The Disruption House

DORA Readiness Report

Product Overview

About the TDH DORA Assessment Journey

The Digital Operational Resilience Act (DORA) aims to enhance cybersecurity and operational resilience by establishing best practice for financial companies and their value chain. Recognising that ICT incidents and a lack of operational resilience have the possibility to jeopardise the entire financial system, DORA applies to more than 22,000 financial entities and ICT service providers operating within the EU, as well as the ICT infrastructure supporting them from outside the EU.

Developed by experts in operational resilience and regulatory compliance, the TDH DORA Assessment questions and answers are aligned to each article of the DORA legislation. TDH DORA Readiness Report marks your capabilities across the five pillars of DORA, highlights red flags that require attention and recommends next steps to ensure compliance. If you have no red flags, look to improve your practices related to the topics with lowest scores.

The Pillars of the TDH DORA Readiness Report

Governance

Information Sharing

Good governance requires policies and procedures that promote transparency, accountability and inclusivity, and ensure the rule of law is followed. Board oversight, stakeholder engagement and regular audits ensure operational integrity and regulatory alignment in a continuously changing environment.

Key topics include access control, human resources policy, identity management and risk management reporting.

Risk

ICT Risk Management

ICT risk management involves identifying, assessing, and mitigating risks to IT systems. This includes establishing policies and procedures, managing vulnerabilities through patching, overseeing project and change management and ensuring robust safeguards against potential threats.

Key topics include ICT asset management, change and project management, and testing ICT business continuity plans.

Operations

Incident Reporting

To minimise operational risk, optimise revenue streams, ensure control and safety and protect the integrity and reputation of the organisation; best practices, roles and responsibilities must be designed and implemented.

Key topics include performance management, response and recovery plans, acquisition and development, logging and policies and procedures.

Security

Digital Operational Resilience Testing

Security measures including firewalls, encryption and access controls are key to managing cybersecurity risks. Third parties to DORA governed entities will need to demonstrate tight security controls across many areas they may never have had to consider in that past.

Key topics include anomalous activities detection, cryptographic controls, security of data and systems, networks and the physical environment.

Third Party Risk

Management of Third-Party Risk

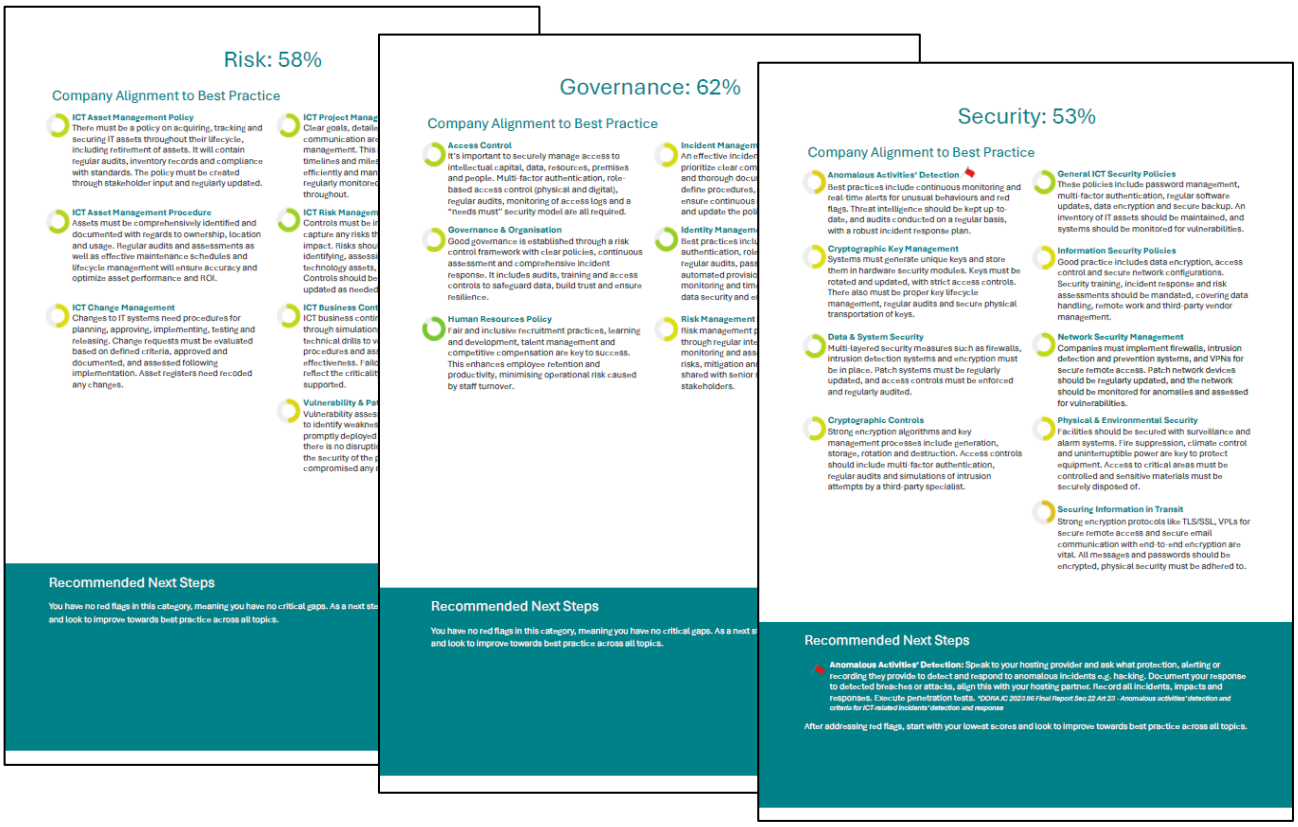
Effective management of third-party risk demands robust policies and procedures that enhance transparency, accountability, and due diligence. By rigorously evaluating and monitoring third-party relationships, organizations can mitigate risks.

Key topics include contractual monitoring, termination of contracts, subcontractor selection and risk monitoring and information sharing.

TDH Readiness Report Preview

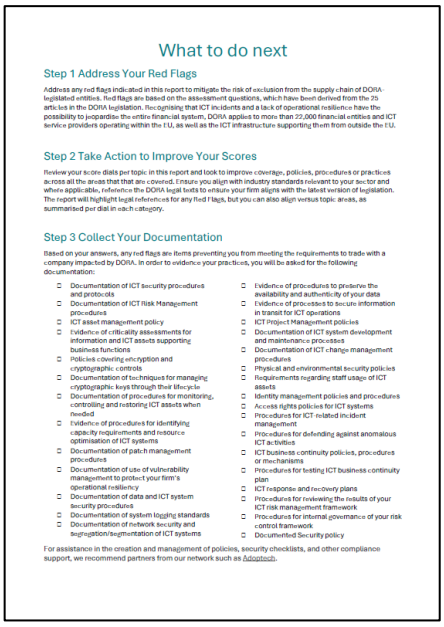
Category Reviews

Reports share an overall alignment score as well as a score in each topic area, directly mapped to DORA regulation. They also identify red flags, which are critical gaps that need to be addressed.



Next Steps

You also receive detailed guidance on what to do next, including all relevant documentation that will be required to evidence your alignment to relevant financial institutions.



DORA-Assessed Badge

Your DORA-Assessed Badge communicates to your stakeholders that you have taken steps to understand the legislation and are ready to demonstrate your capabilities.

For more information, please contact

Info@thedisruptionhouse.com