
# An Introduction to DORA

Sam Glynn, Code in Motion Ltd

June 2023, Version 1.0.

# Introduction

The DORA (Digital Operational Resilience Act) Regulation will apply from January 2025.

The objective of the regulation is to ensure regulated financial services firms (and their external ICT service providers) achieve and sustain a high level of digital operational resilience.

The purpose of this document is:

1. To introduce you to the structure of DORA so you gain a high-level understanding of the regulation, and
2. To suggest a way to get started with your compliance efforts without losing your sanity.

## Intended Audience

Anyone who works in the regulated financial services industry and who needs to get their head around what the European IT / cyber security regulatory environment will look like over the coming years.

## Accessing The Regulation

You can access the official text of the regulation at:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN.

However, there are online resources that make it easier to navigate the text of the regulation. For example, Springflod has developed such a facility at:
https://www.dora-info.eu/.

## Disclaimer

This is not a comprehensive review of the requirements or implications of the regulation. The content is provided in good faith but without warranty of any kind.

# Introducing DORA

## It's not all about you.

There are **64 articles** within the text of the DORA regulation. But…

If you work in a regulated financial services firm, you are likely to focus on **29 of them**.

The other 35 articles discuss how the regulators will operate the regulation and how they can use the regulation to oversee the activities of critical ICT (Information and Communication Technology) service providers.

## The Structure of DORA

**An introduction** into the 'what' and 'who' of DORA is provided in Articles 1-4.

**The 5 key requirement areas** (aka chapters) of DORA are then defined in the following Articles.

| Chapter | Articles |
|---|---|
| 1 - ICT (Information and Communication Technology) Risk Management | 5-16 |
| 2 - ICT Incident Management, Classification and Reporting | 17-20.<br><br>** Plus Article 23 if you are a credit or payment institution.* |
| 3 - Testing of Operational Resilience | 24-27 |
| 4 - IT Third Party Risk Management | 28-30 |
| 5 - Information Sharing | 45 |

## What about the others?

**Articles 31-44 are relevant to critical ICT Service Providers**. These Articles are worth reading. However, unless you work for a regulator or critical ICT service provider (e.g. Microsoft), I don't see anything in these articles that you should focus on right now.

**Articles 21-22 and 46-64 are primarily of relevance to regulators**. Again, worth reading but not an area of focus for you right now.

# How To Get Started

## 1. Check if DORA will apply to you.

The scope of DORA excludes certain types of regulated entities, including:

a. Some managers of alternative investment funds.

b. Some insurance and reinsurance undertakings.

c. Some institutions involved in small occupational pension schemes.

d. Some insurance / reinsurance / ancillary insurance intermediaries.

e. Some post office giro institutions.

So, your first step should be to see if your firm falls into the 'Does Not Apply' list provided in Article 2 (3).

## 2. See if there are any reduced obligations for you.

Your next step should be to identify your firm's type and size (as defined by DORA).

This is worthwhile because you may find that your firm will benefit from the exclusions or reduced obligations defined within certain Articles of DORA.

For example, Article 16 defines reduced ICT Risk Management obligations for certain sizes / types of firms.

### Type

Articles 2 & 3 include definitions for each type of firm that will be within the scope of DORA. The full list is too long to include here.

### Size

Micro, small and medium enterprises are defined in Article 3 (60, 63, 64):

| | Number of Staff | Turnover and/or Balance Sheet |
|---|---|---|
| **Microenterprise*** | < 10 | < €2m |
| **Small enterprise** | < 50 | < €10m |
| **Medium-sized enterprise** | < 250 | < €50m turnover and/or<br>< €43m balance sheet |

** excluding trading venues, central counterparties, trade repositories, and central securities depositories.*

## 3. Identify your Critical and Important Functions

Your next step should be to identify your critical and important functions. Otherwise, you may end up trying to boil the ocean.

DORA defines critical and important functions in Article 3(22):

> *"Critical or important function' means a function the disruption of which would materially impair*
>
> - *the financial performance of a financial entity, or*
> - *the soundness or continuity of its services and activities,*
>
> *or the discontinued, defective or failed performance of that function would materially impair*
>
> - *the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or*
> - *with its other obligations under applicable financial services law"*

To identify your critical and important functions, there may already be sources within your firm to help you – For example:

- Your firm's Business Impact Analysis (BIA) or Business Continuity Planning (BCP) documents.
- The Records of Processing Activities (RPA) register that may have been created as part of your GDPR / data protection compliance efforts.

If you don't have any of these, a rough way to identify some of your critical and important functions is to think about the processes that would cause the most disruption if they were to fail or to operate at a slower pace than normal. These will probably include processes that are client-facing – e.g. payments; customer support.

## 4. Get to know the NIST Cyber Security Framework

The NIST Cyber Security Framework (CSF) (https://www.nist.gov/cyberframework) is a well-known cyber security framework that can help an organisation begin or improve their cybersecurity controls.

Many risk frameworks are organised around the 5 key areas of identify, quantify, manage, monitor, and report (e.g. COSO, ISO 31000).

In a similar way, NIST is organised around 5 'functions':

f. Identify – Where are your assets?

g. Protect – How will you protect these assets?

h. Detect – How will you spot suspicious activity or anomalies?

i. Respond – How will you respond to these?

j. Recover – How will you return to full service?

It is not a coincidence that Articles 8-11 of DORA see to align to NIST's functions:

- Article 8: Identification
- Article 9: Protection and Prevention
- Article 10: Detection
- Article 11: Response and Recovery

If your firm does not already align to a recognised cyber security framework, it may be beneficial for you to use the NIST CSF as a reference during your DORA preparations.

## 5. Get ready for Technical Standards

While DORA already defines specific obligations, it also requires regulators to agree and publish additional 'Technical Standards' over the coming months.

For example: Article 15 requires technical standards to be developed by January 2024 that will provide more specifics on the requirements for:

- ICT security policies, procedures, protocols, and tools,
- controls of access management rights,
- prompt detection of anomalous activities,
- ICT business continuity policy, and
- components of the ICT response and recovery plans.

Other Technical Standards may not be published until July 2024, only 6 months before DORA applies. This includes standards relating to the elements that a financial entity must assess when subcontracting ICT services that will support critical or important functions. (Article 30(5)).

So, while you need to get on with DORA compliance now, you also need to recognise that some of the specific requirements may not become clear until as late as July 2024.

## What Now?

I hope this document helped you to get your head around the structure of DORA, and how you can get started with your compliance efforts without losing your sanity.

If you're interested in delving deeper into the intricacies of the regulation and gaining a more detailed understanding of its requirements, I have developed a short email course to help you.

Each email will delve into the details on each of the 5 areas of DORA, to ensure you have a solid grasp of the obligations.

I will also suggest ways that you could comply with the obligations in a logical, pragmatic way.

Whether you work in a regulated entity or a service provider, whether you are in a compliance role or operational role, this email series will equip you with the knowledge you need.

Don't miss out on this valuable opportunity to deepen your understanding of DORA so you can comply without losing your sanity.

You can sign up at https://codeinmotion.ie/dora/.

# About Me

I'm Sam Glynn.

I interpret IT & Cyber Security Risks and Regulations into Actionable Advice, enabling my clients to manage IT and cyber security risks without losing their sanity.

I am a Certified Information Security Manager (ISACA CISM) and a Certified Data Protection Officer (Compliance Institute CDPO, IAPP CIPP/E, and IAPP CIPM).

I have been working with First Line and Second Line teams in regulated financial services firms for over 25 years, providing independent advice to executives and senior managers.

If you are worried about a cyber attack, but too busy to do anything about it, I can help.

I ensure you do not spend too much of your time, money or sanity implementing a reasonable level of security.

You gain clarity about where you are, where you need to be, and how to get there as quickly and efficiently as possible.

Learn more at https://codeinmotion.ie/