MAMO TCV
ADVOCATES

A Brief Overview of the **Digital Operational Resilience Act (DORA)**

1st edition

July 2024

www.doramalta.com

Check the link above for any updated versions of this overview

What is 'DORA'?

The Digital Operational Resilience Act (DORA) is a directly applicable EU regulation implemented to enhance and improve information and communications technology (ICT) risk requirements across various financial sectors in the European Union, including Malta. Among other things, DORA imposes legal obligations on a vast array of different financial entities as well as certain ICT service providers that assist such financial entities. DORA, with the full name thereof being 'Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011', is part of the EU's wider digital finance package.

When does DORA become effective?

DORA is already in effect, but it will become applicable, across the EU, on **17 January 2025**. Certain financial entities, including those in Malta, are already expected to have commenced their compliance efforts.

Who is in scope of DORA?

Subject to certain exemptions, DORA applies to a vast range of '**financial entities**' *including*:

- Credit institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- AIFMs
- Crypto asset service providers
- Payment institutions
- Central securities depositories
- Credit rating agencies
- Data reporting service providers
- Insurance & reinsurance undertakings
- Insurance intermediaries
- Crowdfunding service providers
- Securitisation repositories.

DORA directly applies to these financial entities as well as certain **'ICT service providers'**. These are defined in DORA as being any undertaking that provides ICT systems and services to financial entities on an ongoing basis, including hardware as a service, as well as hardware services that incorporate technical support through means of software or firmware update.

DORA at a glance:

A key element of DORA is its focus on a thorough risk management framework. Financial entities must establish robust policies and procedures covering all facets of digital operational resilience. This includes identifying, assessing, and mitigating ICT risks, ensuring organisations can effectively anticipate and address potential threats.

DORA also enforces stringent requirements for ICT incident management, compelling financial entities to set up protocols for the timely detection, management, and reporting of incidents. Regular resilience testing is another fundamental aspect of DORA, requiring financial entities to conduct routine tests of their ICT systems, including threat-led penetration testing for critical systems. Furthermore, DORA promotes information sharing among financial entities, fostering a collaborative approach to cybersecurity and aiming to enhance the sector's collective resilience.

DORA in Malta

In Malta, the Malta Financial Services Authority (MFSA) is responsible for overseeing the implementation of DORA. The MFSA ensures that financial entities within its jurisdiction comply with the regulation's stringent requirements, thereby enhancing the resilience of Malta's financial sector.

The MFSA plays a crucial role in this ecosystem by facilitating compliance and ensuring that Malta's financial entities are well-equipped to meet DORA's demands. Through these efforts, the MFSA contributes to the broader goal of a resilient and secure European financial system.

With our extensive expertise in financial regulation, ICT law and ICT risk management, Mamo TCV Advocates provides legal advice and practical solutions tailored to the specific needs of the Maltese financial and ICT sectors.

New Contractual obligations for ICT providers servicing financial entities

DORA establishes specific obligations for contracts between financial entities and ICT third-party service providers regarding ICT services, impacting both existing and future contracts. Here are some high-level points to note in this regard:

- These obligations (including certain mandatory clauses that must be entered into) apply to all contractual agreements involving ICT services, with more stringent requirements for contracts supporting critical or important functions.
- All pertinent contracts must be documented in writing and must clearly define the rights and responsibilities of both the financial entity in question and the relevant ICT third-party service provider.
- The contractual obligations under DORA are closely aligned with the European Banking Authority guidelines on outsourcing.
- New requirements include provisions for service providers to assist during ICT-related incidents affecting the service, either at no additional cost or at a pre-determined cost.
- Providers are required to engage in the financial entities' ICT security awareness programmes and digital operational resilience training sessions.

Before entering into a contract, financial entities must conduct a thorough analysis of subcontracting arrangements, especially with ICT third-party service providers based in non-EU countries. For critical or important functions, financial entities need to evaluate how long or complex subcontracting chains might affect their ability to effectively monitor the contracted services and the supervisory capability of the competent authority.

Mamo TCV Advocates can assist with contract reviewing, drafting and/or amending, alignment with DORA requirements and other compliance matters in relation to ICT outsourcing affected by DORA.

What are DORA's 'five pillar' obligations?

1. Risk Management Framework

Obligation to establish ICT risk management policies and implement procedures for digital operational resilience.

2. ICT Incident Management

Obligation to develop incident response strategies and to ensure timely reporting and resolution of ICT incidents.

3. Third-Party Risk Management

Obligation to conduct due diligence on third-party ICT service providers and to monitor and manage risks associated with outsourcing.

4. Resilience Testing

Obligation to perform regular testing to ensure the resilience of ICT systems which includes threat-led penetration testing for critical systems.

5. Information Sharing

Obligation to participate in information-sharing arrangements to foster collaboration and enhance collective cybersecurity efforts.

How should one start?

1st Assess the Impact: Analyse how DORA affects your business based on your size, services, and operations by:

- Identifying gaps between existing ICT risk management and DORA's requirements.
- Reviewing existing contracts and policies.

2nd Develop an Implementation Plan: Create a detailed plan outlining the steps needed to meet DORA's standards. This includes:

- ***Strengthening ICT Risk Management*:** Establish environment to manage ICT risks.
- ***Incident Management*:** Implement procedures to handle all ICT-related incidents, with mandatory reporting for major ones.
- ***Testing and Third-Party Risk Management*:** Regularly test ICT systems and controls, and manage risks associated with third-party ICT providers.

3rd Consider Third Parties: Third-party providers performing an outsourced service are within scope of DORA and require further consideration.

Third-party considerations

Critical Third-Party Providers: These providers will need to have robust systems and procedures to manage ICT risks they pose to financial entities. Cloud service providers are likely to be designated as critical. Proactive measures include:

(i) Benchmarking existing systems against relevant guidelines; and
(ii) Reviewing contracts to ensure flexibility for compliance.

Third-Country Critical ICT Third-Party Providers: These providers may need to establish an EU subsidiary to continue serving EU financial entities. Early communication between providers and financial entities is crucial.

DORA & Corporate Governance

The management body of any relevant financial entity must actively align business strategy with ICT risk management and digital resilience, reflecting EU guidelines. The directors bear ultimate responsibility for ICT risks. Financial entities, excluding microenterprises, need a dedicated role or senior manager to oversee ICT third-party risk. Management must maintain sufficient knowledge and skills through regular training for all relevant staff and board members to understand and assess ICT risks, taking into consideration the MFSA's Corporate Governance Code.

DORA and ICT Providers

DORA directly applies to ICT providers offering services to financial entities, such as cloud platforms and data analytics services. DORA mandates that these ICT providers implement ICT risk management frameworks, robust incident reporting, and regular resilience testing. Regulatory responsibility is assigned directly by DORA to the ICT providers when they offer services outsourced by financial entities which would otherwise fall within DORA's scope.

DORA and Banking

Credit institutions must, not only ensure their own compliance with DORA, but also take steps to verify the DORA compliance of any ICT Service Provider that handles digital financial data. Specifically, Credit institutions' resilience testing will be strengthened with the new requirements under DORA as further testing will be required to be performed during a specific period of time. DORA requires that credit institutions report all operational or security payment-related incidents (previously reported under Directive (EU) 2015/2366) irrespective of the ICT nature of the incident. Credit institutions should have already performed (or are in the process of performing and concluding) a thorough gap analysis of the current requirements under sectoral legislation versus DORA requirements and in line with the applicable MFSA's supervisory expectations.

DORA and Insurance

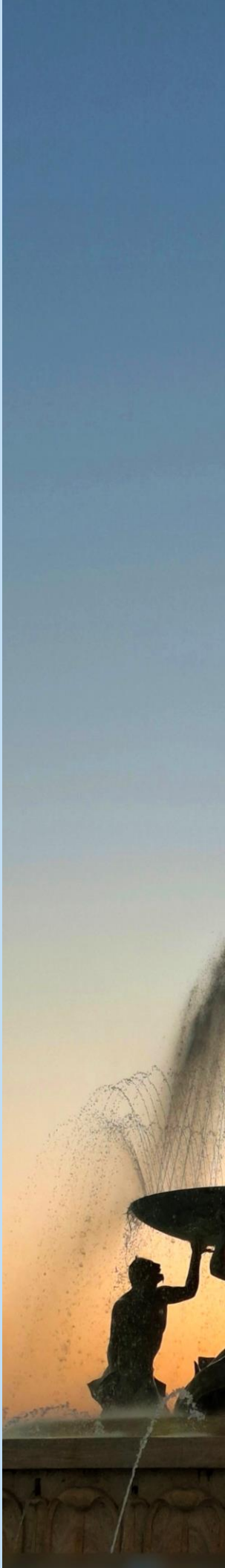
DORA will apply to (re)insurance undertakings within scope of the EU Solvency II Directive and larger (re)insurance intermediaries. (Re)insurance undertakings and intermediaries within scope of DORA already abide by several requirements which are similar to the requirements emanating from DORA. DORA works in conjunction with the existing regulatory framework for risk management of cyber and IT risks for the insurance industry. (Re)insurance undertakings and intermediaries within scope are expected to implement DORA and any Technical Standards, taking into account their size and overall risk profile, as well as the nature, scale and complexity of their services, activities and operations.

DORA and Investments

MIFID firms, Alternative Investment Fund Managers, UCITS Management Companies and other investment service providers within scope of DORA, already had several of DORA's requirements included in ESMA and MFSA requirements. Since most ICT operations of investment firms and AIFMs are outsourced, it is necessary to conduct a review of the contractual relationship with these third-party service providers because ultimately, the management body of the licence holder is responsible for DORA compliance.

DORA and Fintech

For fintech providers subject to DORA including PSPs and EMIs, it is essential to follow any Regulatory Technical Standards which are issued by ESMA and adopted by the MFSA. Although certain requirements were already stipulated under ESMA and MFSA guidelines for BCPs, fintech entities within the scope of DORA must conduct a gap analysis to ensure compliance with these new standards as a matter of urgency.



How can Mamo TCV Advocates help?

***Expert Legal Guidance*:** Our team of seasoned legal experts offers legal advice on DORA compliance, helping your business to:

- Determine DORA's applicability (and extent) to you;
- Develop and implement robust risk management frameworks;
- Prepare for and respond to ICT incidents effectively;
- Better understand and handle third-party risk management;
- Participate in information-sharing networks and other matters; and
- Comply with mandatory reporting obligations.

Contract Review and Drafting: We can also assist you in negotiating, vetting and, amending any contracts you may be entering into with relevant parties, to ensure that such contracts comply with DORA (including drafting mandatory clauses that must be entered into), as well as offer practical solutions in case of existing contracts.

Customised Legal Compliance Solutions: We understand that each business is unique. Our bespoke solutions are tailored to meet the specific needs of your organisation, ensuring you not only comply with DORA but also thrive in a secure digital environment. This includes assistance with drafting of necessary policies as well as advising on other related laws (including the EU GDPR) that may apply to you.

Training and Awareness: We offer training programmes to equip the board of directors and your staff with the knowledge and skills needed to maintain digital operational resilience, fostering a culture of compliance within your organisation.

This document does not purport to give legal, financial or tax advice. For more information, please contact our DORA advisors at: dora@mamotcv.com

www.doramalta.com

Check the link above for any updated versions of this overview

SCAN FOR MORE

MAMO TCV
ADVOCATES

Palazzo Pietro Stiges
103, Strait Street
Valletta VLT1436
Malta

T: (+356) 2540 3000

E: info@mamotcv.com
dora@mamotcv.com

W: www.mamotcv.com