SUPERVISION DORA UPDATE 6

DORA outlook: What to expect in the coming year

In short This is the last 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 what to expect in 2025. We will also address a number of practical matters.

1. Introduction

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. It is important to complete the process of implementation of the DORA requirements as soon as possible in order to be DORA-compliant by 17 January 2025.

DORA will enter into force on 17 January 2025. As of that date, all financial firms that are subject to DORA must comply with the requirements in the Regulation as well as further regulations. In past editions, we have consistently focused on a specific aspect of DORA and discussed what firms need to do. In this last edition, we will outline what firms can expect in 2025. We will explain how the AFM will conduct its supervision of DORA and what requests for information firms can expect to receive from European supervisory authorities (EIOPA, ESMA and EBA – together the ESAs). In this edition, we will also discuss a number of practical matters, such as how firms should submit information to the AFM.

Throughout the past year, the ESAs have been actively working on developing *Regulatory Technical Standards* (RTS) and *Implementing Technical Standards* (ITS). The RTSs and ITSs have been divided into two batches and all have now been submitted to the European Commission. The European Commission makes the final decision on whether or not to adopt these further regulations. The RTSs and ITSs in the first batch have already been adopted and are therefore final. Part of the first batch is the ITS for the *register of information,* which was recently adopted by the European Commission. Regarding the RTSs and ITSs in the second batch, a decision has yet to be made by the European Commission. However, it is expected that they will remain broadly unchanged.

To ensure timely compliance with DORA, firms should have already begun implementing the requirements in the Regulation and the RTSs and should be utilising the templates in the ITSs. Since the further regulations will remain broadly the same, firms can already start working on implementing these requirements. Firms that wait for the European Commission's decision before commencing implementation are unlikely to meet the DORA requirements in time.

AFM

2. Outlook 2025

2.1 What to expect in 2025

Firms can already start working on:
- Filling the register of information.
- Putting in place processes to report incidents.

Once DORA comes into force, national supervisory authorities will begin their supervisory activities related to DORA. This will include establishing reviews to determine whether firms are complying with the requirements, as well as collecting and verifying information requested by the ESAs.

Register of information

The first data request that firms can expect in 2025 concerns the register of information. The deadline for the first submission of registers of information by the national supervisory authorities to the ESAs is set for 30 April 2025. To ensure timely submission of the registers to the ESAs, soon after DORA comes into force the AFM will send a request for information to all organisations with an AFM licence that are subject to DORA. Firms should therefore already be working on preparing their register of information so that it can be shared in a timely manner. During the preparation process, it is important to verify that all mandatory fields are included in the register of information. If any fields are missing or incomplete, the register cannot be shared with the ESAs. In such cases, the firm will have to share the entire register of information with the supervisory authority again.

The AFM and DNB will request the entire register of information from firms each year. The AFM and DNB will then verify that all the fields in the registers of information are complete before forwarding the registers to the ESAs. It is therefore important to ensure the registers are complete before they are shared with the AFM or DNB.

Based on the information from the registers, the ESAs will designate ICT third-party service providers that are considered critical for the financial sector. The ESAs base the designation of critical ICT third-party service providers on the systemic impact on the stability, continuity, or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large-scale operational failure to provide its services. The ESAs also base the designation of critical ICT third-party service providers on the importance of the financial entities to the sector that rely on the relevant ICT third-party service provider. Finally, account is taken of the reliance of financial entities on the ICT services provided and the degree of substitutability of the ICT third-party service provider. The ESAs will supervise the designated critical ICT third-party service providers. Chapter 5, Section 2 (Articles 31-44) of the Regulation sets out, among other things, the responsibilities and powers of the ESAs that will supervise these critical ICT third-party service providers. This Chapter also sets out the manner in which the supervision of these service providers can be conducted.

ICT-related incidents

Firms are also obliged to report major ICT-related incidents. When an ICT-related incident has occurred, firms must determine on the basis of criteria[1] whether a major ICT-related incident has occurred. Once a firm determines that a major ICT-related incident has occurred, it must notify the relevant supervisory authority (AFM or DNB) within 4 hours. Based on the initial notification and follow-up reports, the European or national supervisory authority can determine whether it concerns an ICT-related incident affecting the entire sector. Based on this assessment, the supervisory authority can determine whether additional measures need to be taken. In addition, firms can notify significant cyber threats on a voluntary basis.

1 For the classification of ICT-related incidents, see the RTS (Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS))

TLPT

A number of firms will be identified for *threat-led penetration testing* (TLPT). In addition to the obligations referred to above, these firms are also subject to additional requirements with regard to testing the digital operational resilience. Firms only have to comply with these requirements if notified by the supervisory authority by means of a designation letter. Once the RTS for TLPT is approved by the European Commission, the AFM will contact the firms identified for TLPT. The timing of the test will be scheduled in consultation with the relevant firm.

2.2 What will the AFM do?

Firms can already start working on:
- Verifying access to the DORA Portal.

Like many firms, the AFM has been preparing for the implementation of DORA over the past two and a half years. Much of this programme consisted of preparing the sector for DORA, by means of various publications (such as the DORA updates), conversations with firms during seminars and one-to-one contacts with organisations.

In addition, the AFM has been making internal preparations for the supervision of DORA. This included developing a DORA Portal where firms can submit notifications to the AFM. In addition, a considerable amount of time has been spent preparing our supervisors for DORA. The DORA programme at the AFM will be concluded in the first quarter of 2025. From then on, the AFM will transition to a steady state of DORA supervision. From that moment, our supervisory activities will largely consist of conducting reviews, handling ICT-related incidents, processing the register of information and assessing licence applications.

DORA reviews

To determine whether firms are complying with the requirements under DORA, thematic reviews as well as institution-specific reviews will be conducted. In a thematic review, a number of firms will be selected and the focus will be on a specific aspect of DORA. This could be a review of business continuity management, for example, or inspecting contractual agreements with ICT third-party service providers.

During an institution-specific review, only one firm will be selected and documents will be requested that relate to an aspect of DORA (e.g. ICT risk management or digital operational resilience testing). This type of review may vary from one institution to the next. In both cases, the guiding principle remains that supervision will be conducted according to a risk-based and proportionate approach. This means that the AFM will deploy supervisory capacity where the greatest risks are expected.

Reporting

A second aspect of our DORA supervision is dealing with ICT-related incident reports. Once a major ICT-related incident has occurred, firms must submit an initial notification via the DORA Portal within 4 hours from the moment the incident is classified as major. In addition, an intermediate report and final report must be submitted to the AFM within 72 hours and 1 month, respectively, of the classification of the incident.

The AFM will assess the completeness of the incident report when analysing these reports. It will also assess whether the incident, and its impact, are adequately described in the report. Where this is not the case, the AFM will seek additional information to determine these facts. In addition to major ICT-related incident reporting, financial undertakings may also, on a voluntary basis, notify cyber threats. Both types of reports will mainly be used to determine whether ICT-related incidents have occurred or there are active cyber threats that impact, or could potentially impact, the financial sector.

New contractual agreements with ICT third-party service providers should also be notified to the AFM. Like ICT-related incidents and cyber threats, these can be notified via the DORA Portal. When notifying a contractual agreement with an ICT third-party service provider, firms have the option of indicating whether this concerns a new agreement or there is an existing agreement in which the function supported by this ICT service has become important or critical. Depending on this choice, firms will be asked about the type of ICT service being outsourced or the function that has become important or critical. As with major ICT-related incidents, the AFM will assess the notification and may request additional information.

Financial undertakings with an AFM licence that are subject to DORA will be able to access the DORA page in the AFM Portal from 17 January 2025. This will be part of the AFM Portal that firms are already able to access. If you are unable to access the DORA page on 17 January 2025, it is important that you notify this in a timely manner so that you will be able to submit the mandatory reports and notifications via this Portal.

Licence applications

Since 1 August 2024, the AFM has been testing various DORA requirements during the licence application process for firms that will be subject to DORA. This has been done with the aim of supporting firms obtaining a licence in the run-up to January 2025 in ensuring their timely compliance with the DORA requirements. As part of the licence application process, the AFM assesses, among other things, whether certain policies and procedures that are mandatory under DORA are in place. After 17 January 2025, the AFM will continue to assess these requirements during licence applications. Therefore, it can be advantageous, prior to the licence application, to determine which DORA requirements the firm will have to comply with. During the licence application process, directors will be evaluated on their knowledge and skills in understanding and assessing ICT risks. DORA expects directors to possess this knowledge and these skills and to follow specific training on a regular basis that will enable them to adequately manage ICT risks.

TLPT

Once the TLPT RTS have been adopted by the European Commission, the AFM will notify firms identified for TLPT that they are required to carry out a mandatory TLPT. Next, the AFM's test managers will consult the firm to determine in which period this test should be carried out. The test managers will assist the firm during the preparation and execution phases of the test to ensure that the test complies with the requirements in the Regulation and the RTS. All the reports to be shared with the test managers as part of the test should be submitted in the DORA Portal. After (successful) completion of the test, the firm receives a certificate, which can be used to demonstrate compliance with the requirements related to TLPT.

3. Outlook

This was the last edition in the AFM's series of DORA updates. In the coming period, the latest RTS and ITS will be assessed by the European Commission. For more information on the latest legislative and regulatory developments, please visit the DORA page on the AFM website. You can also monitor developments on the websites of the ESAs:

- Digital Operational Resilience Act (DORA) - AFM
- Digital Operational Resilience Act (DORA) - EBA
- Digital Operational Resilience Act (DORA) - EIOPA
- Digital Operational Resilience Act (DORA) - ESMA

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