cybersecurity
associates

Digital Operational Resiliency Act (DORA)

A Quick Reference Guide to DORA

Executive Summary

The implementation of the DORA regulations mandates companies within the financial sector to adopt cyber resilience methods within their operations by 2025.

A significant increase in cyber incidents within the financial industry led to the European Commission developing a new regulatory framework for digital and cyber risk management.

The scope of the regulations is broad and includes organisations such as insurance companies and IT suppliers, including ICT in the supply chain.

In-scope organisations and their suppliers should begin preparatory work as soon as possible if they haven't already done so.

This Quick Reference Guide details what DORA is, why it is needed, who is enforcing it, how to prepare and how CSA can help.

What is DORA?

The Digital Operational Resilience Act is an EU piece of legislation that mandates financial services firms across Europe to adopt robust cyber security and ICT risk management practices.

Firms must be compliant by 17th January 2025 which is when the legislation is due to come into force.

Five Key Areas

- ICT Risk Management
- ICT Related Incident Reporting
- Digital Operational Resilience Testing
- ICT Third Party Risk Management
- Information & Intelligence Sharing

Non-compliance to the DORA requirements may lead to a fine of up to 2% of a business' annual global turnover.

What is DORA?

Scope

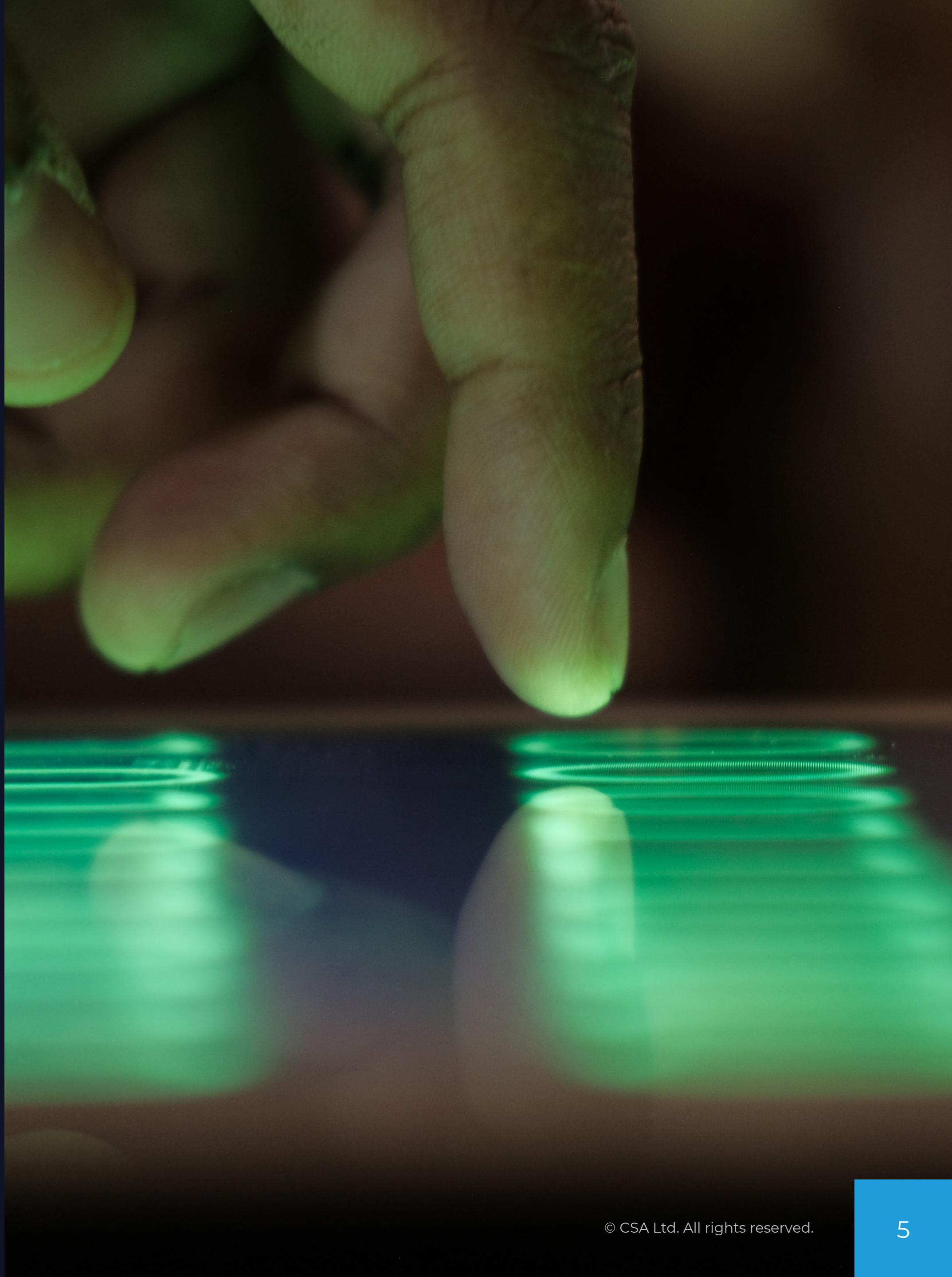
The legislation includes a prescriptive list of the organisations that are in scope.

- Credit Institutions
- Credit Securities Depositories
- Financial Investment Firms
- Insurance and reinsurance undertakings
- Data reporting service providers
- Trading Institutions
- Account information service providers
- Crypto-asset service providers

Please note: ICT Suppliers to these organisations are also in scope and must meet the standards set by these regulations.

Why do we need DORA?

- The increase is cyber-related incidents, particularly within the financial sector, has led the European Commission to believe that a new and more robust solution is required.
- The DORA regulations introduce a Union-wide Oversight Framework on digital risk management and resilience, as well as the management of critical ICT third-party providers.
- Within the 2024 Global Financial Stability Report, the International Monetary Fund estimated that the size of these extreme losses due to cyber incidents has more than quadrupled since 2017 to $2.5 billion.
- The financial sector is uniquely exposed to cyber risk due to the large amounts of sensitive data and high-risk transactions that are handled.



Who enforces the regulations?

The European Supervisory Authorities (ESAs) are institutions that are in charge of publishing Regulatory Technical Standards (RTS). These are technical guidelines on how the DORA requirements should be implemented.

They also act as a point of contact for major incident reporting.

There are currently three ESAs, who are:

- The European Banking Authority (EBA): Homepage | European Banking Authority (europa.eu)
- The European Insurance and Occupational Pensions Authority (EIOPA): About - European Union (europa.eu)
- The European Securities and Markets Authority (ESMA): | European Securities and Markets Authority (europa.eu)

Note: As of July 2024, the majority of the RTS documents are still being drafted.
Be sure to keep up to date with any changes over the coming months.

How to prepare

Failure to prepare is preparing to fail!

Entities have a deadline of January 2025 to comply, however, this doesn't mean that you should wait until then to do anything. Here are some examples of things you can do for now:

Gap Analysis

Review the requirements of the legislation and identify where the compliance gaps are. This will help you to plan your next steps. CSA are highly experienced with this and can support you through the process.

Roles and Responsibilities

Who is in charge of what? Make sure that all responsibilities relating to DORA are clearly defined and understood.

Training and Awareness

It is likely that some people may need to upskill or complete refresher courses. Everyone should have some sort of awareness of DORA and its implications.

Know Your Supply Chain

This is possibly one of the most important things you can do for now. You must be able to determine who your key IT suppliers are. A lot of focus will be on them during your DORA implementation project.

How we can help

Luckily, we are here to help you with all of this. The packages that we offer are customer-made and built to meet your organisation's requirements.

Here are some examples of what we can do for you:

Get in touch to find out more.

www.csa.limited

☎ +44 (0) 1452 886982

✉ hello@csa.limited

Gap Analysis

A Consultant can work with you to complete a gap analysis against the DORA requirements and produce a report with a CMMI maturity score.

Roadmap

We can use these results to produce custom built, costed, prioritized roadmap outlining key activities and timelines.

Documentation

Don't worry if you are missing a few policy documents. We are here to plug in the gaps and build documentation that is bespoke to your company, achievable and ensures full compliance against both DORA and other in-scope regulations.

Support & Maintenance

We provide Security Operations Centre, Penetration Testing, and Incident Response services through our skilled team. Additionally, our Consultancy Team is ready to assist with annual compliance posture reviews and improvement efforts.

Your Trusted Cyber Security
Certified Provider

CSA with SCCS continues to grow its capabilities and security certifications to ensure it remains a world-class Cyber Security Provider. CSA with SCCS currently holds the following certifications:

CSP

ISO 9001
ISOQAR
REGISTERED
alcumus.com
UKAS
MANAGEMENT
SYSTEMS
0026

PCI Security Standards Council
Qualified Security Assessor (QSA)
Certification

ISO 27001
ISOQAR
REGISTERED
alcumus.com
UKAS
MANAGEMENT
SYSTEMS
0026

CREST
VA
PEN TEST
STAR
Intelligence-led PT

Assured Service Provider
in association with
National Cyber Security Centre
CHECK Penetration Testing

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection

CYBER ESSENTIALS
CERTIFIED

CYBER ESSENTIALS
CERTIFIED PLUS

CCoE
Cyber Centre of Excellence
for Local Public Services

cybersecurity
associates

SureCloud.
Cyber Services
a cybersecurity company
associates