Report

DORA Pilot Proprietary Traders

Exploratory research

20 december 2024

AFM

Inhoudsopgave

1 Introduction

On 14 December 2022, the European Parliament adopted new regulations related to cybersecurity: the Digital Operational Resilience Act (**DORA)**. DORA provides a regulatory framework for financial institutions within the EU for the resilience of ICT security and will enter into force on 17 January 2025.

The AFM has conducted an investigation in the form of a pilot study among a limited number of Proprietary Traders (**HERs**). The aim of the pilot study was to determine, with a limited scope, to what extent the institutions meet the requirements of DORA, or are well on their way to being compliant by 17 January 2025. The scope of the study focused on three areas within the *'DORA Regulatory Technical Standards (**RTS**) establishing tools, methods, processes and policies for ICT risk management*'. The areas concerned are:

1 ICT Asset Management
   - Article 4 – ICT asset management policy
   - Article 5 – ICT asset management procedure

2 ICT Project Management and ICT Change Management
   - Article 17 – ICT change management

3 Access control
   - Article 20 – Identity management
   - Article 21 – Access control

These three areas and articles cover IT processes for which requirements are already set out in the Dutch Financial Supervision Act (**Wft**) and the Markets in Financial Instruments Directive (**MiFiD**). The above processes were the focus area for this pilot study. In addition, the AFM discussed the intra-group agreements that have been made within the institutions as they apply to the implementation of the IT processes in scope.

For this pilot study, the AFM requested underlying documentation for the relevant IT processes. In discussions with the HERs, the documentation and the underlying IT process were discussed for the purpose of clarification. This has given the AFM an initial insight into the current structure of the IT processes. This, in turn, has resulted in points of attention that may also be relevant to other market parties.

2 Results

2.1 General points of attention

Based on the documentation and discussions, the AFM has drawn up a number of general points of attention. These are broadly applicable to the IT processes in scope, or arise from related topics that have been discussed, such as internal outsourcing. As a result, some points of attention do not fall directly within the original scope of the study, but are important in the broader context of DORA.

1 **Documentation**. The parties were (partly) unable to provide their documented IT policy and procedures, which are both necessary and useful for determining their compliance with the requirements of DORA. For parties that have recently drawn up policy, the AFM has identified the risk of an incoherent DORA compliance approach.

2 **IT policy completeness**. The IT policy and procedures of the parties were not (yet) fully in line with the requirements set out in the DORA RTS establishing tools, methods, processes and policies for ICT risk management. This RTS specifically prescribes which elements are mandatory in the policy or procedure. If an element is not directly applicable to a financial entity, it must be described as such in the policy. As an example, a financial entity may choose not to expose its ICT assets to external networks (see Article 4(2) of the RTS for ICT risk management). This choice must then be recorded as part of the policy on the management of ICT assets.

3 **Awareness of the Board**. DORA prescribes that the board of directors must be demonstrably aware of information security. The board is responsible for the level of information security for all (outsourced) partners across the entire end-to-end outsourcing chain. There must be a risk-based monitoring system for all these information security aspects.

4 **Internal outsourcing**. In DORA, internal outsourcing is (in principle) equated with external outsourcing. This implies that the Dutch registered entity must have outsourcing agreements with all group entities that provide IT services. In addition, the Dutch entity is obliged to have a fully-fledged Register of Information.

5 **Team procedures**. Having multiple detailed procedures related to processes such as change management and user access by different teams within an institution is a concern. These procedures should not deviate from internal policies to be in line with DORA's requirements. Having multiple procedures is not a risk in itself, but it does require more time and attention to ensure they remain compliant.

6 **Operation of policy and processes**. In addition to aligning policy and processes with DORA, institutions must also be able to demonstrate that they work in this way (operational effectiveness). By demonstrating this, in addition to the design, the institution could be compliant with DORA.

2.2 Focus areas for ICT asset management, ICT change management, identity management and access control

In addition to the general points of attention, the AFM also has a number of more specific points of attention concerning the areas which were the main focus of the pilot study: management of ICT assets, ICT change management, identity management and access control. The points of attention highlighted mainly stem from the specific requirements of the RTS to establish tools, methods, processes and policies for ICT risk management.

1 **Classifying information and systems**. Article 5 of the DORA RTS on ICT risk management states that the classification of information (data) and systems must be based on the criteria of availability, authenticity, integrity and confidentiality. The classification of information and systems is then in line with the classification of ICT-supported business functions as described in Article 8(1) of the DORA Regulation.

2 **Audit trail change management**. There must be a complete audit trail in place, demonstrating the separation of duties. It is important to document IT changes and the approvals of these changes. This is especially true if change approval is given in meetings or if multiple systems are used for change management, such as a pipeline and service management system.

3 **Connections and interdependencies of ICT assets**. Article 4(2) of the RTS for ICT risk management states that the financial entity shall set out in its ICT asset management policy how it will address the links and interdependencies between ICT assets and the business functions that use this ICT asset. This requires extra attention from entities that use multiple records and overviews for their ICT assets, to properly document and monitor this connection and interdependencies.

4 **ICT assets definition**. The policy for the management of ICT assets and recording in overviews is mainly focused on hardware. The definition of ICT assets, as given in Article 3(7) of the DORA Regulation, includes both hardware and software. Extra attention is needed to ensure that the software components are also sufficiently included in the policy and procedure for the management of ICT assets.

5 **ICT user-access**. Within a number of investigated institutions, the AFM was unable to establish that there is a documented working method with regard to user access. While password security is usually well organised, a system for user profiles and associated user IDs was lacking.

3 Conclusion and recommendations

Based on the documentation and interviews with a limited number of HERs, the conclusion may be drawn that the extent to which institutions are ready for DORA as of 17 January 2025 varies greatly. Several parties have recently started implementing the DORA requirements within their organisation and it seems unlikely that they will be DORA compliant by 17 January 2025. For other parties, the question is whether they are fully compliant with all the specific requirements of DORA.

Based on the points of attention highlighted, the AFM has the following recommendations:

- Perform a gap analysis to verify that all required elements from DORA are embedded in the policy documents and procedures. For this, help can be called in from an external advisor or second-line function (compliance, risk management). Once the policies and procedures in line with DORA have been implemented, an internal or external audit can be carried out to obtain assurance for design, existence and operation.

- Parties that rely on a group entity to run their IT processes must ensure that their intra-group outsourcing agreement fully covers the services received. Under DORA, internal outsourcing is (in principle) considered as external outsourcing, which means that the same requirements apply. A review of the intra-group outsourcing agreement is recommended to verify that it meets DORA's requirements.

- For an integrated approach to ICT risk management, it is important to consider all information security criteria (availability, integrity, confidentiality and authenticity) when classifying all ICT supporting business functions and the information and ICT assets. This classification should be reviewed as necessary and at least once a year. It is therefore recommended to plan this ahead as it takes a lot of time to classify all ICT-supported business functions and the information and ICT assets. Here, too, there must be a demonstrable and recorded process.

Apart from the investigation that was carried out, the AFM also draws attention to the register of information. After DORA enters into force on 17 January 2025, the register of information will be the first thing to be requested from the market parties. The AFM must submit these registers to the EBA by 30 April 2025 at the latest. To this end, the AFM intends to send a request for information to all companies with an AFM licence that fall under DORA in February 2025.