Brochure

Digital Operational Resilience Act

Assess and implement what you need.
Comply with EU regulation

WITH secure

Why financial sector resilience matters

The purpose of the Digital Operational Resilience Act (DORA) is to increase the resilience of the financial sector to information and communication technology (ICT) threats.

Financial services significantly contribute to the EU economy. The banking sector alone employs over 2 million people. One in every 100 jobs in the EU is in banking[1].

Over the last decade, cyber threats have become more widespread, frequent and damaging. Despite spending $23 billion worldwide on cyber security, in 2022, cybercrime costs are predicted to hit $10.5 trillion annually by 2025[2], which represents the greatest transfer of wealth in history.

Regulators are concerned that the traditional way that financial institutions managed operational risk, by allocating capital, is no longer adequate.

1. https://www.ebf.eu/factsandfigures/
2. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

EU response to financial sector threats

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system. The Digital Operational Resilience Act (DORA) is an EU regulation, a binding legislative act and must be applied in its entirety across the EU.

DORA consolidates and upgrades the ICT risk requirements addressed so far separately in the different Regulations and Directives. It obliges financial institutions to establish and maintain the capabilities necessary to be resilient to ICT-related incidents.

DORA requirements in 250 words

ICT risk management

- Financial entities must have a sound, comprehensive, well-documented ICT risk management framework in place as part of their overall risk management system, to ensure a high level of digital operational resilience.

ICT-related incident management and reporting

- Financial entities must implement an ICT-related incident management process to detect, classify, manage and notify ICT-related incidents to the relevant supervisory authority and the entity's stakeholders.
- Supervisory authorities must be notified of ICT-related incidents within the same working day unless the incident is detected within 2 hours of the end of the working day[3].

Digital operational resilience testing

- Financial entities must maintain a crisis communications plan that is regularly tested. Workarounds must be maintained in the event that normal channels of communication are compromised.
- All critical ICT systems and applications must be tested at least yearly
- Business impact analyses based on “severe business disruption” scenarios must be carried out.

ICT third-party risk

- DORA defines minimum requirements that third party ICT service providers must meet, with additional rules for outsourcing of critical functions.
- DORA prohibits concentration of risk and states that organizations shouldn’t rely on a single service provider for business-critical processes.
- Critical suppliers must have a functioning EU subsidiary by 17 January 2025 if they are to continue to supply ICT services to financial entities.

Information sharing

- Financial entities can share amongst themselves information and intelligence about cyber threats, including indicators of compromise, tactics, techniques, procedures, cyber security alerts and configuration tools.

3. https://www.allenovery.com/global/-/media/allenovery/2_documents/news_and_insights/publications/2021/01/webinar_new_eu_legislative_proposals_on_digital_operational_resilience_dora.pdf?

Compliance

DORA came into force on 16 January 2023. Regulatory technical standards will be developed over the next 12 months.

Organisations need to have a logical, defensible security strategy that includes an explicit position on resilience.

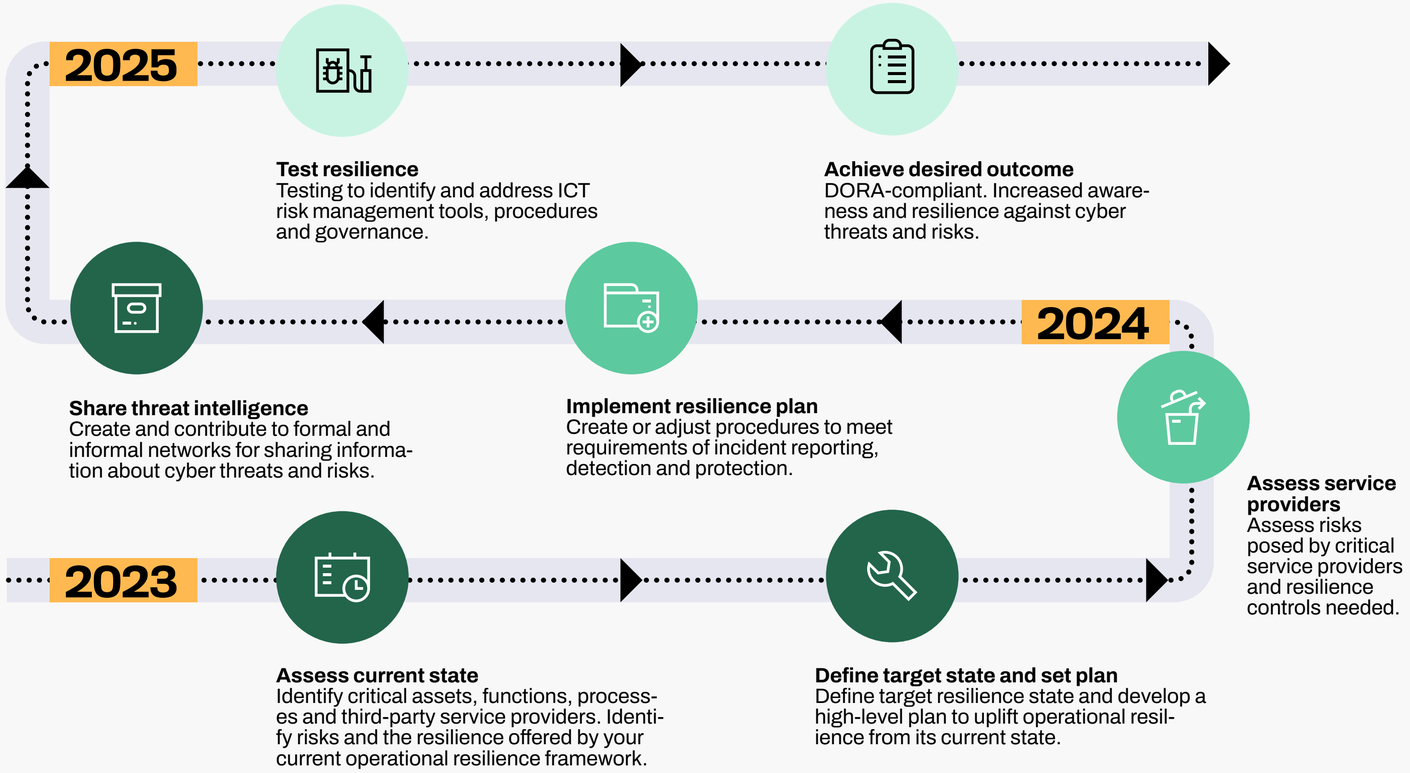
Although no one knows yet how supervisory control will be implemented, organisations should consider taking preparatory steps to achieve the minimum resilience standards prescribed by DORA.

What organisations need to do

The largest financial entities will have the capability and resources to make necessary adjustments to comply with DORA. The same cannot be said for the rest of the financial sector. They will have a larger gap to close, with fewer resources to do it.

The steps necessary to achieve the minimum resilience standards prescribed by DORA are depicted below.

Financial entities that do not have in-house resources to take these steps should look to an experienced security partner to support them.



We conduct threat-based testing and we help clients to implement ISMS systems and risk management frameworks to remain resilient. The consulting and threat-based assurance services we use are shown below.

Systemic risks to consider

Internet access: 90% of international internet traffic flows through 436 cables that in a geo-political dispute can easily be severed.

Concentration risk: 60% of workloads are performed by 3 CSPs creating commercial and technical risk.

IT complexity: the attack surface of organisations is dynamic and growing, and they have never had less control.

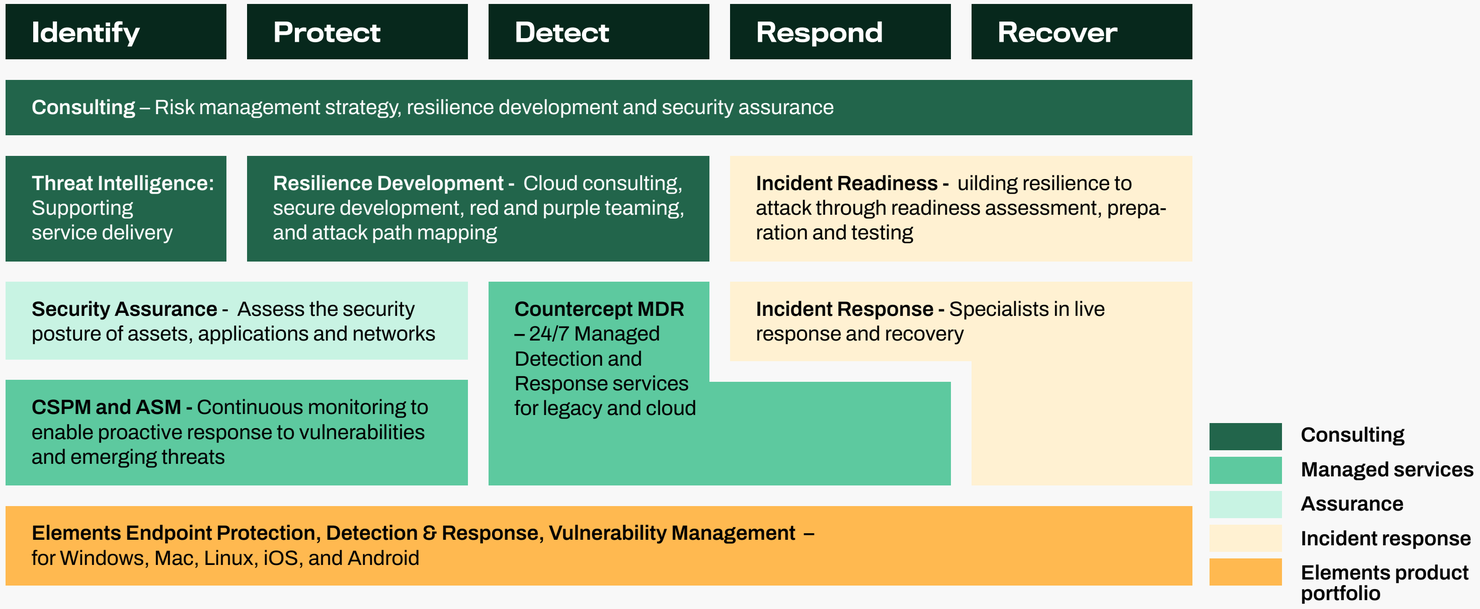
How we can help:

WithSecure™ is a global provider of cyber security services. We are listed on the Nasdaq Helsinki, and we have offices in nearly 30 countries.

We provide consulting and managed services directly to over 700 enterprises. Our clients are members of the FTSE 100 and the Dow Jones. They include 20 of the world's largest banks, manufacturing and tech giants. We excel at solving hard, complex, security problems. Our red team is one of the most formidable offensive units in the world. Our incident responders are government-certified to combat threats from advanced state actors.

Consulting services relevant to helping you to improve your resilience to ICT-related threats and to comply with DORA, are depicted here.

Feel free to call us for an initial free-of-charge consultation.



The 5 most insightful DORA articles

Typing 'Digital Operational Resilience Act' into the search bar of your browser, will return tens of millions of search results. There is no shortage of material to read. To save the sanity of those seeking further information, here are the best reads:

If you want to understand what DORA means to your business, law firms Clifford Chance and Allen and Overy provide the best balance of brevity and detail:

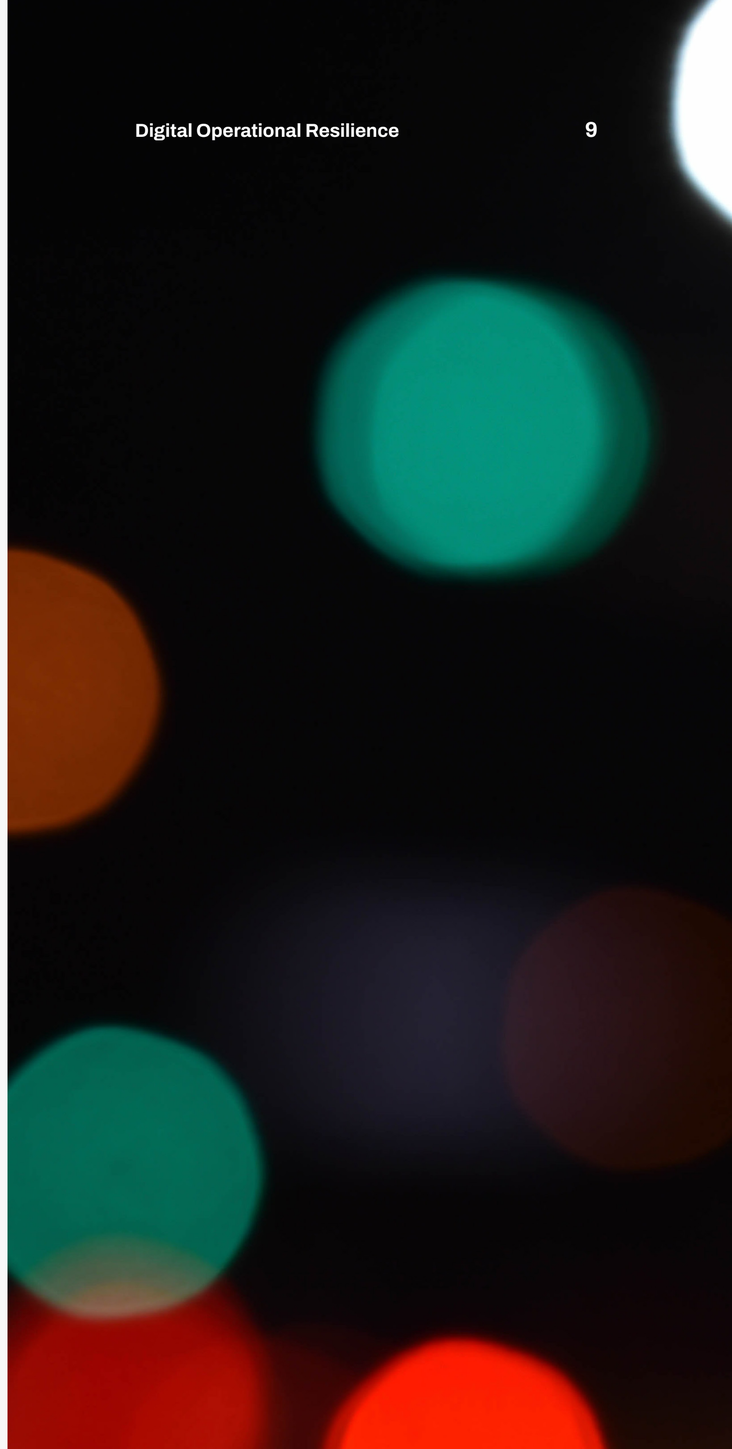
- https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/dora-what-the-new-european-framework-for-digital-operational-resilience-means-for-your-business.pdf
- https://www.allenovery.com/global/-/media/allenovery/2_documents/news_and_insights/publications/2021/01/webinar_new_eu_legislative_proposals_on_digital_operational_resilience_dora.pdf

If you want to understand what systemic risks concern regulators, the Carnegie Endowment Organisation provides an illuminating overview

- https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531

FTI Consulting has produced several insightful reflections on the practical implications for DORA compliance:

- https://www.fticonsulting.com/insights/fti-journal/good-news-not-good-news-reporting-requirements-dora
- https://www.fticonsulting.com/insights/fti-journal/what-you-may-not-know-about-dora-but-should
- https://www.fticonsulting.com/insights/fti-journal/managing-risk-understanding-your-firms-obligations-under-dora



Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

W / T H™
secure