Digital Operational Resilience Act

Reducing Cyber Risk for the EU Financial Sector

Anton Yunussov
Director, Head of Cyber Advisory
Anton.Yunussov@Mazars.co.uk
+44 (0) 7583 042 769

James Ross
Cyber Security Consultant
James.Ross@Mazars.co.uk
+44 (0)7977 356 477

What is DORA? Why does it exist?

The Digital Operational Resilience Act is a new piece of EU legislation that applies to financial firms and their critical third parties, in order to ensure resilience against outages/cyber attacks.

Cyber Risk

The EU are concerned about the systemic cyber risk as a result of the current IT interconnectedness across their financial sector.

Standardising Rules

Some EU member states currently have more stringent IT resilience standards than others, DORA will help to standardise these.

To Remedy Inconsistencies

DORA fills in gaps and inconsistencies within some of the prior legal acts.

Improve Contracts

Currently, contracts between financial entities and their third parties often do not allow adequate oversight.

Threat Intelligence Sharing

DORA puts in place guidance for threat intelligence sharing.

How Does DORA Differ From UK Regulations?

Who does DORA Apply to?

DORA applies to all financial entities who are regulated by the EU, this includes the following, among others:

- Credit Institutions
- Payment Institutions
- Electronic Money Institutions
- Investment Firms
- Crypto-Asset service providers
- Central Securities Depositories
- Central Counterparties
- Data Reporting Service Providers
- Insurance and Reinsurance Undertakings and intermediaries
- Occupational retirement pensions companies

There are also a number of exceptions to DORA. Some notable examples are:

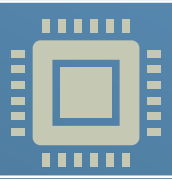
- Particular Micro-entities (If they also meet other criteria)
- Entities which individual EU states choose specifically to be exempt, and are already excluded from the scope of certain previous prudential supervision requirements

Please note: *the specific eligibility criteria for 'Critical third parties' under DORA is still being finalised by the regulator. There will be additional clarification on this by July 2024.*

Key Requirements of DORA

Governance and Risk Management

Introduces new governance structure and controls requirement for financial entities. Management bodies are required to be responsible for a firms risk management practices and provide continual oversight.
Financial firms will have to establish a new role dedicated to managing third parties.



Information sharing

DORA contains provisions which should facilitate the sharing, among Financial Entities, of cyber threat information and Intelligence.

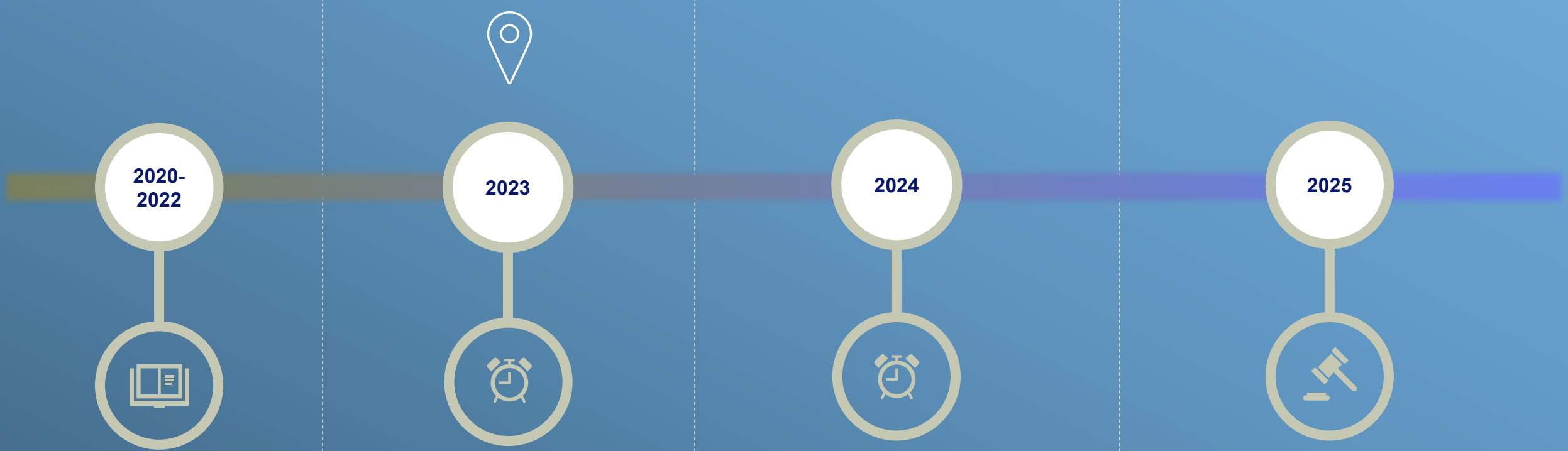
Testing

Introduces a requirement to implement a testing programme that demonstrates IT systems are operationally resilient. Under some circumstances, testing must be undertaken by an independent party for financial entities. Certain financial institutions must carry out advanced testing of their ICT tools, systems, and processes at least every three years using threat-led penetration tests.

Incident Reporting

Introduces new IT incident reporting requirements (including an initial reporting requirement of 24 hours to the relevant authorities).
Root cause analysis reports must be provided by financial entities one month at the latest, after a major IT incident occurs.

Implementation Timeline



Company A

A medium size insurance company operating in the UK and EU.

They currently have:

An IT risk management framework, but no IT resiliency strategy

Ad-hoc internal Security controls testing

Heavy reliance on third party IT service providers, including an outsourced managed SOC that resides outside of the EU.

Examples of DORA compliance difficulties:

Policy / Strategy changes

Hiring new staff and dedicating internal resources to DORA compliance

Implementation of a regular testing schedule, including Red Teaming

Changes to third party suppliers

Next Steps

Financial Entities
&
Critical IT Third Party Service Providers

- Identify relevant third party organisations
- Conduct current state benchmark assessments
- Carry out Third Party compliance assessments
- Develop short and medium term compliance plans
- Contract review and uplift

Questions