Getting ready for DORA: ICT risk management

In short This is the third 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 ICT risk management. By paying careful attention to ICT risk management, firms can gain a comprehensive understanding of their ICT risks and how to minimise the related effects. In this way firms can analyse their current status in this regard and what actions they may need to take to ensure compliance with the Regulation.

1. ICT Risk Management in DORA

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, including with regard to ICT Risk Management. Firms are already able to analyse their compliance with the DORA requirements in this respect and take action, if needed. They are advised to start working on this as soon as possible in order to be DORA-compliant by 17 January 2025.

ICT risk management is a key element within DORA. Effective ICT risk management helps firms detect and manage ICT risks in a structured way. The requirements are set out in Chapter II (Articles 5 to 16) of the Regulation. These articles deal in detail with, among other things, the ICT risk management framework, Business Continuity Management (BCM) and employee learning and evolving in relation to ICT security and digital operational resilience.

Alongside the requirements set out in the Regulation, various topics are further elaborated in a Regulatory Technical Standard (RTS)[1]. This RTS includes an elaboration of the ICT risk management tools, methods, processes, and policies (Article 15) and the simplified ICT risk management framework (Article 16(3)). Article 15 applies in this regard to all firms, as described in Article 2(1), while Article 16 describes a simplified ICT risk management framework for a number of specific types of firms[2].

The articles cited from DORA are explained in the following sections. We will also address some of the topics which are further elaborated in the RTS. It is important to note here that the RTS texts were submitted to the European Commission (EC) in January 2024. It is possible that certain changes might yet be made to the wording of the RTS, although it is common for a text to remain broadly the same.

1 RTS on ICT risk management framework and on simplified ICT risk management framework;

2 The firms concerned are small and non-interconnected investment firms, payment firms exempted pursuant to Directive (EU) 2015/2366; firms exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money firms exempted pursuant to Directive 2009/110/EC; and small firms for occupational retirement provision.

Table 1

Further elaborations	Subject	Completed
RTS for Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	Already submitted to EC
RTS for Article 16(3)	Simplified ICT risk management framework	Already submitted to EC

2. Getting started on ICT risk management

Risk Management in DORA (Articles 6 to 14)

Firms can already start working on:
- Developing an ICT risk management framework (including in relation to outsourcing);
- Checking compliance with the requirements as regards Business Continuity Management (BCM).

Article 6 of the Regulation sets out the requirements for the ICT risk management framework. It is important that firms have a sound, well-documented ICT risk management framework in place to enable them to address ICT risks quickly, efficiently, and comprehensively. This framework must include, among other things, the strategies, policies, procedures, and ICT tools that are necessary to protect all ICT assets[3] and relevant physical components.

The ICT risk management framework must be reviewed at least once a year (or periodically in the case of microenterprises) and any adjustments to the framework must be documented. The framework must be continuously improved on the basis of lessons derived from implementation and monitoring. Finally, the ICT risk management framework must be subject to independent audits on a regular basis. The conclusions from the audits must be acted upon.

DORA sets out requirements with regard to Business Continuity Management (BCM) aimed at ensuring the stability of a company's services. These requirements are set out in Articles 8 to 12 of the Regulation.
- Firms must clearly map their ICT landscape. For this, it is important that all ICT-supported business functions, roles, and responsibilities are identified, classified and documented. The same also applies to the ICT assets and applications supporting these business functions.
- Firms must continuously monitor and review the security and functioning of ICT systems[4]. This will have a positive impact on the protection of ICT systems and reduce the risk of cyber incidents.
- Firms can further reduce their ICT risks on ICT systems by implementing ICT security tools, policies and procedures that aim to ensure the resilience, continuity, and availability of ICT systems. Since not all incidents can be prevented, it is important that financial firms have in place detection mechanisms to promptly detect anomalous activities and to identify single points of failure. Firms must respond appropriately upon the detection of an anomaly.
- Development and implementation of an ICT business continuity policy. This policy must include arrangements, plans, procedures, and mechanisms aiming, among other things, to ensure that the continuity of critical functions is safeguarded, that ICT-related incidents are appropriately resolved in a way that limits damage and that all relevant internal and external stakeholders are informed of the incident that has occurred.

Certain topics related to BCM, such as testing of the BCP and the response and recovery plan, are elaborated further in the RTS. We will return to this in the next section.

The final two articles of the Regulation concerning ICT risk management (Articles 13 and 14) concern learning and evolving and communication. As regards learning and evolving, it is important that firms have in place adequate capabilities and staff to gather information on vulnerabilities, cyber threats, and ICT-related incidents. Financial entities must take account of technological developments, the results of digital operational resilience testing and ICT incidents that have occurred.

In the event of an ICT-related incident, it is important to analyse the cause or causes of the disruption and to identify any required

3 All the software or hardware in the network and information systems that are used by the financial entity.

4 All ICT assets that work together to perform a particular business function.

improvements to prevent any recurrence of the disruption. It is also important for firms to have in place crisis communication plans enabling an adequate response in case of major ICT-related incidents. This includes, among other things, the responsible disclosure of vulnerabilities to staff, clients, and other direct stakeholders.

Further elaboration of ICT risk management in the RTS (Article 15)

Firms can already start working on:
Developing/implementing policies and procedures with regard to ICT asset management, network security and encryption and cryptography, among other things.

In this section, we will explain some of the topics in the RTS. These topics are a further elaboration of Article 15 of the Regulation. In the interest of providing a clear overview, a selection of topics from the RTS was chosen. The fact that not all the topics from the RTS are discussed in this publication does not mean that the other topics are less important. Firms must comply with all the requirements detailed in the RTS by 17 January 2025.

Business Continuity Management

Certain topics related to BCM are elaborated further in Chapter IV (Articles 24 to 26) of the RTS. They include the testing of the Business Continuity Plan (BCP) to ensure the continuity of critical and important business functions. Firms must perform the testing of the BCP on the basis of realistic test scenarios that attempt to simulate potential disruption. The testing must also include the testing of ICT services provided by third parties, if possible. Test results must be documented and any identified deficiencies resulting from the tests must be analysed, addressed, and reported to the management body.

In addition to testing the BCP, firms must develop a response and recovery plan to minimise the impact of disruptions. In this regard, firms must take into account the results of the Business Impact analysis (see also Article 11(5) of the Regulation). The ICT response and recovery plan must, among other things, specify the conditions prompting its activation (and any exceptions), describe what actions must be taken to ensure the availability, integrity, and confidentiality of critical and important systems, and lay down the conditions to declare successful execution of the response and recovery plan.

ICT Asset Management

As part of ICT asset management, firms must develop (and implement) a policy and procedures, with a view to preserving the availability, integrity, and confidentiality of data. The policy must describe how the organisation monitors and manages the lifecycle of its ICT assets. In addition, firms must keep records of all ICT assets, including their location, classification, the identity of the system owner and the business function or functions supported by the ICT assets. Finally, a procedure must be developed detailing how the company determines whether an ICT asset or application is critical or important.

Encryption and cryptography

As with ICT asset management, firms must develop and implement a policy documenting their data encryption and cryptographic key management. Firms must include in this policy a description of the criteria to select cryptographic techniques and use practices, among other things. It must also be laid down under what circumstances and conditions a company will switch to a new cryptographic technique to increase resilience against cyber attacks. It is important that firms lay out the requirements for managing cryptographic keys through their entire lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmission, retiring, revoking, and destroying keys.

Network security
In order to ensure the security of networks within the organisation, it is important that firms develop and implement policies and procedures laying out measures to safeguard against intrusions and data misuse. The mapping and visual representation of the various network connections and data flows within the organisation provide firms with a clear overview of the network. Furthermore, it is important that network connections passing over corporate networks, public networks, domestic networks, third-party networks, and wireless networks are secured and encrypted to prevent unauthorised access to the data. Finally, firms can ensure the security of their network by reviewing on a regular basis the firewall rules and by performing regular reviews of the network architecture and of the network security design.

Vulnerability and patch management
To further secure the networks of firms, firms must develop and document vulnerability as well as patch management procedures. The vulnerability management procedure must describe, among other things, how the institution ensures the performance of (automated) vulnerability scanning on a regular basis and how any identified vulnerabilities are addressed and monitored. At the same time, the patch management procedure must ensure that software and hardware patches are identified using automated tools and are tested in an environment separate from the production environment (to the extent possible) and that a deadline is set for the installation of patches and updates.

Logging
In addition to vulnerability and patch management and network security, firms must ensure they are protected against intrusions and data misuse by logging user events. The firms must identify for themselves which events are to be logged, the retention period of the logs and the measures to secure and handle the log data. To safeguard the accuracy of the logs, it is also important that measures are taken to protect the logs against unauthorised access, manipulation/deletion and disruptions affecting the logging system.

Change management
As part of the safeguards to preserve the availability, integrity and confidentiality of data, firms must develop and implement an ICT change management procedure. This procedure must set out how the organisation verifies that ICT security requirements have been met, that changes are requested, tested, approved, and implemented by the appropriate staff members, and how emergency changes must be implemented. It is also important for firms to consider procedures to evaluate and monitor changes after their implementation and what steps should be taken when a change is aborted or cannot be implemented.

Logical access control
As part of their logical access control, firms must also develop and implement policies and procedures which must set out the identification and authentication of natural persons and systems accessing the institution's information. For this, it is important that all (external) staff members are assigned a unique identity corresponding to their user account. Firms must maintain records of these identities/user accounts, which must also be reviewed and verified on a regular basis. Identity verification includes the creation, change, temporary deactivation, and termination of user accounts. In addition to user identification, it is important that staff members' access to data is properly managed by the organisation. In this context, firms must implement measures aimed at limiting as much as possible staff members' access to data (least privilege principles), avoiding conflicts related to segregation of duties, and ensuring that staff members can be identified for the actions performed in ICT systems (in particular where shared user accounts are used). Finally, it is important that changes to access rights are implemented promptly and correctly.

Table 2

Further elaborations	Description	Completed
RTS for Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	Already submitted to EC

Simplified ICT risk management framework (Article 16)

Article 16 of the Regulation sets out the requirements for the simplified ICT risk management framework applicable to various exempted firms[5]. Part of the requirements for the framework are set out in the Regulation, while another part is elaborated in the RTS.

An analysis of the ICT risk management framework indicates that the simplified framework is broadly similar to the "regular" ICT risk management framework. As is the case with the regular ICT risk management framework, the simplified variant must be documented and reviewed periodically (as well as upon the occurrence of major ICT-related incidents). The frequency of the periodic review is dependent on the institution's risk profile.

The biggest difference is in the number of requirements that the simplified framework must meet. Also, these requirements are often less detailed. The reasoning behind this is that the simplified framework includes the elements that are the minimum necessary to preserve the availability, integrity, and confidentiality of data, while taking into account the risk, size and complexity of the company. Firms to which the simplified framework applies are therefore only required to develop an information security policy setting out general, overarching guidelines and rules aimed at preserving the availability, integrity, and confidentiality of data. In addition to this information security policy, firms are also required to implement adequate security measures for, among other things, logical access control, network security, ICT systems management and change management.

To minimise the risk of unauthorised access, firms must, for example, develop and implement procedures aimed at limiting as much as possible staff members' rights and ensuring that individual users can be identified for the actions performed in ICT systems. Firms must furthermore establish a standard process for granting, changing, and revoking rights, and those rights must be reviewed periodically.

Firms must also develop a procedure for change management. However, the requirements for this are more concise than those for firms to which Article 15 applies. The simplified change management procedure must ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented, and verified.

With regard to network security, firms must configure the network in such a way that systems connected to the internal and/or external network are adequately protected against unauthorised access, intrusions and data misuse. For this, it is important that measures are taken to protect data (in use, in transit and at rest) and to ensure the authenticity, integrity and confidentiality of data during network transmission. In addition, consideration must be given to how unauthorised connections to the network are prevented and detected in a timely manner, and a process must be in place for securely deleting data.

Finally, as part of ICT asset management, firms must identify all ICT systems supporting a critical or important business function. Firms must additionally develop and implement an ICT systems acquisition, development, and maintenance procedure. This procedure must clearly define the information security requirements and how ICT systems are tested prior to their first use. In this context, it is also important to monitor the life cycle of the ICT system, to ensure that it continues to meet and support the organisation's requirements.

5 This applies to small and non-interconnected investment firms, payment firms exempted pursuant to Directive (EU) 2015/2366; firms exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money firms exempted pursuant to Directive 2009/110/EC; and small firms for occupational retirement provision.

The requirements set out in the RTS for the simplified ICT risk management framework are therefore broadly in line with the requirements for the regular ICT risk management framework. However, the specified requirements are less extensive in the case of the simplified ICT risk management framework. In this way, account is taken of the size of the firms to which Article 16 applies.

Table 3

Further elaborations	Description	Completed
RTS for Article 16(3)	Simplified ICT risk management framework	Already submitted to EC

3. Outlook

At this time, the first as well as the second batch of RTSs and ITSs have both been published. The first batch (including that for Articles 15 and 16(3)) has already been submitted to the European Commission for assessment and decision-making. The second batch was submitted by the ESAs to firms in the financial sector for public consultation. This batch will probably be submitted to the European Commission in the third quarter of 2024.

In the meantime, the AFM will continue its preparations for conducting DORA supervision. Subsequent publications in this series will consider other aspects of the Regulation. The next edition will be published in the second quarter of 2024.

For further elaboration on ICT Risk Management in DORA, the following pages can be consulted:
News release concerning the first set of rules for ICT risk management (RTS), among other matters (esma.europa.eu)

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