Digital Operational Resilience Act (DORA)

Navigate DORA with confidence

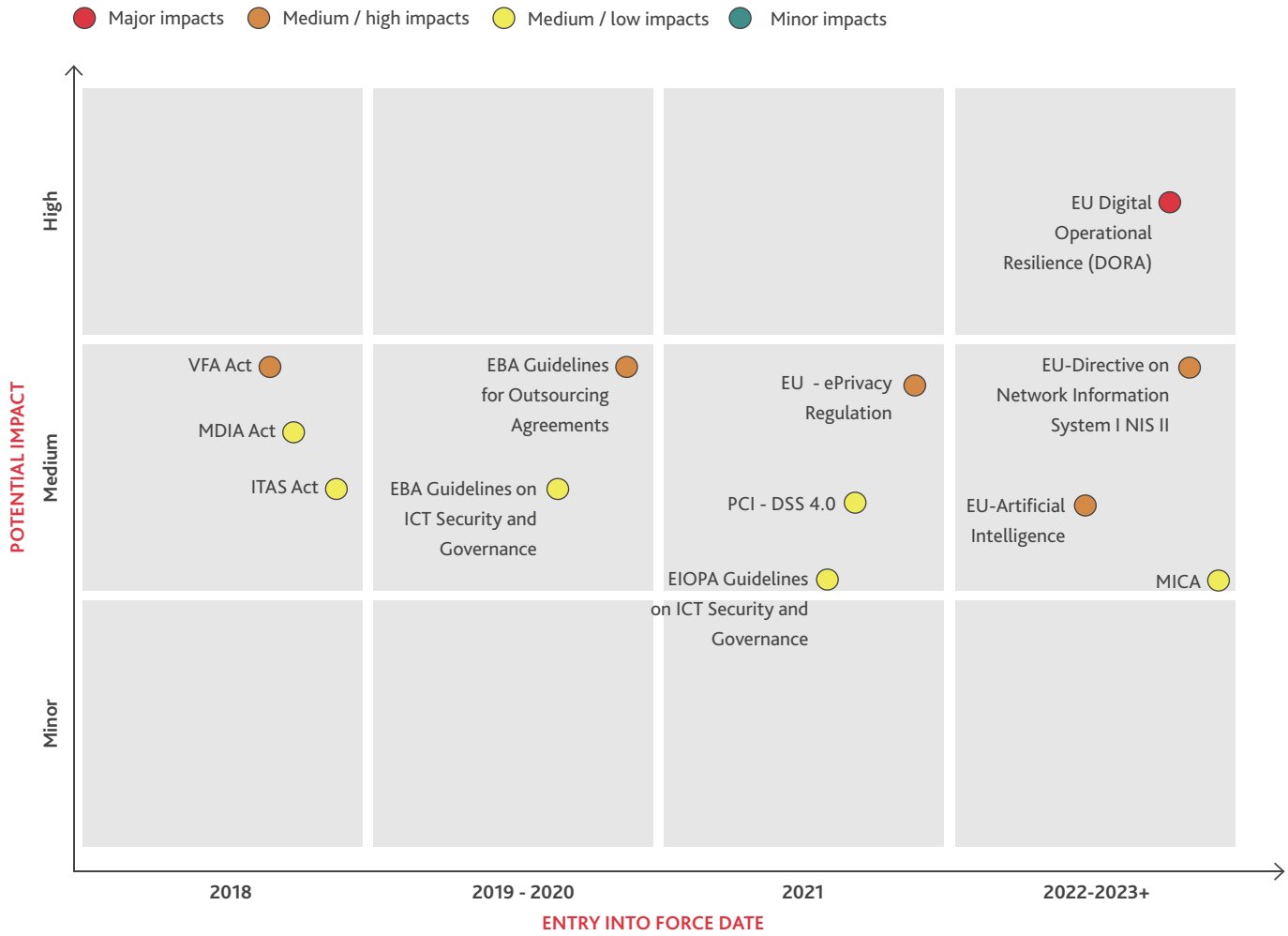
BDO MALTA

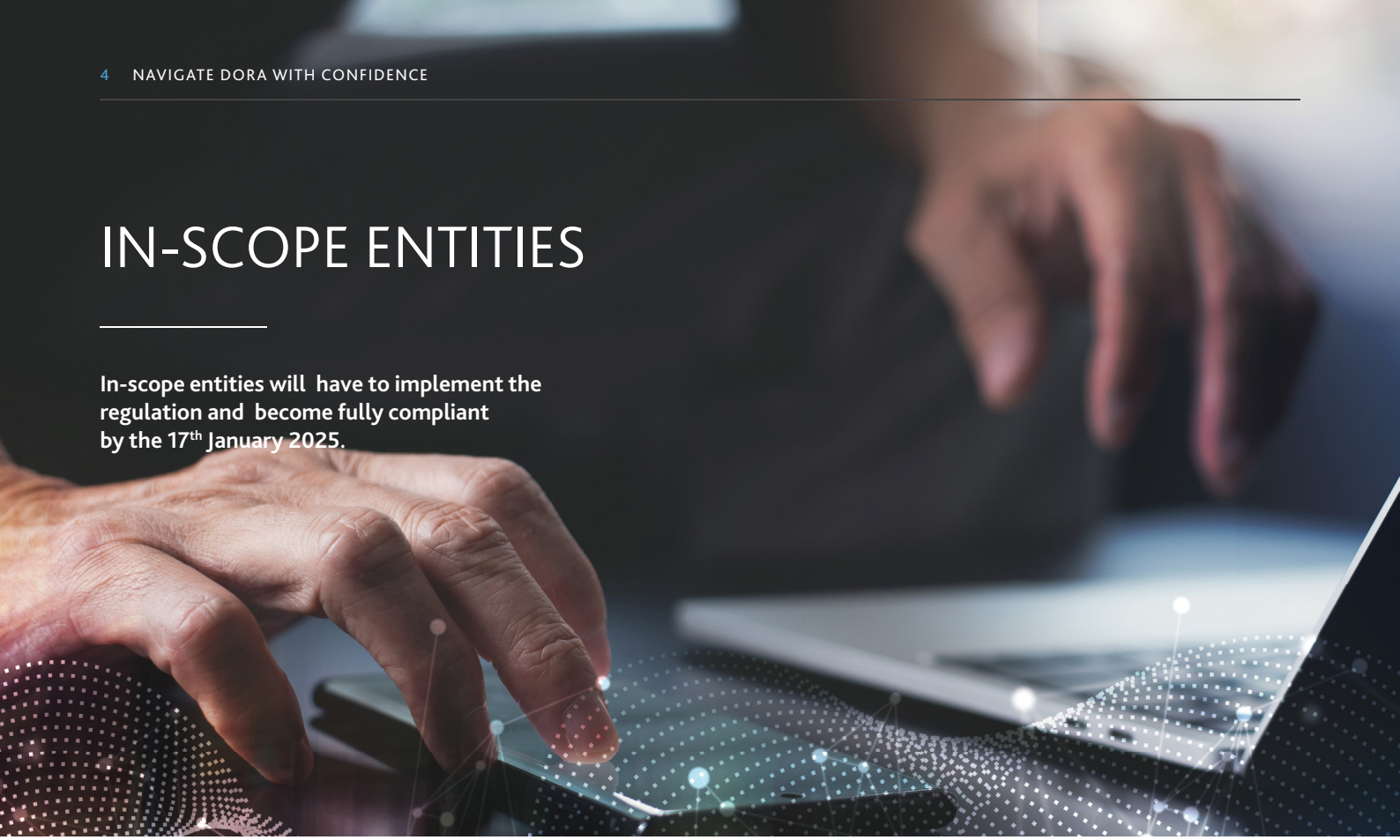
OVERVIEW OF DORA

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 European Union Council adopted the Digital Operational Resilience Act (DORA) regulation to ensure that digital infrastructure, including the systems and networks that underpin critical services in the financial sector, is secure and resilient against potential threats. While cyberattacks cannot be avoided, financial stability in Europe can still be achieved if organisations mitigate the impact of cyber threats on information and communication technologies (ICT).

Regulatory trends for in-scope entities





IN-SCOPE ENTITIES

In-scope entities will have to implement the regulation and become fully compliant by the 17th 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 17th 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.
- Commence scenario planning for a large-scale penetration test.
- Consolidate the Register of Information for all ICT third-party providers.

REQUIREMENTS

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

ICT risk management requirements
(Articles 5 to 16)

- Governance: accountable management body
- Risk mangement 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
- Anonymised EU-wide reports

Digital operational resilience testing
(Articles 24 to 27)

- Comprehensive testing programme, with focus on technical testing
- Large scale threat tests performed by independent testers every 3 years

Managing of ICT third-party risk
(Articles 28 to 44)

- Strategy, policy and standardised register of information
- Guidelines for pre-contract assessment, contract contents, termination, stressed exit

Information sharing arrangements
(Article 45)

- Encouraged to share threat information and intelligence

OUR SOLUTION

We provide expert guidance on DORA compliance, including risk assessments and gap analysis, incident management, business continuity plans, cybersecurity, continuous support and monitoring.

How can BDO help with DORA compliance?

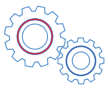
We can help you with DORA compliance by providing expert guidance on the regulation, conducting risk assessments and gap analysis, developing and implementing incident management and business continuity plans, and providing ongoing support and monitoring.

We can also assist with cyber implementation and assurance services to ensure that the infrastructure is secure and resilient against potential threats. This includes penetration testing, vulnerability assessments, and incident response planning.

Additionally, we can provide training and education to employees to help them understand and comply with DORA requirements.

A practical approach to achieve compliance with DORA:

1. Conduct regular risk assessments to identify potential threats and vulnerabilities.



2. Develop and implement incident management and business continuity plans to ensure that the organisation can respond effectively to a major incident.

3. Establish robust governance and oversight to ensure that DORA requirements are met and that the organisation's digital infrastructure is secure and resilient.

4. Regularly testing the incident management and business continuity plans.

FOR MORE INFORMATION:

BDO MALTA

Triq it-Torri
Msida
MSD 1824
Malta

Tel: +356 2342 4000

info@bdo.com.mt

www.bdo.com.mt