Getting ready for DORA: Management of ICT risk for third-party providers

December 2023

This is the second 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 January 17 2025 onwards. This edition focuses on the management of ICT risk for third-party providers. It enables firms to analyse where they stand in this and any further steps they need to take to comply with the regulation.

Continue reading

AFM

Contents

01 The role of third-party providers in DORA

DORA aims to ensure that financial institutions 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 the risks stemming from the use of third parties, i.e. third-party risk. 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 January 2025.

DORA devotes a lot of attention to the so-called third-party risk in order to limit supply chain risks as much as possible. The requirements are set out in Chapter V (Articles 28 through 44). These articles cover the required policy documents, risk analyses and contractual provisions, among other things. These articles also define the oversight framework for critical third-party providers of ICT services.

Some subjects are currently being worked out in greater detail by the European Supervisory Authorities (ESAs) in Regulatory and Implementing Technical Standards (RTS and ITS). At the time of this edition's publication, the ESAs have already shared some of these products to the market for the purpose of consultation.
The accompanying timelines are included in Table 1.

The following sections address the aforementioned articles and discuss the actions that organisations can already start working on in order to be DORA-compliant in time. We also cover the ways in which proportionality recurs within this subject.

Table 1

Further elaborations	Subject	Completed
RTS for Article 28(1)	Policy on ICT services performed by 3rd parties	No later than January 2024
ITS for Article 28(9)	Templates for the register of information	No later than January 2024
RTS for Article 30(5)	Elements when sub-contracting critical or important functions	No later than July 2024
Call for advice for Article 31(8)	Criticality criteria	September 2023
Selection of critical ICT service providers for Article 31	n/a	No timeline notified
Guidelines for Article 32(7)	Cooperation between ESAs and CAs regarding the structure of oversights	No later than July 2024
RTS for Article 41	Information on oversight conduct	No later than July 2024
Call for advice for Article 43(2)	Oversight fees	September 2023

02 Getting started on third-party risk

General principles for managing ICT risk for third-party providers

Firms can already start working on:

- The ICT risk management framework, including in terms of subcontracts.
- The strategy for managing ICT risk for third-party providers.
- The register of information of all contractual arrangements with third-party providers of ICT services.
- The exit strategy, if third-party providers support critical or important functions.

Articles 28 and 29 of DORA outline the different general principles for third-party risk management. To be resilient against cyber threats and ICT disruptions throughout the chain, it is important to be mindful of the risks of using ICT services from third-party providers. Articles 28 and 29 focus on the measures firms should take before concluding an agreement with a third-party provider. This involves the same requirements for external agreements as for intragroup agreements.

First of all, firms should explicitly assess and address the ICT risks arising from using services from third-party providers. This risk assessment is not an isolated exercise, but should be part of the organisation-wide ICT risk management framework. Additionally, DORA requires firms to develop a strategy for third-party risk management, in which the risks of outsourcing critical services are regularly reviewed. Micro-undertakings are exempt[1] from the obligation to develop this strategy.

1 The same applies to firms listed in the first paragraph of Article 16(1): small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions 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 institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision.

All contractual arrangements for the provision of ICT services must be recorded in a register of information. Firms should also include in this register of information whether the services purchased support critical or important functions. Supervisory authorities may request a copy of this register of information. The register of information is important for an institution's internal control, but will also be used by the ESAs to designate Critical Third Party Service Providers (CTPPs) of the European Union. See also Section 4 of this DORA update.

Furthermore, DORA requires firms to report annually to the supervisory authority which third-party ICT agreements were entered into that year. When a firm enters into an agreement relating to critical or important functions, they have to actively report this to the supervisory authority. Also, when a function becomes critical or important, this must be reported by the firm to the supervisory authority.

Prior to concluding agreements with third-party providers, various aspects should be analysed, such as the required ICT security level and the required frequency and scope of audits and inspections. It is also important to consider any concentration risks. Further subcontracting by the service provider may also have an impact on this. Additionally, firms also need to have an exit strategy in place if third-party providers support critical or important functions. Such an exit strategy has to consider any risks that may occur on the part of the service provider, such as a disruption in provision, deterioration in quality or (premature) termination of the agreement.

The ESAs are currently developing a standard model for the register of contractual arrangements. They are also further elaborating the key principles for third-party risk management in an RTS. The timelines for this are summarised in Table 2. At the time of this edition's publication, the ESAs already published these documents as part of the first DORA consultation package.

Table 2

Further elaborations	Description	Completed
RTS for Article 28(1)	Policy on ICT services performed by 3rd parties	No later than January 2024
ITS for Article 28(9)	Templates for the register of information	No later than January 2024

Important contractual provisions to be put in writing

Firms can already start working on:

- Analysing whether the existing contractual arrangements are in line with DORA's requirements.

Article 30 of DORA includes different provisions that firms need to include in contractual arrangements with third-party providers. It distinguishes between elements that must be included in all agreements, and additional obligations for agreements that support critical or important functions.

Examples of elements that must at all times be included in agreements are:

- Both parties' rights and obligations.
- A full description of the services provided.
- The regions and/or countries where the services are to be provided and where data are to be processed.
- The service level to be provided.
- The level of data protection, in terms of availability, authenticity, integrity and confidentiality.
- Support in case of incidents.
- The termination rights and related minimum notice periods.

In addition to the elements above, contractual arrangements on the use of third party services supporting critical or important functions will need to include at least the following:

- The service provider's reporting obligations.
- The requirement for the service provider to implement and test business contingency plans.
- The obligation of the service provider to cooperate in the financial institution's Threat-Led Penetration Tests (TLPTs)[2].
- The right of inspection and audit by the financial entity or an appointed third party.
- It also sets additional and more in-depth requirements for the provisions that apply to all means of subcontracting, such as detailing the services provided through accurate key performance indicators.

Micro enterprises may agree with the service provider that audits and inspections are performed by an independent party appointed by the service provider, rather than micro-undertakings performing them themselves. However, in doing so, micro-undertakings should always be able to request the necessary information from this party.

In addition to these requirements, the ESAs are currently preparing the conditions for subcontracting services supporting critical or important functions. The timelines for this are summarised in Table 3.

Table 3

Further elaborations	Description	Completed
RTS for Article 30(5)	Elements when sub-contracting critical or important functions	No later than July 2024

2 See also Article 26 of DORA: some firms are required to complete advanced testing via Threat-Led Penetration Testing.

Critical third-party providers of ICT services are now also under supervision

A large part of the ICT services of the financial sector is being outsourced to a limited number of ICT providers. That entails concentration risks, which is why DORA enables the supervision of these service providers. These critical ICT service providers are crucial for the stability of the European financial sector. At present, these articles do not yet directly impact financial undertakings. Ultimately, this oversight will be able to bring firms greater certainty about the digital resilience of outsourcing partners. Articles 31 through 44 describe this new mandate in the so-called oversight framework.

The ESAs are currently setting up a selection of service providers that will be covered by this framework. Among other things, they will base the instruction on the service provider's impact on the system, and the level of dependability and substitutability of this service. A lead overseer will be appointed for each service provider that will be responsible for the supervision. Depending on the sector most serviced, this will be ESMA, EIOPA or EBA. Ultimate supervision will be performed by a team of European and national supervisory authorities. See Table 4 for an overview of elements that are to be further elaborated.

Table 4

Further elaborations	Description	Completed
Call for advice for Article 31(8)	Criticality criteria	September 2023
Selection of critical ICT service providers for Article 31	n/a	No timeline notified
Guidelines for Article 32(7)	Cooperation between ESAs and CAs regarding the structure of oversights	No later than July 2024
RTS for Article 41	Information on oversight conduct	No later than July 2024
Call for advice for Article 43(2)	Oversight fees	September 2023

03 **Outlook**

The various RTS and ITS will now be further developed according to the timelines 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 first quarter of 2024.

For further elaboration on third-party risk in DORA, the following pages can be consulted:

- ESAs Report on the landscape of ICT third-party providers in the EU (eba.europa.eu)
- ESAs consult on the first batch of DORA policy products (RTS and ITS) (esma.europa.eu)
- If you have any further questions, please contact the AFM.

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.