers or financial counterparts of service disruptions.

    - You should also have established internal communication procedures if incidents require escalation or expertise from another team.
- Processes in place to inform relevant senior management of major incidents to ensure that they are aware of the impact, resolutions and controls that may be required as a result.
- Operational and technical playbooks in place to ensure services are restored in a timely manner.
- Processes in place to follow up post-incident to ensure that root cause analysis is carried out and documented to prevent recurring incidents.

Rootly streamlines incident workflows and facilitate compliance with reporting processes like DORA. Benefit from integrated on-call capabilities, ensuring reliable and timely team notification upon incident detection, minimizing downtime and maximizing response efficiency.

Let's dive deeper into each stage of the incident lifecycle and take a look at how to integrate DORA requirements into your existing incident workflows.

Monitoring and Detection

Incidents can be detected from a multitude of sources - externally by your customers or internally by automated monitoring systems. For DORA reporting, make sure you have identified your critical services and monitoring is in place to detect when these services degrade. For reporting purposes, ensure you capture the timestamps of when an incident has been detected and when you classify it as major under DORA.

Familiarising yourself with the criteria and materiality thresholds of when an incident is a major under DORA is a helpful guide to understanding what monitors to put in place. This leads us to the next stage - incident classification.

Incident Classification

Earlier in this guide we have discussed the classification criteria for major DORA incidents. Take some time to understand and document how your existing incident classifications map to DORA's. A major incident under DORA won't necessarily map to what you classify internally as major.

Creating a shared understanding of the severity and priority of incidents is vital to ensuring appropriate incident response. Provide clear guidance to your teams so they understand how to classify major DORA incidents and are equipped to kick off the processes for DORA reporting in a timely manner.

Communications

> *Financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate."*[14]

Internal and external communications are important aspects of incident management. Make sure the teams that are managing incidents understand how to communicate to external customers, financial counterparts and regulators during major incidents. It can range from updating an external status page to informing account executives to communicating with customers directly.

Internally your team needs to be able to work together and have a platform to communicate during incidents - this could be a messaging tool or conference call or a mix of both. You might even have internal status pages that provide real time information to internal stakeholders of the status of critical services.

Ensure that key contact details are documented and shared with the relevant teams. It's useful to document critical service providers, key client stakeholders and regulator contact details. If you are delayed in submitting your DORA reports, your team should know how to inform the CA of the delay and agree on an extension.

In the next section on roles and responsibilities we will discuss the importance of assigning a communications lead / scribe to an incident.

Roles and Responsibilities

Every organisation will have their own protocols for managing incidents, workflows will differ depending on the size and complexity of the organisation. If you are a small organisation you might want everyone to lend a helping hand during a major incident. If you are a larger organisation, coordinating a large number of people during an incident and numerous threads of information can be tough. Rather, have a focused group that are assigned clear roles and responsibilities. Pull in expertise as and when needed for more efficient incident response and resolution.

Rootly simplifies incident role assignment and responsibilities. Integrated workflows within communication platforms like Slack and MS Teams enable effortless identification of incident managers and their roles. Key information is readily accessible via pinned incident channels and Rootly bot queries, fostering seamless collaboration and efficient coordination.

Managing a major incident is akin to navigating stormy seas, you want to have a seasoned captain at the helm - to steer the team in the right direction, keep pace and make the optimum calls. Consider assigning an incident commander when the incident is raised. Anyone participating or observing the incident should be able to ascertain who the commander is with ease. The commander will be responsible for ensuring that incident response runs smoothly and post-incident processes are conducted, such as root cause analysis and follow up actions.

The commander doesn't have to be the person that identifies the incident - evaluate what the incident size and scope is and delegate accordingly. If you have an out-of-hours or global team, ideally assign the role to a team member that can see the incident through to the end. If an incident is long running, consider tag-teaming and handing over the commander role.

The commander should at all times understand the state of the incident, what investigations or actions are in progress and what the next steps are to move the incident towards resolution. Coordinating collaboration across different teams and ensuring the right stakeholders are notified and pulled in when necessary is also part of the commander's role. With a commander at the helm, everyone participating in the incident should have a clear idea about what they should be doing (assigned actions) and there shouldn't be duplication of work.

For major incidents, some organisations might consider having a rota of major incident commanders. This group of individuals may consist of more senior members of technical,

product or management staff that have the authority and expertise to make critical decisions. Consider providing the major incident commanders more extensive training on handling major incidents and business continuity protocols.

> *"At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose."*[14]

There are often a lot of moving parts during an incident and the main focus should be on restoring service. In the heat of an incident communications can be an afterthought, which is why we recommend assigning a communications lead/ scribe to focus on the comms. It's good practice for the communication lead to provide regular updates - internally and externally when required. There are various benefits:

- Stakeholders can stay up to date with the progression of the incident without having to ask for status updates or debriefs - they can self-serve by reading the updates in an incident channel or status page
- You build the timeline of events in real time which means you have the information at hand for documenting the post-incident review and for any other reporting requirements
- Internal and external parties that are impacted by the incident can utilise the information from the updates to mitigate any potential impact to their services

If there is widespread impact to external customers, you may require an account executive or customer service lead to coordinate communications to customers.

For certain domains or types of incidents you may require other roles and expertise. For DORA you may have a Risk and Compliance lead that understands the reporting requirements in depth, is responsible for the reporting process and managing the communications with the CA.

Service Recovery

It's good practice to have operational and technical playbooks at hand so that your teams can swiftly recover from incidents. You will encounter scenarios that you won't have planned for and will be dependent on the ability of your team to recover services and minimize downtime. Nonetheless, it can be indispensable to have playbooks for failure scenarios that you can plan for and learnings obtained from past incidents.

A lot of factors play into the speed of service recovery, the complexity can grow with organisation size and technical footprint. Some points to consider when thinking about improving service recovery:

- Do you have good monitoring in place to detect incidents early on?
- Does your team need to be trained so that they are familiar with incident response protocols?
- Is your incident management workflow easy to use?
- Do you have experienced team members with domain expertise and a good understanding of how to restore your critical services?
- Do you need to consider the design of your critical systems - can they failover or self-heal?
- Are you able to restore data from backups or other means should you encounter data loss?
- Do you have alternatives in place if a CTPP fails - can a process fallback to manual workaround or are you dependent on a CTPP to recover before you can recover?

One of criteria for classifying whether an incident is major under DORA is the downtime of critical services. If your critical service downtime exceeds 2 hours or if the duration of the incident is over 24 hours - it would meet the criteria. Review your past incidents and evaluate which incidents would have met the criteria - what could have been done to reduce the time to recover?

Reporting

> *"As DORA does not provide for a transitional period, the ESAs emphasise the importance for financial entities to adopt a robust, structured approach in order to meet their obligations in a timely manner."*[1]

It's important to reiterate that the aim of DORA is regulatory harmonisation - FEs have many reporting requirements and DORA will actually supersede some of them. One example being that DORA will be the lex specialis for the financial sector for the NIS2 framework[2]. There won't be a transitional period for DORA, FEs need to be ready to classify and report major incidents when DORA is applied.

As part of your DORA readiness preparation, you should have identified your CTPPs as part of the groundwork for the register of information (ROI). These are the TPPs that are supporting critical and important functions that underpin your ability to operate. If your FE type is permitted

to use aggregated reporting, consider reaching out to your CTPPs to discuss whether they are planning and prepared to submit aggregated reports should they have a major DORA incident. Remember to inform your CA of the CTPPs that will be submitting aggregate reports and gain their approval.

Consider assigning a reporting lead for major incidents - this might be someone from the compliance team or part of the incident commander responsibility. Once you have decided, document and share this information with your team.

Post-incident protocols

After an incident when service has been restored, it's advisable to take the time to carry out a root cause analysis, document your findings and assign any post-incident actions. Keeping a log of your past incidents is beneficial as it provides reference material for your team to learn from past incidents. Post-incident documents can be shared with senior management if they need to be briefed on major incidents. The information captured in your post-incident document should contain relevant material to help complete your DORA final report.

Understanding the root cause of an incident is vital to ensure you take appropriate actions to prevent recurring incidents. Once you have identified the actions, prioritise completing the actions to decrease the risk of recurring incidents. Remember that under DORA non-major incidents can be classified as major if they occur twice or more during a six month period and have the same root cause. Consider how you will capture and surface recurring incidents with the same root cause within a six month period to stay compliant with DORA reporting requirements.

4. How to prepare your team for effective incident management

So far we have covered the nuts and bolts of incident management under DORA, the following section will cover how to prepare your teams to effectively manage incidents.

Incident management tooling

Using a reliable incident management platform can improve your team's incident response so you can recover faster from service disruption. During an incident the number of things that need to be done can quickly add up. For example, your communication lead is posting an update to the status page, an engineer is investigating some logs and your compliance lead pulled in to submit the initial notification for DORA. Keeping track of all the tasks can be challenging.

It's beneficial if your incident management tooling allows you to do the following:

- Allows for you to classify incidents and supports custom classification types
- Create custom incident workflows depending on the classification of incident
- Send notifications and reminders when important tasks are due
- Assign tasks to different people in your organisation during an incident and keep track of what has or hasn't been done
- Assign roles and responsibilities and allow for creating custom roles
- Integrate with your monitoring and paging systems
- Provide support for generating post-incident review documents

Training and awareness

In many organisations understanding incoming regulatory requirements is often left to a subset of teams such as compliance, risk or legal departments. While it makes sense that there are go-to people that understand regulation in depth, it's also beneficial to ensure that relevant teams have a basic understanding of incoming regulation that can impact day-to-day operations or how products are built.

So who needs to know about DORA? This will depend on how your organisation and incident management processes are structured. In some organisations all software engineering teams are empowered to raise incidents and expected to resolve incidents within their domain, whereas in other organisations there are dedicated operations teams who are responsible for incident response. Some organisations outsource certain types of incident resolution, such as security operations, to external companies.

The first step to figuring out who to raise awareness to is to understand who in your organisation will be involved in the classification and incident resolution process. Take a note of the teams and/or personas so that you can target who you train. The list of personas could look something like:

- Software or IT engineer that adopts the incident commander role during incidents and partakes in the root cause analysis
- Site Reliability Engineer that is on-call and responsible for out-of-hours support
- Customer Support Engineer that raises incidents from issues detected by customers
- Compliance team member that manages the relationship with the CAs
- Legal team member that is responsible for managing contractual agreements with TPPs
- Security Operations engineer that is on the front line for resolving cyber threats

Once you have figured out who to train, decide on how you want to raise awareness and carry out the training. If you already have existing incident management training processes - that's great, including DORA relevant material shouldn't require too much work. If your processes are less established, it might be a good time to take action and consider how to improve your incident response.

Here are some suggestions for a few key resources that are useful to have documented and shared with your team:

- Overview of your incident management process
- The expectations and responsibilities for each incident role
    - Include information about who is responsible for submitting DORA reports to the CA

- Communications plan
- Existing incident classifications and how they map to DORA incident classification for major incidents
- DORA major incident criteria and materiality thresholds
- Brief explanation of what the DORA regulation is and what the reporting requirements are
- Guidelines on how to submit DORA reports and the reporting timelines
- Overview of what your critical services are and your CTPPs

Once you have developed these resources, make them mandatory reading as part of your incident response training.

As part of operational resilience testing, you are likely to have mapped out your critical flows and likely failure scenarios for your product and services. Consider using these scenarios in your incident training to simulate what a major outage to critical services would look like. Not only will it make incident response training more engaging but it will also help identify potential gaps in operational processes or your product.

ⓘ *Using a service catalogue can provide teams with a one stop shop to easily visualise and identify which services are critical. This is especially helpful if your product is backed by many services and teams.*

The exercise to categorise which services are critical or part of a critical flow can be complicated to figure out in larger organisations - involve team members with product and technical domain expertise to collaborate on mapping this out.

Use past incidents as inspiration for mock incidents and training. Review some past incidents to evaluate which would be classified as major under DORA and which would not. It's a simple exercise that can improve your incident commanders ability to classify DORA major incidents vs internal high priority incidents. Have your teams try out the different roles during the mock incidents so they can gain experience before attempting to adopt a certain role in the heat of an incident.

5. Conclusion

While DORA introduces reporting requirements for major incidents, the incident management protocols outlined in DORA should coexist with your existing incident management processes. Non-compliance with DORA can result in penalties, reputational damage and the termination of contracts with CTPPs.

Some recommended actions to align your organisation with DORA incident management requirements:

- Familiarise yourself with the classification criteria for major DORA incidents
- Take note of the reporting time limits
- Understand what information needs to go into the reports
- Find out how to submit your reports to your CA
- Document what your critical services are
- Document your CTPPs and reach out to them if you are outsourcing any reporting
- Raise awareness and train your teams to respond to major DORA incidents

The impact of the DORA incident requirements will vary depending on how mature your incident management processes are. For some organisations, the reporting burden may actually decrease if they only need to report their incidents under DORA. For other organisations, DORA may be a chance to increase the maturity of their incident management processes.

Embrace DORA as an opportunity to strengthen your operational resiliency. Take the chance to contribute to the information sharing opportunities to improve the understanding of EU wide incidents.

#Appendices

1. https://www.esma.europa.eu/sites/default/files/2024-12/JC_2024_99_ESAs_Statement_on_DORA_application.pdf
2. https://www.centralbank.ie/news/article/speech-implementing-dora-speech-by-gerry-cross--director-of-financial-regulation-policy-and-risk-23-nov-2023
3. **Article 35 (8), EU Regulation** 2022/2554
4. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_
5. ITS Article 6, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
6. ITS Article 6 (5), https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
7. **ITS starts from page 21**, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
8. ITS Article 2, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
9. ITS Article 3, https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
10. **RTS Article 15,** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Repo rt_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf
11. https://www.centralbank.ie/docs/default-source/regulation/dora/dora-industry-event-slides.pdf?sfvrsn=88f5671a_3
12. **RTS Article 7,** https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf
13. **Article 17, EU Regulation** 2022/2554
14. **Article 14, EU Regulation** 2022/2554


rootly