REPORT ANALYSIS

DORA in practice: observations and recommendations on ICT risk management framework

In short – The importance of financial markets' digital resilience grows as the digitalisation and complexity of financial markets increases. Against this background, the Digital Operational Resilience Act (DORA) was introduced to strengthen the digital operational resilience of financial entities. DORA has been fully applicable since January 2025. The AFM conducted a thematic review of trading venues' compliance with ICT risk management framework requirements under DORA. In this report, the AFM shares its observations and recommendations to raise awareness and support improvements across the sector.

JUNE | 2026

AFM

Management Summery

The increasing digitalization and complexity of financial markets have significantly increased their reliance on resilient ICT systems. ICT disruptions, cyber incidents and system failures can disrupt trading, undermine market confidence and pose risks to market integrity. To address these risks in a harmonized manner across the European Union, the Digital Operational Resilience Act (DORA) entered into full application in January 2025. DORA sets uniform requirements for financial entities, including trading venues, to strengthen their digital operational resilience.

Digital operational resilience is a key priority in the AFM's supervisory strategy for 2023–2026. As ICT risk management is a core pillar of DORA and fundamental to resilient and orderly market infrastructures, the AFM conducted a thematic review of trading venues' compliance with the ICT risk management framework requirements under DORA. This review marks the starting point of the AFM's DORA-related thematic supervision.

The thematic review assessed the design of ICT risk management framework policies and procedures of four trading venues against the requirements set out in Commission Delegated Regulation (EU) 2024/1774 supplementing DORA. To obtain a broad view of compliance while limiting supervisory burden, the AFM focused on the design of controls. Trading venues were requested to submit relevant documentation and were given the opportunity to clarify and supplement their submissions during the review process.

The AFM observed that trading venues generally have an extensive set of ICT-related policies and procedures in place and that many DORA requirements are addressed at a design level. However, the review also identified that a number of requirements are not yet fully met and that further improvements are required to achieve full and sustainable compliance.

Four recurring areas for improvement were identified. These relate to the insufficient granularity of DORA gap assessments, possible improvements of the design and coverage of core ICT risk management framework controls, insufficient distinction between policies and procedures, and the adoption of DORA compliant policies and procedures defined at corporate (group-level) in intragroup ICT arrangements.

The AFM expects trading venues to carefully consider and implement the observations and recommendations set out in this report as part of their ongoing DORA implementation. The AFM will continue to closely monitor compliance with DORA requirements and will keep digital operational resilience firmly on its supervisory agenda. Where necessary, the AFM may take supervisory or enforcement action to ensure compliance with applicable regulatory requirements.

Table of Contents

1. Introduction

The AFM's supervisory strategy for the period 2023–2026 places strong emphasis on safeguarding the integrity and resilience of capital markets in an increasingly digital environment. Financial markets are becoming ever more dependent on ICT systems, and digital disruptions, cyber incidents and ICT failures can disrupt trading, undermine market confidence and affect the orderly functioning of markets. Given the interlinkages and dependencies within the financial market ecosystem, issues related to the digital operations of a financial entity may have spillover effects and impact other entities within that ecosystem. Strengthening digital operational resilience is therefore a key supervisory priority.

To address these risks in a harmonized manner across the European Union, the Digital Operational Resilience Act (DORA) was introduced. DORA has been fully applicable since January 2025 and establishes uniform requirements for financial entities, including trading venues, in areas such as ICT risk management, incident reporting, testing and third-party risk management.

ICT risk management forms a core pillar of DORA. Financial entities are required to maintain a sound, comprehensive and well-documented ICT risk management framework to ensure that ICT-related risks can be identified and addressed in a timely and effective manner.

Against this background, the AFM initiated a thematic review to assess the extent to which trading venues have designed their ICT risk management frameworks in line with the DORA requirements. The objective of the review was to identify common strengths and areas for improvement and to share observations and recommendations that support effective and consistent implementation.

As DORA has only recently become fully applicable, this thematic review marks the starting point of the AFM's DORA-related thematic supervision and aims to promote a high level of digital operational resilience across the sector. The insights gained are therefore also shared with the broader financial sector through the publication of this report.

2. Scope

The thematic review focused on trading venues' compliance with the ICT risk management framework as defined by DORA. The detailed requirements applicable to this framework are specified in Commission Delegated Regulation (EU) 2024/1774 supplementing DORA (hereafter: CDR ICT RMF).

The ICT risk management framework under DORA consists of a set of detailed requirements set out across multiple provisions of DORA and further specified in delegated regulations, in particular the CDR ICT RMF. These requirements can be grouped into ten subject areas and cover, among other things, access control, business continuity, ICT operations security, and ICT-related incident detection and response (including security monitoring). Together, these elements form the overall structure of the ICT risk management framework.

The AFM opted to review a broad set of requirements to obtain a broad view of trading venues' compliance with those requirements. A total of four trading venues was included in the scope of the review. To manage the supervisory burden for trading venues within scope, the assessment of compliance was limited to the design of required controls, such as policies and procedures.

In June 2025, the trading venues in scope were requested to demonstrate compliance with Article 1 to 26 of the CDR ICT RMF by providing all relevant documentation. After an initial assessment of the documentation received, the AFM formulated preliminary findings. Subsequently, two iterative rounds followed during which trading venues were given the opportunity to clarify their approach and provide additional substantiating documentation.

3. Observations and recommendations

The AFM observed that the assessed trading venues generally have in place a vast number of policies and procedures, covering the majority of the assessed DORA requirements at the design level. However, the review also identified that several DORA requirements were not yet fully met and that further improvements are required. In this context, the AFM identified the following recurring themes and areas for improvements

Recommendation 1: Ensure a sufficiently detailed DORA gap assessment

What we observe
The AFM observed that the initial DORA gap assessments conducted by trading venues were often insufficiently granular. In several cases, a significant part of the required documentation was only provided after the AFM had shared its preliminary findings. This indicates that not all applicable DORA requirements had been fully identified or mapped at the outset.

What we recommend
Trading venues should conduct a comprehensive and sufficiently detailed self-assessment of their ICT risk management framework. This assessment should clearly identify all applicable DORA requirements and map them to existing policies, procedures and controls, enabling timely remediation where gaps are identified.

How to address this
A granular DORA gap assessment should be embedded as a recurring element of the ICT risk management framework. This is particularly important given that Article 6(5) of DORA requires financial entities to review their ICT risk management framework at least annually, as further specified in Article 27 of the CDR ICT RMF. Performing a structured and detailed gap assessment supports both initial and ongoing compliance and contributes to the effective identification, management and mitigation of ICT-related risks.

Recommendation 2: Improve the design and coverage of core ICT risk management framework controls

What we observe
The AFM identified several key ICT risk management control areas that require further attention. These included:

- the required administration/record keeping of required elements in the ICT asset inventory or in relation to legacy systems;
- the completeness of procedures including keeping up to date with the latest technologies;
- the logging control and the frequency and scope of other security controls;
- the scope and frequency of security controls including firewalls;
- the defined emergency change procedure, and
- the scope of business continuity planning and testing including the prescribed scenarios in article 26 (2) of the CDR ICT RMF.

What we recommend
Trading venues should ensure that their ICT risk management framework adequately addresses all relevant control areas, in particular the following:

- ICT business continuity management;
- security monitoring;

- access controls;
- emergency change procedures;
- the scope and frequency of security controls (including ongoing maintenance), and
- logging-related controls.

How to address this
Given these commonalities, trading venues are encouraged to pay particular attention to compliance with relevant requirements in these areas. As the AFM considers security monitoring and access control to be key areas in ensuring cyber resilience, trading venues are encouraged to place additional focus on these areas when demonstrating compliance with the related DORA requirements.

Recommendation 3: Ensure that policies are correctly scoped and formally approved in line with Article 2(2) CDR ICT RMF

What we observe
The AFM observed that trading venues do not always clearly distinguish between documents that qualify as policies and those that constitute procedures or other supporting documentation. As a result, it is not always evident whether requirements that must explicitly be laid down in policies are adequately captured as such.

What we recommend
Trading venues should ensure that requirements under the CDR ICT RMF are correctly translated into policies or procedures, as applicable, and that supporting documentation (such as standards, process descriptions or wiki like pages) is clearly mapped to the relevant policies and procedures. Policies should comply with the requirements of Article 2(2) of the CDR ICT RMF, including formal approval by the management body.

How to address this
Trading venues should make a clear distinction between policies and procedures. This is important because the requirements set out in Article 2(2) of the CDR ICT RMF apply exclusively to policies. A clear distinction between policies and procedures is therefore essential to ensure proper governance, management body oversight and demonstrable compliance with DORA.

Recommendation 4: Apply group level DORA compliant policies for intragroup ICT services

What we observe
The AFM observed that trading venues making use of intragroup ICT service providers do not always consistently embed DORA related requirements in the governance and documentation of these arrangements.

What we recommend
Trading venues using intragroup ICT service providers should consider adopting DORA compliant policies and procedures defined at corporate (group) level and formally incorporating these into the intragroup outsourcing agreement. This approach provides a clear and consistent framework for the design of required ICT controls and their documentation.

How to address this
By applying group level DORA compliant policies trading venues ensure that DORA related improvements benefit the entire group rather than a single entity, while also reducing the risk of inconsistencies or conflicting standards within the group. Such practice supports a coherent and efficient implementation of DORA requirements across intragroup ICT arrangements.

4. Conclusion and next steps

Digital operational resilience is essential for the sound and orderly functioning of financial markets. Given the interlinkages and dependencies within the financial market ecosystem, issues related to the digital operations of a financial entity may have spillover effects and impact other entities within that ecosystem. Such events may therefore also affect financial market stability. Compliance with DORA therefore remains a key supervisory priority for the AFM.

The AFM conducted a thematic review to assess trading venues' compliance with the ICT risk management framework requirements under DORA. This assessment mapped the design of relevant policies and procedures against the requirements of the CDR ICT RMF. This thematic review marks the starting point of the AFM's DORA-related supervisory activities.

The observations and recommendations in this report underline that effective compliance with DORA requires a thorough and ongoing assessment of ICT risk management frameworks, well-designed and adequately scoped controls, clear governance arrangements and a clear distinction between policies and supporting documentation. In addition, consistency in the application of DORA requirements, including in intragroup ICT arrangements, is essential to avoid fragmentation and ensure coherent risk management.

Given the increasing digitalisation and complexity of financial markets, robust ICT risk management is indispensable for the sound and orderly functioning of financial markets and for maintaining confidence in those markets.

Going forward, the AFM encourages trading venues to carefully consider and implement the observations and recommendations set out in this report as part of their ongoing DORA implementation efforts. The AFM will continue to closely monitor compliance with DORA requirements and will keep digital operational resilience firmly on its supervisory agenda. The AFM notes that future assessments are likely to focus not only on the design of required controls, but increasingly on the implementation and operational effectiveness of those controls. Where necessary, the AFM may take supervisory or enforcement action to ensure compliance with applicable regulatory requirements.