DORA
Whitepaper

What cybersecurity challenges will the financial sector face?

Abstract

The Regulation on Digital Operational Resilience in the Financial Sector (DORA) is an EU regulation that aims to strengthen the digital security and resilience of financial organisations. It aims to ensure that financial institutions take appropriate precautions to protect themselves against cyberattacks and other IT-related risks. DORA sets out requirements for risk management, monitoring and reporting of IT incidents. It also requires financial organisations to carefully monitor and control third-party providers of IT services. The aim is to ensure the stability and integrity of the European financial system in an increasingly digital world.

Introduction

On 17 November, the European Council adopted the Regulation of the European Parliament and of the Council on digital operational resilience in the financial sector ("DORA" for short) and it will enter into force 20 days after publication in the Official Journal of the EU. 24 months later, i.e. from 17 January 2025, the regulation will then apply directly and bindingly in every member state. As it is a regulation, no separate national implementation is required; the text applies equally in all member states. The regulation is part of the European Commission's action plan from 2018 with the aim of creating a competitive and innovative European financial sector. The primary objectives of the action plan are to improve the cyber resilience of financial companies and to harmonise specific requirements for the security of financial companies' information and communication technology (ICT).

Scope of application

Due to the objective of creating a coherent approach to the management of ICT risks in the financial sector in the EU - with the aim of strengthening the digital operational resilience of the financial services industry - a very broad scope has been chosen, which, in addition to traditional credit institutions, payment institutions and financial market infrastructure institutions such as central securities depositories, central counterparties and trading centres, also includes all financial service providers in the broader sense, such as investment firms, investment funds, providers of crypto services, account information service providers, insurance companies and insurance and reinsurance undertakings, insurance intermediaries, credit rating agencies and all their data reporting services and third-party ICT service providers. Article 2 provides for some (few) exemptions from the Regulation as well as certain simplifications (e.g. a simplified ICT risk management framework) for financial service providers that are recognised as "micro-enterprises" (fewer than 10 employees and an annual turnover or annual balance sheet of less than EUR 2 million). In all regulations, reference is made to the principle of proportionality, in which the size, overall risk profile and the type, scope and complexity of the financial service provider's services and transactions must be taken into account. DORA is regarded as a lex specialis for NIS 2, which was adopted at the same time.

Therefore it replaces NIS 2 for all affected companies. At the same time, DORA is significantly more comprehensive and far-reaching in some points (e.g. requirements for the ICT risk management framework and protective measures to be implemented) than the similarly designed NIS 2 Directive, which means that it can be assumed that the national supervisory authorities will be guided by the more detailed requirements of DORA when implementing the standards.

Risk management requirements

Article 5 Governance and organisation requires financial entities to have an internal governance and control framework that *ensures effective and prudent management of ICT risks in order to* achieve a *high level of digital operational resilience.* The financial company's management body is responsible for implementing all arrangements relating to the ICT risk management framework. This includes, but is not limited to, the allocation of *appropriate budget resources.* The management body must also ensure that it is kept up to date on all risk-related issues, including agreements on the use of ICT services. Furthermore, DORA requires that the members of the financial organisation's management body have sufficient *up-to-date* knowledge and skills on ICT risks - this means that they must regularly complete specific training courses. It can be assumed that this will be included in an extended catalogue of requirements for Fit & Proper examinations.

Section 2 of DORA then sets out detailed requirements for the ICT risk management framework, which must include strategies, policies, procedures, ICT protocols and tools to *properly and adequately* protect all ICT assets, as well as all relevant physical components and infrastructure, e.g. premises, data centres and designated sensitive areas. This ICT risk management framework must be documented and managed by an independent control function in accordance with the three lines of defence model and reviewed at least annually. The ICT risk management framework must describe the risk tolerance threshold, define key performance indicators and risk metrics and continuously review its effectiveness through testing and monitoring. Furthermore, an ICT reference architecture must be defined and the systems covered by it must *always be* kept up to date. The following articles describe the security lifecycle of "identification", "prevention" and "detection",
"Response" and "Recovery" all the minimum requirements that the ICT risk management framework must contain to fulfil the security objectives. This concerns all the key topics described by common security standards such as ISO 27001 or NIST 800-53: Scenario analysis, business impact analysis, asset management, change management, protection of availability, authenticity and integrity of data, authorisation management and authentication through to business continuity guidelines and contingency planning. Technical measures are also described in concrete terms, such as the ability to recognise anomalies and immediately disconnect or segment network connections if necessary. By specifying concrete technical capabilities at regulation level, DORA goes further than any existing legal text at EU level. DORA also specifies very concrete requirements with regard to disaster recovery & BCM, guidelines for recovery times and recovery points, which minimise the potential overall impact on the market efficiency, as well as redundant ICT capacities with

sufficient resources and their own risk profile, which must also be comprehensively tested on a regular basis, including the full failover tests often feared by IT departments. DORA explicitly demands that the agreed service quality is also achieved *in extreme scenarios.*

Handling of critical incidents and reporting obligations

Chapter 3 deals with the handling of ICT-related incidents, which also include "*significant cyber threats*". Early warning indicators must be used for these and suitable classification, response and communication measures must be provided. Furthermore, DORA - analogous to NIS - provides for a reporting obligation for serious security incidents, with an initial report, interim reports and a final report. The exact deadlines and formats of the reports will be defined by the ESA within 18 months as part of technical regulatory standards. Financial service providers are given the right to outsource reporting obligations under this article to a third-party service provider, whereby they always retain full responsibility for fulfilling the requirements. Furthermore, the ESAs are to examine the extent to which further centralisation of reporting is possible and what the requirements are for the establishment of a uniform EU reporting platform. This would make it easier for financial companies to fulfil their current multiple reporting obligations.

Testing resilience

DORA also focuses on requirements for testing digital resilience, to which a separate chapter is dedicated. The central point is that all ICT systems and applications that support critical or important functions must undergo appropriate testing at least once a year. Tests are very broadly defined and include vulnerability assessments and scans, open source analyses, network security analyses, physical security checks, software solution scans, source code checks, scenario-based tests, compatibility tests, performance tests, end-to-end tests and penetration tests. These tests must be carried out by independent, internal or external testers, with at least every third test being carried out by external parties. Financial organisations that are classified as significant are also required to carry out a threat-led penetration test (TLPT) at least every three years, which must include several or all critical or important functions of a financial organisation and must be carried out on live production systems. Third-party ICT service providers may also be involved in these tests. Once the tests have been completed, a summary of the relevant results, the corrective action plans and the documents proving that the test was carried out as required must be submitted to the authority. With regard to TLPTs, the ESA will also develop technical regulatory standards within 18 months that specify the scope and test methodology in more detail.

Management of ICT third-party risk

Another key point of DORA is the management of ICT third party risk, which is dealt with in Chapter 5. Financial companies are obliged to manage the ICT Third-party risk as an

integral part of ICT risk and a strategy and associated guidelines must be drawn up for this purpose. Companies are obliged to keep an information register of all contractual agreements with third-party ICT service providers and to keep it up to date. The management body is required to regularly monitor and review the risks associated with contractual agreements on the use of ICT services; a separate function must be set up to monitor the use of ICT services. Before entering into any contractual agreement for the use of ICT services, financial organisations must ensure that these service providers comply with *appropriate information security standards* and, in the case of critical or important functions, even the *latest and highest quality standards for information security*. This must be ensured throughout the selection and evaluation process and is seen as part of due diligence. Financial companies must ensure that third-party ICT service providers meet their information security and resilience requirements and integrate them into their relevant training programmes as required. Financial organisations must also ensure that contractual agreements for the use of ICT services can be terminated if demonstrable weaknesses in the ICT third-party service provider's general ICT risk management become known, particularly in the way in which it ensures the availability, authenticity, security and confidentiality of data. To this end, suitable *exit strategies* must also be defined that allow the financial company to withdraw from contractual agreements without interrupting its business activities and without jeopardising the continuity and quality of the services it provides to customers.

Regulatory & technical standards

Although the requirements are already relatively specific in the text of the regulation, the three ESAs (EBA, EIOPA and ESMA) have been tasked with specifying the requirements for many requirement areas in much greater detail as part of regulatory technical standards. The European Commission adopted the **first tranche** of the drafts of the three E S A s (EBA, EIOPA and ESMA) on 13 March 2024 and they are currently in the 3-month review phase before they are published. The first tranche of regulatory and implementing technical standards includes:

- RTS on the ICT risk management framework (Art. 15) and the simplified ICT risk management framework (Art. 16 para. 3)
- RTS on Criteria for the of ICT related incidents (Art. 18 para. 3)
- RTS on the Guideline on the use of ICT services of critical or important functions (Art. 28 para. 10)
- ITS for the creation of a standard template for the information register (Art. 28 para. 9).

The consultation phase for the second tranche of the RTS and ITS drafts has already been successfully completed. These include:

- Threat Led Penetration Testing (Art. 26 para. 11)
- Specification of elements in the subcontracting of critical or important functions (Art. 30 para. 5)
- Determination of the reporting of serious ICT incidents (Art. 20.a)

- Specification of the details of reporting on major ICT-related incidents (Art. 20.b)
- Harmonisation of the conditions for carrying out monitoring activities (Art. 41)

The feedback on the drafts will now be evaluated by the European working groups with the aim of also sending the final drafts to the European Commission by 17 July 2024.

Monitoring framework for critical ICT third-party service providers

In order to mitigate concentration risks, DORA also provides for a separate *monitoring framework for critical third-party ICT service providers.* This should include third-party ICT service providers that have a systemic impact on the stability, continuity or quality of the provision of financial services or that serve a (yet to be determined) number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs). This should also take into account the degree of substitutability of the third-party ICT service provider. Group-internal ICT service providers should not fall within the monitoring framework of critical third-party ICT service providers. The ESA will draw up, publish and update the list of critical third-party ICT service providers. A separate supervisory authority will be established for these, which will assess whether each critical ICT third-party service provider has comprehensive, sound and effective rules, procedures, mechanisms and arrangements for the management of ICT risks listed in Article 33 and complies with the requirements for financial undertakings. To this end, an individual monitoring plan is drawn up for each critical ICT third-party service provider, in which the planned annual monitoring objectives and key monitoring measures are described. The supervisory authority is given extensive powers and sanction options for this purpose, ranging from the imposition of fines amounting to 1% of the average global daily turnover and the restriction of subcontracting to the possibility of obliging financial companies to terminate the contractual agreements concluded with this critical ICT third-party service provider. The expenses incurred by the supervisory authority for the performance of supervisory tasks are charged in full to the critical ICT third-party service providers.

Supervisory framework and sanctions

The Regulation also establishes *appropriate administrative sanctions and remedies for breaches of* the Regulation for financial undertakings themselves, which should be effective, proportionate and dissuasive.
DORA establishes a strict supervisory framework for operational risks that is standardised across Europe for the first time. In addition to the strict measures defined by DORA, which should lead to a further improvement in the resilience of European financial service providers, this will bring harmonisation, particularly for internationally active financial service providers, which will lead to improved legal certainty within the European framework.

The complete legal text can be found at
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554