



BDO Malta

**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.

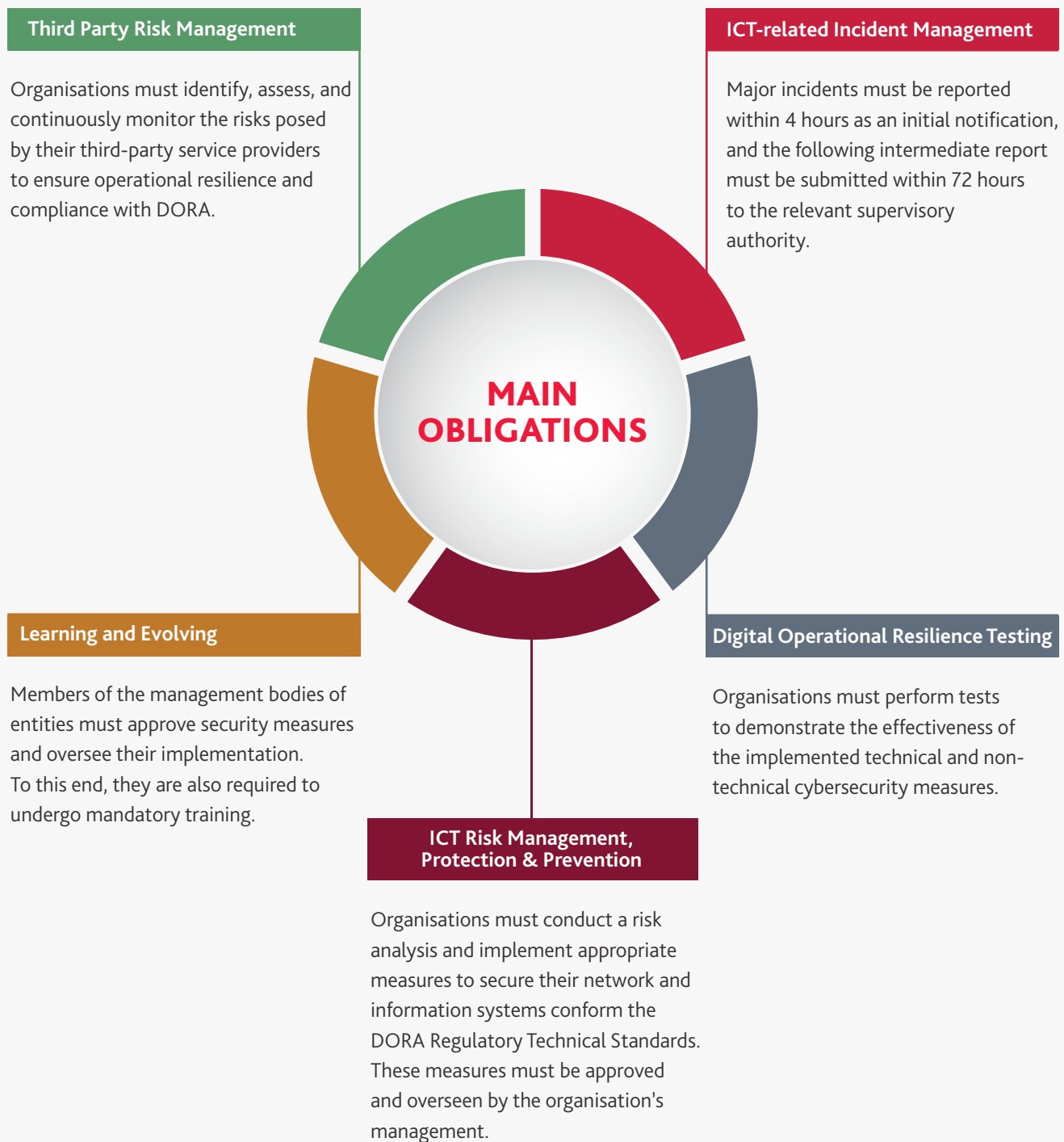
The Digital Operational Resilience Act establishes a unified set of requirements for the security of network and information systems of companies and organisations operating in the financial sector, as well as third parties that provide ICT-related services to them (e.g., cloud platforms or data analytics 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.

**"To strengthen the ICT security and resilience of financial entities in Europe in the face of a severe operational digital disruption, and harmonise the rules for operational resilience across the European financial sector."
(ESMA)**



Main Obligations







DORA In-Scope Entities

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.



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.

**This is not an exhaustive list. Please contact us for an assessment relevant to your business.*

Responsibility for DORA Compliance

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.

Board responsibility for DORA Compliance - Art. 5 (2)

 Ultimate Responsibility	 Digital Resilience Strategy	 Third-Party Service Providers
 Data Integrity and Confidentiality	 Business Continuity and Response Plans	 Monitoring Third-Party Arrangements
 Clear Roles and Responsibilities	 Internal Audit and Budgeting	 Continuous Education



Impact & Implications



Wider Implications

The goal of the EU-wide uniform legal framework for digital operational stability is to make sure that companies can react to ICT-related threats and interruptions. Cyber hazards are to be avoided or reduced in this way.

Management bodies would be completely accountable for their:

- ▶ ICT risk management;
- ▶ Establishing and approving its DORA strategy;
- ▶ Approving policy in relation to the Third-party ICT service providers

Companies are challenged to increase their operational resilience capabilities and concentrate on being able to map and understand the relationship between their ICT assets, processes and systems and how they support service delivery



Financial Entities

Significantly updated classification, notification, and reporting guidelines will put pressure on businesses to improve how they gather, analyze, escalate, and communicate information about ICT incidents and risks.

DORA requires that the impact of incidents and root cause analysis be assessed.

Streamlining of ICT incident reporting is required by the framework and this will ease the strain of meeting various incident reporting standards in the financial sector and contribute to a better understanding of global cyber risks.

DORA requires that management develop redundant and sustainable systems to support their critical functions.



Penalties

Competent body can levy administrative penalties and remedial measures in case of any breach of the DORA regulations. However, the penalties for financial entities have not yet been set.

For a maximum of six months, critical ICT third-party service providers will be subject to fines of up to 1% of their average daily worldwide turnover from the prior business year, imposed daily until compliance is achieved.



Requirements

DORA lays out several key requirements, referred to as Level 1 regulations, to achieve its objectives.

Described in the Act itself, these requirements are discussed in the context of DORA's five foundational pillars.

LEVEL 1



ICT Risk Management Requirements (Articles 5 to 16)

- ▶ Governance: accountable management body
- ▶ Risk management framework and associated activities (identification, protection, detection, response and recovery, learning and evolving, crisis communication)



ICT-Related Incidents Management, Classification, and Reporting (Articles 17 to 23)

- ▶ Standardised incident classification
- ▶ Compulsory and standardised reporting of major incidents
- ▶ Anonymized EU-wide reports



Digital Operational Resilience Testing (Articles 24 to 27)

- ▶ Risk-based and proportionate testing program
- ▶ Large-scale threat tests performed by independent testers every 3 years



Managing of ICT Third-party Risk (Articles 28 to 44)

- ▶ Strategy, policy and standardized ICT service provider register
- ▶ Guidelines for pre-contract assessment, contract contents, termination, stressed exit



Information Sharing Arrangements (Article 45)

- ▶ Encouraged to share threat information and intelligence

LEVEL 2

The main text of DORA is supplemented by important technical detail in a body of secondary legislation, referred to as level 2 regulations. The three European supervisory authorities (ESAs) were jointly appointed to draft these standards. The ESAs consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

- ▶ RTS on ICT risk management framework and on simplified ICT risk management framework.
- ▶ RTS on criteria for the classification of ICT-related incidents
- ▶ RTS and ITS on content, timelines and templates on incident reporting
- ▶ RTS on threat-led penetration testing (TLPT)
- ▶ RTS to specify the policy on ICT services performed by ICT third-party providers
- ▶ ITS to establish the templates for the register of information
- ▶ RTS on subcontracting of critical or important functions
- ▶ RTS on oversight harmonization

These technical standards consist of two types:






- ▶ Regulatory technical standards (RTS), of which there are seven;
- ▶ Implementation technical standards (ITS), of which there are two.



BDO Services

BDO offers a comprehensive range of services designed to help clients manage their risks and comply with DORA.

By leveraging BDO's deep knowledge of business operations and risk management, combined with technical capabilities and threat intelligence, clients can effectively manage their cybersecurity risks. BDO's services include employee awareness training, incident response, third-party risk management, penetration testing, and internal audits. These services are aimed to ensure they comply with DORA regulations.

				
Governance	Third Party Risk Management & Assurance	SOC-SIEM	Threat Led Penetration Testing	Internal Audit
<ul style="list-style-type: none"> ▶ Boardroom training ▶ Crisis simulations ▶ Employee awareness ▶ Phishing campaigns 	<ul style="list-style-type: none"> ▶ Baseline assessment ▶ Due Diligence Questionnaire ▶ Third Party Risk Management ▶ Third Party Monitoring ▶ Third Party Assurance (ISAE3402 – SOC1 / ISAE3000-SOC2) 	<ul style="list-style-type: none"> ▶ Managed SOC Services ▶ Threat Intelligence Services ▶ Vulnerability Scanning ▶ Incident Response ▶ Forensic support 	<ul style="list-style-type: none"> ▶ Vulnerability Assessment ▶ Risk analysis ▶ External penetration testing ▶ Internal penetration Testing ▶ Web Application Testing ▶ Social Engineering ▶ Advanced Red Teaming (ART) 	<ul style="list-style-type: none"> ▶ DORA implementation assessment ▶ Review control framework ▶ ICT Risk Management Framework ▶ ICT Response & Recovery Plans ▶ ICT Third Party Suppliers



FOR MORE INFORMATION:

BDO MALTA

Triq it-Torri Msida
MSD 1824
Malta

Tel: +356 2342 4000

info@bdo.com.mt

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO Malta to discuss these matters in the context of your particular circumstances. BDO Malta, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO Malta or any of its partner, employees or agents.

BDO Malta, a Maltese civil partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

Copyright © May 2025 BDO Malta. All rights reserved. Published in Malta.

www.bdo.com.mt

