MITRATECH

Mastering DORA's
Regulatory Framework
White Paper

Mastering DORA's Regulatory Framework

Navigate through the challenges in your DORA compliance journey and leverage the powerful business opportunities of becoming compliant with this regulation.

GENERAL OVERVIEW OF DORA

Let's start at the beginning.

Why is DORA needed?

DORA aims to homogenize requirements across the EU, so that financial services organizations are able to withstand, respond, recover and maintain their operations even under severe operational disruptions.

Since 2008 and following the financial crisis, the European Commission (EC) has been focusing on strengthening the financial resilience of the financial sector. ICT risks were covered indirectly or partially by some of the Member states and this disparity resulted in inconsistencies and duplication of rules, especially for areas like incident reporting, security requirements and testing.

In April 2020, the three European Supervisory Authorities (EBA, ESMA and EIOPA) collectively called for a coherent approach to address the ICT risks in the financial sector and recommended strengthening the digital operational resilience of the financial services industry through a EU specific initiative.

In September 2020, the EC published its draft on DORA as part of the Digital Finance Package. The legislative proposal seeks to establish supervisory convergence by building on regulatory initiatives introduced by various European regulators, including the European Central Bank (ECB).

DORA shifts the focus from only guaranteeing firms' financial resilience to also ensuring they can maintain resilient operations through an incident of severe operational disruption. Furthermore, DORA establishes a comprehensive and cross-sectoral digital operational resilience framework for all regulated financial institutions. The regulation additionally introduces unprecedented direct supervision of critical ICT third-party providers through financial authorities.

The key objective of DORA is to improve operational resilience in financial services institutions and enhance business continuity practices in the event of a significant business disruption. The regulatory framework touches five main areas:

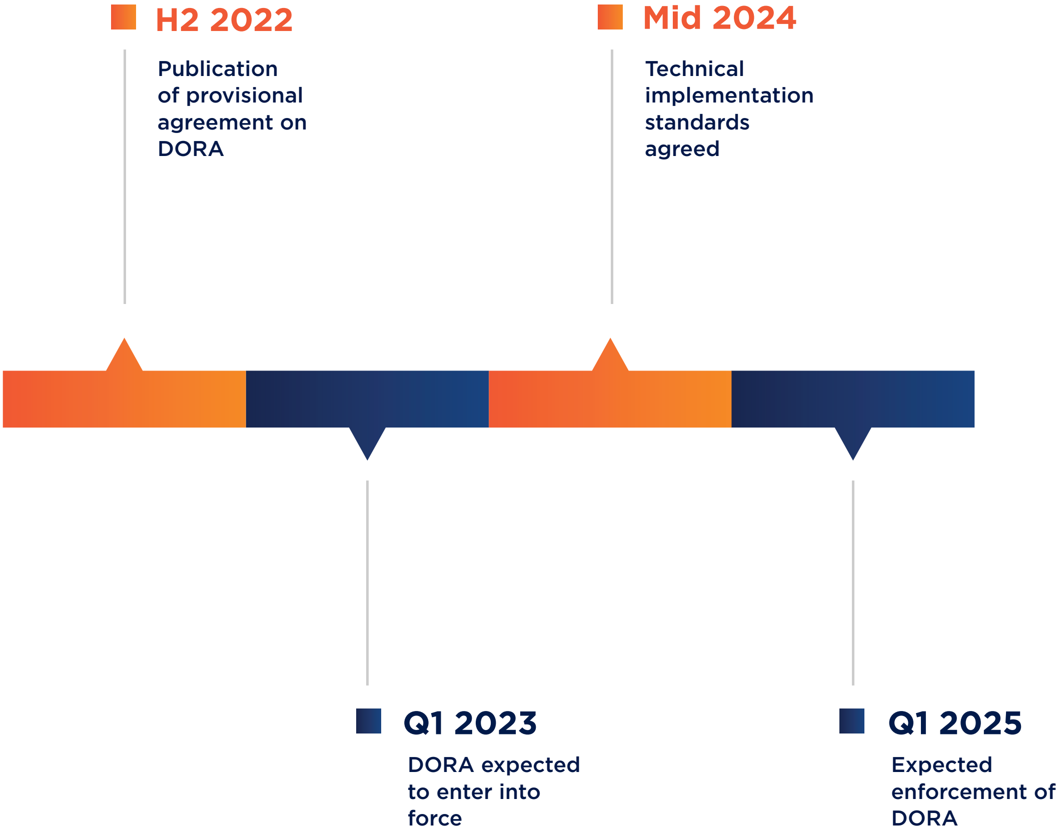
- **ICT Risk Management**
- **ICT Incident Management & Reporting**
- **Digital Operational Resilience Testing**
- **ICT Third-Party Risk Management**
- **Information & Intelligence Sharing**

DORA TIMELINE

After the co-legislators (European Commission, European Parliament and European Council) reach a provisional agreement on the wording of the legal text on September 24th 2022, DORA will be expected to enter into force in February 2023.

The legal act comprises high level ***framework principles,*** which are specified and detailed by technical implementation measures. The European Supervisory Authorities (ESAs) have been tasked with developing acts to provide technical guidance to relevant entities in implementing the requirements under DORA.

Nearly all financial services institutions operating in the EU and impacted third-parties must ensure compliance with DORA's regulatory framework by January 2025.



H2 2022

Publication of provisional agreement on DORA

Q1 2023

DORA expected to enter into force

Mid 2024

Technical implementation standards agreed

Q1 2025

Expected enforcement of DORA

KEY PROVISIONS & UNIQUE DORA REQUIREMENTS

DORA includes 56 articles organized in 6 chapters, highlighting several unique requirements in comparison to other existing EU and financial regulations:

CHAPTER 1

General Provisions

Establishment of a new direct Oversight Framework of European Supervisory Authorities (ESAs) towards Critical Third-Party Providers (TPPs).

DORA's scope encompasses nearly all financial services institutions: banks, credit institutions, alternative fund managers, insurance companies, payment institutions, as well as crypto-currency, crypto-asset issuers, token issuers, and more.

CHAPTER 2

ICT Risk Management

Operational risk broadly encompasses risk factors related to a firm's people, processes, and technology. To comply with DORA, financial services institutions must maintain digital operational resilience, with an expanded and more granular risk definition that includes malfunction, capacity overrun, failure, disruption, impairment, misuse, and loss.

Prescriptive standards for a sound ICT Risk Management Program, that include:

- Digital Resilience Strategy
- Defined Risk Tolerance (ICT Risk)
- Identification, Classification, Documentation of all ICT-Related Business Functions & Information Assets
- ICT Policy / Procedure In Line with ESA + ENISA Tech Specs

Financial institutions are required to have a comprehensive ICT risk management framework with a strong business continuity strategy, as well as identification and classification of critical business functions.

The regulation does not impose specific standardization, but rather builds on leveraging internationally accepted standards.

CHAPTER 3

ICT-Related Incidents, Management, Classification and Reporting

Financial services institutions already must collect data on ICT incidents, report major issues to the authorities and act on supervisory feedback. Under DORA, they must extend these incidents within critical third-parties. Naturally, this means the volume of incidents to report will increase.

Furthermore, financial services institutions are required to have a streamlined process to log/classify all ICT incidents and determine major issues.

Reporting of major incidents needs to be harmonized through standard templates. Centralization of the reporting process might be explored by establishing a single EU hub for reporting of major incidents.

KEY PROVISIONS & UNIQUE DORA REQUIREMENTS

CHAPTER 4

Digital Operational Resilience Testing

Financial services institutions will conduct digital operational resilience testing, with broader threat-led penetration. These testing must include third-party service providers, to help assess whether their cybersecurity is fit for purpose. This will require ongoing review, in light of the rapidly changing nature of threats.

The regulation also requires that all entities perform periodic basic ICT testing of tools/systems and advanced Threat Led Penetration Testing (TLPT) for ICT services which impact critical functions. It further details requirements for testers and reporting of the TLPT results across the EU.

The Threat Led Penetration Testing (TLPT) should be conducted by an external independent tester, scenarios should be approved by regulators and all critical TPPs should be included in TLPT.

CHAPTER 5

ICT Third-Party Risk Management

Critical third-party providers must be held accountable for providing services consistent with DORA, which might even require financial institutions to renegotiate contracts or change suppliers. It's likely that some providers will raise their prices to recoup the cost implications of DORA compliance.

Critical ICT TPPs would need to establish a subsidiary in the EU and will be subjected to direct supervision of the regulators.

Furthermore, the regulation will allow financial services institutions to monitor ICT third-party risks even during the termination, conclusion and post contractual phases. It seeks to promote subjecting critical ICT third-party service providers to a EU oversight framework.

CHAPTER 6

Information & Intelligence Sharing Arrangements

DORA encourages financial services institutions to voluntarily share cyber threat intelligence, detection techniques, mitigation strategies, response and recovery procedures across the industry. It allows financial services institutions to set-up arrangements amongst themselves to exchange these information.

Navigate Through The Challenges & Leverage The Opportunities of DORA

- Do not treat DORA compliance as a one-off, check-in-the-box exercise.
- Leverage GRC technology to streamline your process.
- Obtain visibility of operational resilience blind spots within your organization.

HOW MITRATECH'S ALYNE CAN HELP

As of January 2023, DORA can be found within Mitratech's Alyne Library in both English (Original Version) and fully translated into German. Customers can now download the regulation from the Library Store and start building and mapping.

Mitratech's Alyne GRC solution offers a fully centralized and customizable platform for managing compliance with DORA and all other relevant standards, laws, and regulations that impact your organization. Businesses can tailor the solution to their own unique environment, requirements and processes, making it easier to implement and manage compliance. This enables organizations to automate key compliance tasks, streamline their efforts and easily track their progress.

Furthermore, leverage Alyne's automated risk assessments to easily identify and prioritize risks in order to proactively take measures to mitigate these risks and ensure compliance.

Mitratech Alyne's real-time monitoring enables organizations to detect and respond to threats quickly, reducing the risk of non-compliance and potential damage to the organization. Moreover, Alyne provides detailed reporting and analytics capabilities that enable data-driven decision-making.

Reach out to our team for more information on how to leverage Mitratech's Alyne in your DORA compliance journey and utilize the powerful advantages of partnering with next-generation GRC technology.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

Mitratech serves over 7,700 organizations worldwide, including 30% of the Fortune 500 and over 500,000 users in 160 countries.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com