REPORT ANALYSIS

DORA-update 7

In short - Over the past eighteen months, many financial firms have focused on implementing the Digital Operational Resilience Act (DORA). From submitting the registers of information and gaining the first experiences with DORA supervision, to navigating further clarifications within the underlying regulatory framework, the sector has made significant progress in a relatively short period. At the same time, several areas for improvement remain, providing firms with opportunities to further strengthen their operational resilience and DORA compliance. In this DORA update, we reflect on the key developments, experiences, and important considerations since the introduction of DORA.

AUGUST | 2026

AFM

Table of Contents

1. DORA register of information

Information request

The AFM has requested the registers of information from all entities subject to DORA on two occasions. During the first reporting exercise, 40% of the registers were accepted by the European Banking Authority (EBA). In 2026, this acceptance rate increased significantly to 94%.

The register of information was the first (and largest) reporting exercise that firms faced after DORA became applicable. During this annual exercise, the EBA requests all national competent authorities to collect the registers of information of DORA-regulated entities and submit them to the EBA. The EBA subsequently uses these registers to identify critical ICT third-party service providers (CTPPs) that will fall under the direct oversight of the European Supervisory Authorities (see "DORA Oversight activities" below).

As firms were required to submit their registers of information in the first quarter of 2025, there was still uncertainty regarding the xBRL-CSV format and how the register should be filled. To facilitate the first reporting cycle, we decided, as a one-off measure, to perform the conversion to xBRL-CSV on behalf of firms. This allowed companies to submit their register of information in Excel format, enabling them to focus on the accuracy and completeness of the underlying data. Ultimately, 40% of the registers submitted in 2025 were accepted by the EBA.

For the 2026 submission, firms were required to submit their registers of information directly in xBRL-CSV format. At the same time, we configured our internal process so that the registers were automatically submitted to the EBA and the feedback was automatically retrieved. As a result, companies were able to submit a new version as often as necessary. In 2026, 94% of the registers of information were accepted by the EBA. This increase compared with 2025 can partly be explained by firms having a better understanding of the exercise and its requirements following their first reporting experience. In addition, we observed that many firms engaged external service providers in 2026 to support the xBRL-CSV conversion process and assist with completing the register.

Q&A session

During the 2026 submission exercise, we organised a Q&A session that provided firms with an opportunity to ask questions about the register of information. The objective was to answer as many questions as possible. The session also helped us identify the key challenges firms encountered when completing the register.

Following the submission deadline, we analysed both the questions raised during the session and the submitted registers to identify the most common errors and their solutions. Based on this analysis, we compiled an overview of frequently encountered errors and guidance on how to resolve them. This overview has been included in the Questions and Answers from the Q&A Session (PDF, 240 kB).[1]

[1] https://www.afm.nl/~/profmedia/files/onderwerpen/dora/20260305-qa-dora-sessie.pdf

DORA Oversight activities

Based on their analysis of the registers of information submitted across the Member States, the European Supervisory Authorities (EBA, EIOPA and ESMA—collectively, the ESAs) have designated nineteen critical ICT third-party service providers.[2] These entities are subject to direct oversight by the ESAs under the DORA Oversight Framework. As a national competent authority, the AFM contributes to Joint Examination Teams (JETs) that carry out DORA oversight activities at various CTPPs.

DORA oversight activities can be divided into the following categories:

- Ongoing monitoring. This includes periodic information gathering and continuous engagement with CTPPs regarding their current operational resilience, risk profile, and emerging issues, such as operational incidents or new threats.
- General investigations. These are more in-depth reviews of specific risk areas. They are conducted in accordance with the oversight work programme and focus on addressing newly identified concerns or assessing remediation measures implemented following previous reviews.
- Inspections. Inspections are similar to general investigations but are more intrusive and aimed at a detailed assessment of risks posed by service providers to financial entities. They include powers to request files, data and other relevant documentation.
- Requests for information. This tool allows supervisors to request information from CTPPs without initiating a comprehensive assessment or inspection. Information requests may be used, for example, to clarify a specific situation that requires additional information or explanation from the provider.
- Recommendations. Recommendations address identified deficiencies at a CTPP within specific assessment areas. Follow-up on recommendations takes place through ongoing monitoring and reporting, in which the measures taken and improvements implemented in response to the recommendations are described.

Further information on DORA oversight activities can be found in the guidance previously published by the ESAs.[3]

[2] The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act | European Banking Authority.

[3] JC 2025 29 Guide on DORA oversight activities

2. DORA supervision

In 2025, our supervision of compliance with the DORA requirements focused on ICT risk management (Chapter II of the Regulation). During our inspections, we requested and reviewed firms' policies and procedures to assess the extent to which they comply with DORA requirements. We observed that financial entities do not always have all the policies and procedures in place that are required under DORA. In addition, not all submitted policies and procedures met the requirements set out in the Regulation and in Commission Delegated Regulation (EU) 2024/1774.

We therefore recommend that firms periodically conduct a self-assessment to determine whether their existing policies and procedures comply with DORA requirements. By doing so on a regular basis, for example, as part of the mandatory review of the ICT risk management framework, financial entities can also ensure that their policies and procedures are aligned with current risks and the actual operating practices of the organisation.

Furthermore, we note that financial entities that are part of a larger group often rely on policies and procedures developed at group level. In many cases, this is more efficient than having individual entities within the group develop their own policies. However, the DORA-regulated entity (i.e., the licensed entity) remains fully responsible for compliance with DORA requirements. It is therefore important for firms to verify independently that all relevant DORA requirements have been fully incorporated into their policies and procedures.

Finally, we observe that most firms have implemented sufficient measures to detect (potential) disruptions in a timely manner. At the same time, we see that firms often have not yet established adequate preventive measures to avoid such disruptions. In particular, there is still room for improvement in the areas of logical access management and patch and vulnerability management.

TLPT

The first financial entities began conducting Threat-Led Penetration Testing (TLPT) in 2025. These are comprehensive tests that emulate the tactics, techniques, and procedures used in practice by real-world threat actors (such as hackers). The tests are carried out under the supervision of the AFM's TLPT test managers.

Firms designated by the AFM to perform TLPT are required to conduct tests periodically and ensure that they comply with the requirements set out in DORA. Throughout the testing process, the DORA TLPT test managers verify that the activities are performed in accordance with the requirements contained in the Commission Delegated Regulation (EU) 2025/1190.[4] Upon completion of the test, firms receive an attestation confirming that they have successfully carried out a TLPT exercise.

After the test has been completed, the results, including the Test Summary and the Remediation Plan, are shared with the AFM's supervisory departments. This enables the findings and the implementation of the remediation plan to be monitored and followed up.

[4] Delegated regulation - EU - 2025/1190 - EN - EUR-Lex

DORA notifications

In 2025, we received 123 DORA notifications from DORA-regulated entities under our supervision. Of these, 65 notifications related to major ICT-related incidents. Another 54 notifications concerned new contractual arrangements with ICT service providers. Four notifications involved significant cyber threats.

As the number of reported incidents remains below our expectations, we recommend that firms review their incident management processes to ensure they are properly designed and implemented. In particular, it is important that these processes enable incidents to be detected, recorded, managed, classified, and reported in a timely manner.

Three types of notifications

DORA distinguishes between three types of notifications that firms must or may submit to their competent supervisory authority on an ongoing basis. The first type concerns major ICT-related incidents. These must be reported no later than four hours after the incident has been classified as major, or within 24 hours of its detection, whichever comes first. An intermediate report must then be submitted within 72 hours of the initial notification. A final report must be provided no later than one month after the incident has been classified.

Given these strict deadlines, it is important for firms to design their incident management processes in such a way that mandatory notifications can be submitted to the supervisory authority within the required timeframes.

In addition to incident reporting, DORA requires firms to report, at least annually, all new contractual arrangements concluded with third-party ICT service providers. Finally, firms may, on a voluntary basis, report significant cyber threats that are relevant to the financial sector.

Further information on the obligations relating to DORA notifications can be found in Articles 18, 19, and 28(3) of the Regulation, as well as in the delegated regulation on the reporting of major ICT-related incidents and significant cyber threats[5].

[5] Delegated regulation - EU - 2025/301 - EN - EUR-Lex

3. Developments for insurance intermediaries

For a long time, there was uncertainty regarding how to determine whether insurance intermediaries fall within the scope of DORA. The European Supervisory Authorities (ESAs) have now provided further clarification on this matter in Q&A DORA099[6] and DORA237[7].

The Regulation includes an exemption for small and medium-sized insurance intermediaries (fewer than 250 employees and an annual turnover of less than EUR 50 million and/or a balance sheet total of less than EUR 43 million). Since insurance mediation constitutes only a limited part of the activities of some insurance intermediaries, questions arose as to how these criteria should be applied to entities for which insurance mediation is not their primary activity. In addition, there was uncertainty regarding how the number of employees, annual turnover, and total balance sheet should be calculated for entities that are part of a group.

Q&A DORA237 addresses the question of how the number of employees, annual turnover, and balance sheet total should be calculated when insurance mediation represents only a limited part of an undertaking's overall activities. EIOPA's response indicates that, in general, the figures for the undertaking as a whole should be considered. However, in accordance with the principle of proportionality, entities whose insurance mediation activities are only of limited significance should consider solely the activities and resources dedicated to those insurance-related activities.

For insurance intermediaries that are part of a group, it must first be determined whether the group is a financial group or a non-financial group. Where an undertaking forms part of a non-financial group, only the individual undertaking should be assessed. For financial entities that are part of a financial group, consideration must be given to the participation they hold in other undertakings, or the participation that other undertakings hold in them.

Where an undertaking holds between 25% and 50% of the shares or voting rights of another undertaking, the undertakings are classified as partner entities. In such cases, the number of employees, annual turnover, and total balance sheet of the partner entity must be included on a pro rata basis when calculating the relevant thresholds. In the case of linked entities, where there is a majority shareholding or control, the number of employees, annual turnover, and balance sheet total of the linked entity must be included in full when calculating those thresholds.

[6] 3100 - DORA099 - European Insurance and Occupational Pensions Authority
[7] DORA237 - 3350 - European Insurance and Occupational Pensions Authority

4. Outlook

For more information on regulatory developments, please consult the **DORA page** on the AFM website. In addition, you may wish to monitor developments on the websites of the European Supervisory Authorities (ESAs):

- 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.

Links to previous publications:
Publications
Handelssystemen vragen om scherpere ICT-risicobeheersing onder DORA
Effective management requires more than just policy