RAPID7

SOLUTION BRIEF

SUPPORTING DORA COMPLIANCE WITH RAPID7

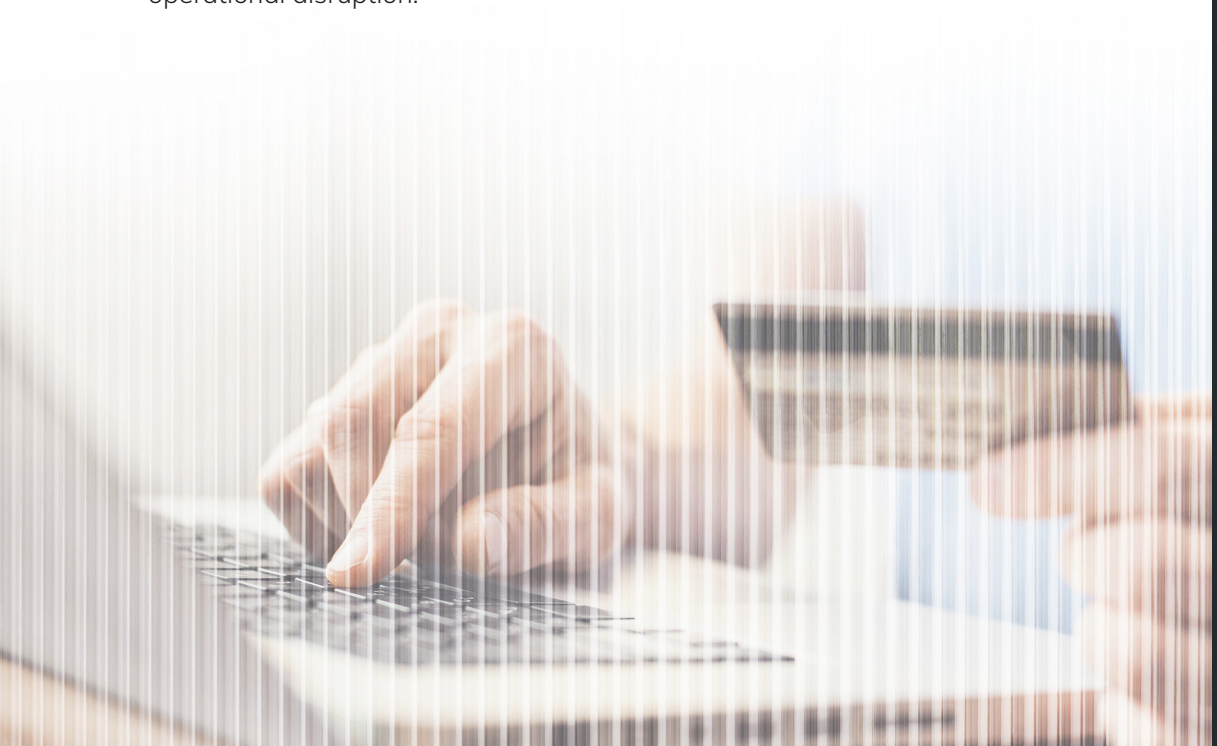
Over the past two decades the financial sector has undergone profound change as a result of digital transformation.

From providing primarily bricks and mortar based services we have now moved to mostly online banking and financial services. However as financial services have become more efficient and accessible this has added additional cyber risks that expose a highly interconnected industry to cyber attacks that can often not be contained to a single financial institution or country.

In short? It's big, messy, and complicated.

This heightened exposure to cyber attacks alongside the critical and interdependent nature of the financial services industry is the background to the Digital Operational Resilience Act (DORA).

The DORA EU regulation entered into force on 16 January 2023 and will apply as of 17 January 2025. Where previously financial services risk was focused on ensuring that firms had enough capital to cover operational risks, DORA forces financial services firms to focus on their information and communication technology (ICT) operational risks. It aims to ensure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.



Who does DORA apply to?

The DORA regulation will exist alongside the NIS2 Directive (Directive (EU) 2022/2555), a legislative act also aimed at achieving a high common level of cybersecurity across the European Union. NIS2 enforcement began on 18 October 2024. While DORA focuses specifically on enforcing cyber resilience across financial services companies and their suppliers, NIS2 applies to a broader range of organisations across the EU that are deemed critical to the EU economy for example the energy, transport and health sectors.

Financial Institutions

DORA applies to all financial institutions in the EU. This includes traditional financial entities, such as banks, investment firms and credit institutions, and non-traditional entities, including crypto-asset service providers and crowdfunding platforms.

Third Party Service Providers

DORA also applies to third-party service providers that supply financial firms in the EU with ICT systems and services. This includes cloud service providers that provide critical information services, such as credit rating services and data analytics providers.

Enforcement of DORA will be carried out by “competent authorities” in each EU member state. ICT providers deemed critical, based on information provided by the individual competent authorities, will be directly supervised by overseers from the European Supervisory Authorities (ESAs). Both the competent authorities, ESA lead overseers can request remediation and penalise noncompliant ICT providers. DORA allows lead overseers to levy fines on ICT providers amounting to 1% of the provider’s average daily worldwide turnover in the previous business year. Providers can be fined every day for up to six months until they achieve compliance.

The DORA Pillars

The DORA regulation is built on five main pillars;

1. **ICT risk management**
   Organisations must establish a comprehensive framework that not only identifies and documents critical ICT functions but also continuously monitors and mitigates risks.

2. **ICT-related incident management, classification and reporting**
   DORA mandates that organisations have a robust incident reporting process. Entities must have the ability to quickly detect, assess, and respond to incidents, minimising their impact on operations and financial stability

3. **Digital operational resilience testing**
   Financial organisations must conduct regular, comprehensive tests of their ICT systems to ensure they can withstand and recover from disruptions

4. **Managing ICT third-party risk**
   Financial entities must develop and maintain a robust ICT Third-Party Risk Management Policy and perform risk assessments (financial, security and technical) on potential 3rd party suppliers prior to any formal agreements.

5. **Information Sharing**
   Entities should participate in trusted communities where they can share and receive information about cyber threats and incidents and report significant ICT-related incidents to their National Competent Authorities (NCAs).

How Rapid7 Supports DORA Compliance

As per EU NIS2 compliance, it is likely that multiple cybersecurity and other solutions will be required to support an organisation's overall compliance with the DORA regulation. At Rapid7, our solutions can be used to help support the requirements contained in all five pillars of the DORA regulation.

The table illustrates how the Rapid7 Command Platform can support your DORA compliance.

DORA Pillar	Rapid7 Solution
ICT Risk Management	• Surface Command • Exposure Command • Managed Threat Complete
ICT-Related Incident Management	• Managed Threat Complete
Digital Operational Resilience Testing	• Surface Command • Exposure Command • Managed Threat Complete • Vector Command
Managing ICT Third-Party Risk	• Partner
Information Sharing	• Surface Command • Exposure Command • Managed Threat Complete

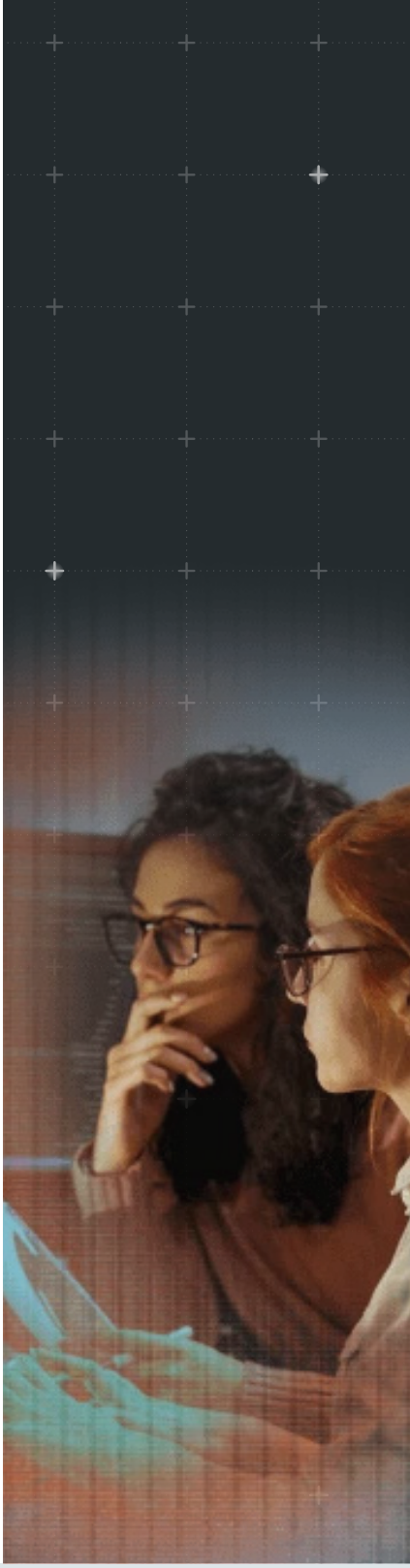
Next Steps

DORA compliance within the EU financial services industry and for suppliers to EU based financial services organisations is no longer discretionary but mandatory, with significant financial penalties for non-compliance. As an organisation, Rapid7 continues to monitor and contribute to the development of emerging industry and regulatory cybersecurity standards and requirements. Within our portfolio of products we offer and continue to extend our compliance solutions that either map to or partially support standards and emerging regulatory requirements. Leveraging our suite of compliance packs and policy tools for both cloud and on-prem scenarios can enable you to tailor your compliance requirements and achieve optimal visibility into your assets, speeding up both regulatory compliance and ROI.

If you would like to find out more on how Rapid7 can support your DORA compliance please visit: https://www.rapid7.com/products/command/exposure-management/ or contact your local Rapid7 representative or partner.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.



RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight