Getting ready for the arrival of DORA

July 2023

This is the first edition in a series of AFM publications on the Digital Operational Resilience Act (DORA). This edition is intended for all firms that will have to comply with this European regulation from 2025. The various parts of DORA are explained in this publication. It enables firms to see where they stand in terms of cyber security and any further steps they need to take to comply with the regulation.

Continue reading

AFM

Contents

01 What does DORA mean for the financial sector?

The Digital Operational Resilience Act (DORA) has been in force since January 2023. DORA is a European regulation that aims to ensure that financial organisations have better control of IT risks and are thus more resilient to cyber threats. This is because resilience is not keeping pace with growing IT threats. This is evidenced by a recent report by the National Coordinator for Counterterrorism and Security (NCTV) among others. The regulation also brings further harmonisation of IT requirements for the financial sector.

In this regard, DORA sets requirements in areas such as IT risk management, IT incidents, periodic testing of digital resilience and the control of risks in outsourcing to critical third parties. These take account of the size, risk profile and systemic importance of individual organisations. Microenterprises, for example, are exempt from various parts of the regulation, while for Chapter II of DORA ('ICT risk management') a simplified framework is being developed for certain types of license. This is explained further in the sections below.

There are also two additional effects that contribute to the resilience of financial institutions. First, DORA is intended to improve the security of the supply chain, as it also includes a framework that will apply to the most critical ICT service providers for the financial sector. Finally, the regulation also has provisions on information exchanges, enabling financial institutions to exchange information and intelligence on cyber threats and thereby further limit the risks.

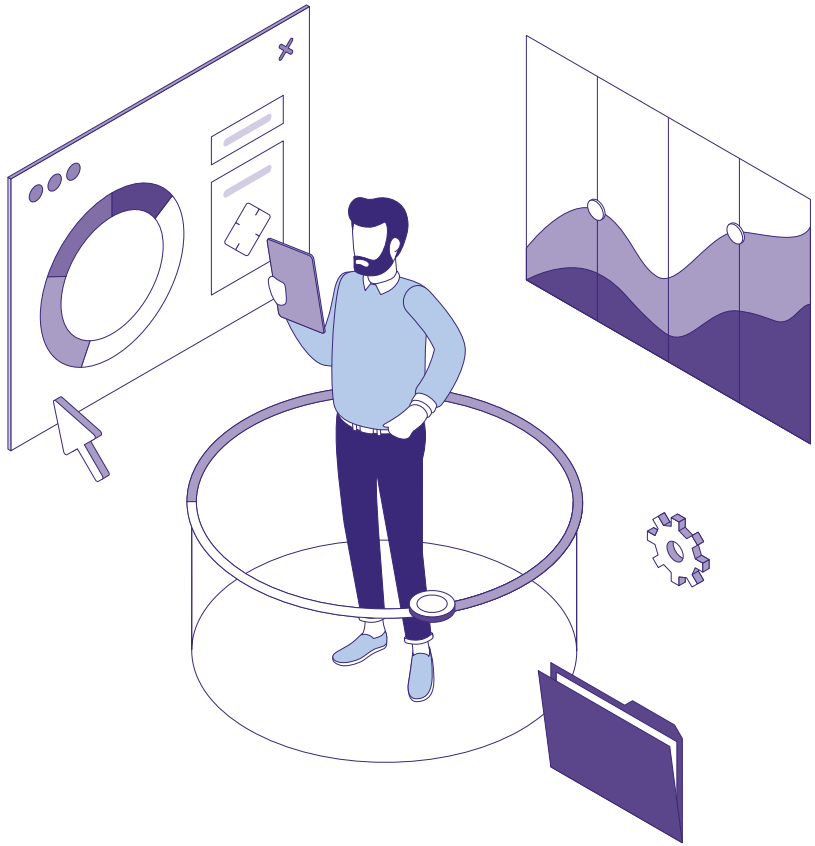
Firms have until January 2025 to comply with the regulation. After that, DORA will officially enter into force and the AFM will supervise the regulation. Some firms are already subject to DORA-related requirements under existing laws and regulations.

02 Getting down to work on increased digital resilience

Firms can already start analysing the gaps they need to fill to comply with DORA and can start setting up activities accordingly. Firms are advised to start work on this as soon as possible in order to be DORA-compliant by January 2025.

Some topics are currently being elaborated in greater detail by the ESAs (European Supervisory Authorities) in regulatory and implementing technical standards (RTS and ITS), although these themes are already described in broad terms in DORA. The other topics in the regulation will not be developed any further. Firms can therefore already start work with the existing texts.

The following sections provide guidance on preparations for DORA based on the four main topics of the regulation. In addition, the governance and organisation aspects run as a common thread through the various chapters of DORA and are therefore dealt with separately in the final section. For each topic, there are also details of the parts for which additional standards are currently being developed and when these will be submitted to the European Commission (EC).



ICT risk management

ICT risk management is an important means of detecting and managing ICT risks in a structured way. DORA describes both the process side of risk management and its implementation in technical measures. As a basis, DORA requires firms to have a governance and control framework enabling them to establish a control cycle and conduct continuous evaluations.

Another important part is the allocation of the necessary ICT roles, such as an independent function to manage ICT risks and an internal auditor to periodically assess the framework.

In addition to the governance and control framework, DORA prescribes a specific ICT risk management framework (ICT RMF). IT is closely associated with other business processes, so this framework must be in line with the enterprise risk management (ERM). For some license types, an RTS is being developed including simplified guidelines on the establishment of the ICT risk management framework.

Business Continuity Management (BCM) in IT is important to ensure the stability of a firm's services. DORA therefore states that BCM plans must be periodically tested and that the necessary crisis communication arrangements must be in place.

In addition to prevention, reactive measures also play an important role. For example, DORA requires firms to establish detection mechanisms, as well as processes and techniques to deal with detected deviations. An important part of this is the production of back-ups in case risks nevertheless materialise.

Employees play an important role in the implementation of IT policy. DORA therefore also focuses on the development of IT awareness programmes, which must take account of the differences in employees' work.

Firms can already start working on:

- The framework for ICT risk management, in line with the Enterprise Risk Management;
- The arrangements for monitoring, handling and follow-up of deviating activities, including the production of back-ups;
- The ICT business continuity plan that is periodically tested;
- IT awareness programmes, aligned with the employees' responsibilities.

Further elaboration	Description	Submission to the EC
RTS for Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	No later than 17 January 2024
RTS for Article 16(3)	Simplified ICT risk management framework	No later than 17 January 2024

ICT-related incident management

It is important that IT incidents are dealt with adequately. For effective incident management, DORA expects firms to establish a process to detect and deal with ICT incidents and cyber threats.

In addition, firms must keep a record of past incidents. This promotes careful handling and follow-up of incidents and provides an opportunity for evaluations and root cause analyses.

DORA requires major IT incidents to be reported to the supervisor. This is already mandatory. Criteria and templates for the reporting obligation under DORA are currently being developed. See the table below for the associated timelines.

Firms can already start working on:

- The process for detecting and dealing with incidents;
- Maintaining a record of past IT incidents.

Further elaboration	Description	Submission to the EC
RTS for Article 18(3)	Classification of ICT-related incidents and cyber threats	No later than 17 January 2024
RTS for Article 20(a)	Reporting content and templates	No later than 17 July 2024
ITS for Article 20(b)	ITS to establish the reporting details for major ICT-related incidents	No later than 17 July 2024

Digital operational resilience testing

Regular testing gives a firm insight into the actual security of the IT environment and enables targeted improvements to be made. DORA therefore requires firms to develop a risk-oriented programme to test and increase digital resilience. The content of this programme depends on the identified risk profile of a firm. Various types of tests are conceivable, including vulnerability scans, penetration tests and red teaming.

Firms can already start working on:

- A risk-based programme to test digital operational resilience.

Among other things, DORA applies proportionality for microenterprises, exempting them from the relevant articles on this subject.

Further elaboration	Description	Submission to the EC
RTS for Article 26(11)	Advanced testing of ICT tools, systems and processes based on TLPT	No later than 17 July 2024

Managing of ICT third-party risk

DORA devotes a lot of attention to third-party risk in order to limit supply chain risks as far as possible. Firms are required to include third-party risk explicitly in the ICT risk management framework and to develop a strategy for outsourcing, including of IT.

The regulation also specifies the elements that are important to consider when outsourcing. For example, a firm must always have mutual agreements in place with the service provider covering service levels (e.g. in service level agreements). In the case of critical outsourcing, an exit strategy must always be available. There are also a number of fixed elements that the firm must include in an agreement. An example is the power to require an inspection or audit by the institution, a designated third party or the competent supervisory authority.

A firm must also maintain a register of existing outsourcing arrangements, including relevant characteristics.

Firms can already start working on:

- A strategy and risk management structure for ICT outsourcing;
- A register of existing outsourcing arrangements, including relevant characteristics.

Further elaboration	Description	Submission to the EC
RTS for Article 28(1)	General principles for a sound management of ICT third-party risk	No later than 17 January 2024
RTS for Article 28(9)	Register of information on outsourcing arrangements	No later than 17 January 2024
RTS for Article 30(5)	Key contractual provisions	No later than 17 July 2024
Input for advice on criticality criteria for Article 31(6)	N/A	No later than 17 July 2024
Selection of critical IT service providers for Article 31	N/A	No timeline notified

Common threads of governance and organisation

The subjects of governance and organisation play an important role in DORA and arise throughout the regulation. For many processes prescribed by the regulation, for example, there is a requirement that firms set clear roles and responsibilities.

DORA also places great emphasis on the establishment of the three-lines model. Firms are expected to appoint both a control and audit function, and to position these sufficiently independently within the organisation. There is also a requirement that some of the described processes are continuously evaluated and that this is embedded in processes.

The regulation also requires members of the management board to keep their knowledge up to date by means of training and education.

Firms can already start working on:

- Allocating the required, sufficiently independent IT roles in line with the three-lines model;
- Continuous evaluation of the IT organisation and control effectiveness

03 **Outlook**

The various RTS and ITS will now be further developed as set out in the previous sections. The ESAs will also present these to firms in the financial sector by means of a public consultation, with the possibility of responding to the documents.

In the meantime, the AFM is preparing to conduct DORA supervision. Subsequent publications in this series will consider individual aspects of the regulation in greater depth. The next edition will be published in the third quarter of 2023.

Further information on the scope of DORA can be found, among others, in the following parts of the regulation:

- The scope of application is described in Article 2;
- Definitions (such as 'microenterprise') are provided in Article 3.

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

Any questions or comments about this publication?

Send an email to: redactie@afm.nl

The Dutch Authority for the Financial Markets
PO Box 11723 | 1001 GS Amsterdam

Telephone
+31 20 797 2000

www.afm.nl

Follow us:

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.