

A close-up photograph of a hand resting on a computer mouse, positioned on the left side of the image. The background is a dark, blue-tinted scene with floating binary code (0s and 1s) and faint, semi-transparent lines of code, suggesting a digital or data environment.

# Digital Operational Resilience Act (DORA)

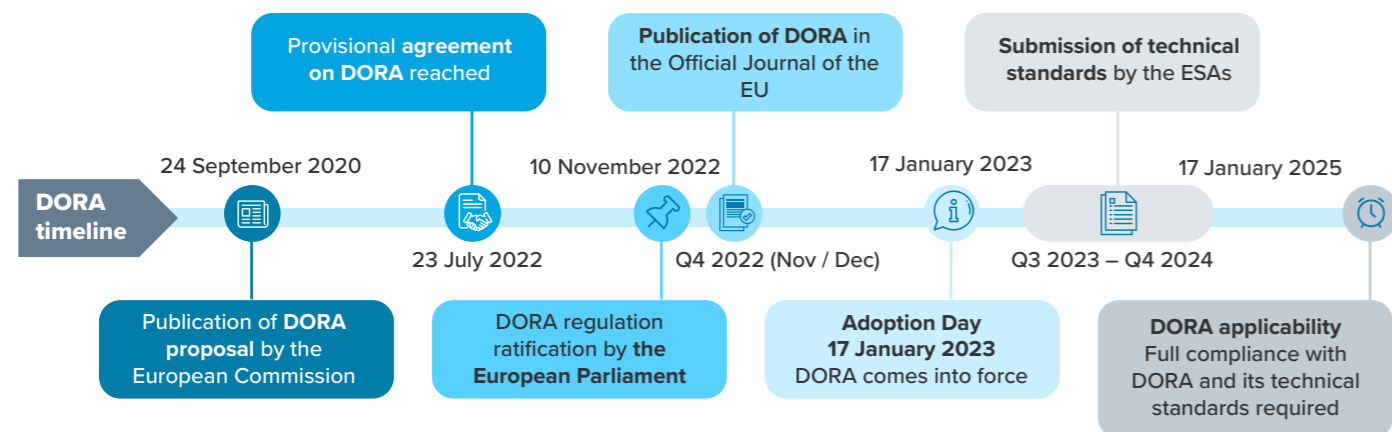
Navigate DORA with confidence

# OVERVIEW OF DORA

The objective of DORA is to improve the cybersecurity and operational resilience of all regulated European financial institutions and of critical, third-party ICT service providers.

The Digital Operational Resilience Act establishes a unified set of requirements for the security of network and information systems of companies and organisations operating in the financial sector, as well as third parties that provide ICT-related services to them (e.g., cloud platforms or data analytics services). In addition, DORA establishes a regulatory framework on digital operational resilience, where all firms need to ensure they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. The requirements are the same across all EU member states, as they aim to prevent and mitigate the growing number of cyber threats.

## The DORA implementation timeline



# IN-SCOPE ENTITIES

In-scope entities will have to implement the regulation and become fully compliant by the 17<sup>th</sup> January 2025.

DORA applies to a wide range of organisations, including licensed financial institutions, such as banks, insurance companies, investment firms, stock exchanges, fintech companies, etc. and ICT third-party service providers such as cloud computing services, software, data analytics services and data centres.

DORA puts the relationship between the financial institutions and their technology suppliers in a new light to jointly address the regulatory requirements.

Financial entities and ICT third-party service providers should increase their collaboration to address the requirements of this new regulation.

## Who is responsible?

Overall, responsibility for this framework, and other governance obligations imposed by DORA, will rest on the firm's management, which will be responsible for reviewing, approving, implementing and updating the risk management framework.

Management will be required to have full awareness and understanding of the financial institution's ICT usage, services and risk profile. Companies may want to assess how reporting lines from their ICT department to senior management actually operate on a daily basis.

The financial institutions that are subject to DORA must appoint a senior executive responsible for digital operational resilience and report incidents to the appropriate authorities.

## Entities affected by DORA as per Article 2 - Scope

### Financial entities

- ▶ Credit institutions
- ▶ Payment institutions
- ▶ Account information service providers
- ▶ Electronic money institutions
- ▶ Investment firms
- ▶ Crypto-asset service providers and issuers of asset-referenced tokens
- ▶ Central securities depositories
- ▶ Central counterparties
- ▶ Trading venues
- ▶ Trade repositories
- ▶ Managers of alternative investment funds
- ▶ Management companies
- ▶ Data reporting service providers
- ▶ Insurance and reinsurance undertakings
- ▶ Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- ▶ Institutions for occupational retirement provision
- ▶ Credit rating agencies
- ▶ Administrators of critical benchmarks
- ▶ Crowdfunding service providers
- ▶ Securitisation repositories

### ICT third-party service providers\*

- ▶ Providers of cloud computing services
- ▶ Software
- ▶ Data Analytics services
- ▶ Providers of data centre services
- ▶ Undertakings that are part of a financial group and provide ICT services predominantly to their parent undertaking, or to subsidiaries or branches of their parent undertaking
- ▶ Financial entities providing ICT services to other financial entities
- ▶ Participants in the payment services ecosystem, providing payment processing activities or operating payment infrastructure

*\*The entities listed are examples of ICT Third Party Service Providers.*



## IMPACT OF DORA

**While DORA allows a transition period until 17<sup>th</sup> January 2025, compliance can be challenging and time-consuming for the in-scope entities.**

Achieving compliance with the onerous DORA obligations within the stipulated timeframe will be challenging and time-consuming. While DORA allows a transition period until 17 January 2025, BDO recommends that in-scope organisations kick-off preparations immediately.

BDO recommends adopting a phased approach whereby the in-scope entities chart a DORA compliance program with the aim of achieving DORA compliance by the end of the transition period.

Failure to achieve compliance may lead to severe fines from January 2025 onwards.

### Compliance

The respective national competent authorities will take the role of Lead Overseer and enforce the regulation as necessary. EU Member States will have the right to impose penalties for breach of obligations.

The significant penalties will take the form of a periodic payment of 1% of the average daily global turnover of the organisation in the preceding business year. This will be applied by the Lead Overseer daily until compliance is achieved for no more than a period of six months.

### Our recommendation

We recommend the following action points:

- ▶ Perform a maturity assessment against the DORA requirements, with associated gap analysis and mitigation plan to reach compliance by the end of 2024.
- ▶ Enhance your ICT Risk Management program making sure you have a complete view on your critical systems and measures in place to mitigate or minimise risk.
- ▶ Build a register of critical ICT service providers and perform third-party risk assessments.

# REQUIREMENTS

DORA consists of 58 articles and is structured around five key pillars:




## OUR SOLUTION


Cyber attacks have been dominating the risk landscape for organisations around the world for years. Critical sectors to our society such as finance, health, transportation and energy are increasingly dependent on technology making these sectors vulnerable to serious disruptions if technology risks are not mitigated sufficiently.


As a result, businesses have been increasing their investments to up their resilience and security maturity significantly. It is important to realise that all these investments in good governance and secure digital infrastructure are not lost but rather are in itself already corner stones of past and upcoming cyber regulations such as DORA and NIS2.


At BDO, we recognise these efforts and are there to help you assess your current level of compliance and development needs in an efficient and controlled manner.

### How BDO can help?

- 

1 Assess the extent to which the DORA regulation applies to your organisation
- 

2 Perform a DORA gap analysis and assess your current cyber maturity and resilience level
- 

3 Define a prioritised security roadmap that includes DORA specific requirements for your organisation, but which also keeps an eye on compliance with other applicable legislation and regulations.
- 

4 Assist with project management and/or hands-on execution of the security roadmap, e.g. putting in place key policies and procedures, performing resilience testing, managing the penetration testing and implementation of subsequent recommendations, performing third-party/vendor risk assessments, ...



## FOR MORE INFORMATION:

### **RONALD WESTERVEEN**

Senior Manager BDO NL  
Ronald.Westerveen@bdo.nl

### **HARRY WALLACE**

Assistant Manager BDO UK  
Harry.Wallace@bdo.co.uk

### **IVAN SPITERI**

Director BDO Malta  
ivan.spiteri@bdo.com.mt

### **TOMAS KUBICEK**

Partner BDO Czechia  
Tomas.Kubicek@bdo.cz

### **MARTIN HORICKY**

Partner BDO Czechia  
martin.horicky@bdo.cz

### **AYKUT BUSSIAN**

Partner BDO Germany  
Aykut.Bussian@bdo.de

### **CHRISTOPHE DAEMS**

Partner BDO Belgium  
Christophe.Daems@bdo.be

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities. The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV July 2023

[www.bdo.global](http://www.bdo.global)