



DORA Compliance

SERVICE BENEFITS

- ✓ Achieve a better understanding of breaches cost-effectively without any disruption to systems and processes.
- ✓ Demonstrate the potential impact of a targeted cyber attack.
- ✓ Determine any inefficiencies or weaknesses within your response capabilities.
- ✓ Improve critical decision-making through improved communication between internal departments.
- ✓ Determine the roles of all relevant personnel in case of a cyber attack.

BOOST YOUR DIGITAL OPERATIONAL RESILIENCE

Compliance with the Digital Operational Resilience Act (DORA) will be mandatory from 25 January 2025. It's designed to ensure that financial organisations can withstand, respond to and recover from all types of ICT related disruptions and threats. DORA is a comprehensive regulatory framework aimed at enhancing the resilience of the financial sector against cyber threats, ICT risks and operational disruptions.

As the deadline approaches, financial organisations must prioritise cybersecurity measures to meet the stringent requirements. Razorthorn, as an established cybersecurity consultancy, can help your organisation navigate the complexities of compliance.

The framework introduces a set of robust requirements encompassing governance, risk management, incident reporting, digital operational resilience testing and third party risk management. Financial institutions must establish comprehensive policies, procedures, and controls to effectively manage and mitigate ICT risks, safeguard critical functions and protect sensitive data.

DORA COMPLIANCE: THE RAZORTHORN APPROACH

Tailored Solutions

At Razorthorn, we understand the unique challenges financial organisations face when it comes to cybersecurity and regulatory compliance. Our dedicated team of consultants specialises in providing tailored solutions to address the specific requirements outlined in the DORA legislation. By partnering with us, you gain access to our extensive knowledge and experience in the field. This ensures your organisation remains ahead of the curve in this rapidly evolving landscape.

Gap analysis

We will review your current status by performing a DORA gap analysis review. This will highlight the areas that need to be addressed to meet with the requirements of the DORA Act. A report will be provided to you detailing what testing has been carried out and why, along with a comprehensive list of activities to be completed to ensure compliance.

Consulting & Security Tools

Preparing for DORA implementation involves overcoming key challenges that financial organisations commonly encounter. Our cybersecurity service equips you with the necessary tools, strategies and expertise to tackle these challenges head on. Whether it's developing robust incident response plans, enhancing third-party risk management, or bolstering your organisation's overall security posture, we provide comprehensive guidance and advice every step of the way.

Creating a Compliance Roadmap

Understanding the distinctions between DORA and existing ICT guidelines is crucial to ensure compliance. Our consultants possess in depth knowledge of both DORA and existing frameworks. This enables us to bridge any gaps and align your cybersecurity practices accordingly. By mapping your existing security measures with DORA requirements, we help you optimise your resources and minimise disruptions during the compliance journey.

