



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.

Risk: 58%

Company Alignment to Best Practice

- ICT Asset Management Policy**
There must be a policy on acquiring, tracking and securing IT assets throughout their lifecycle, including retirement of assets. It will contain regular audits, inventory records and compliance with standards. The policy must be created through stakeholder input and regularly updated.
- ICT Asset Management Procedure**
Assets must be comprehensively identified and documented with regards to ownership, location and usage. Regular audits and assessments as well as effective maintenance schedules and lifecycle management will ensure accuracy and optimize asset performance and TCO.
- ICT Change Management**
Changes to IT systems need procedures for planning, approving, implementing, testing and releasing. Change requests must be evaluated based on defined criteria, approved and documented, and assessed following implementation. Asset registers need recorded any changes.
- ICT Project Management**
Clear goals, detailed communication and management. This includes timelines and milestones and must be regularly monitored throughout.
- ICT Risk Management**
Controls must be in place to identify and manage risks. Controls should be updated as needed.
- ICT Business Continuity**
ICT business continuity plans should be tested through simulation and drills to verify effectiveness. Plans should be updated as needed.
- Vulnerability and Penetration Testing**
Vulnerability assessments should be promptly deployed. There is no disruption to the security of the system if any compromise occurs.

Recommended Next Steps

You have no red flags in this category, meaning you have no critical gaps. As a next step and look to improve towards best practice across all topics.

Governance: 62%

Company Alignment to Best Practice

- Access Control**
It's important to securely manage access to intellectual capital, data, resources, premises and people. Multi-factor authentication, role-based access control (physical and digital), regular audits, monitoring of access logs and a "needs must" security model are all required.
- Governance & Organisation**
Good governance is established through a risk control framework with clear policies, continuous assessment and comprehensive incident response. It includes audits, training and access controls to safeguard data, build trust and ensure resilience.
- Human Resources Policy**
Fair and inclusive recruitment practices, learning and development, talent management and competitive compensation are key to success. This enhances employee retention and productivity, minimising operational risk caused by staff turnover.
- Incident Management**
An effective incident response plan should be clear and through documented procedures, ensure continuous and update the plan.
- Identity Management**
Best practices include authentication, role-based access control, regular audits, pass automated provisioning and timely data security and access control.
- Risk Management**
Risk management should be integrated into monitoring and assessment, mitigation and reporting with senior stakeholders.

Recommended Next Steps

You have no red flags in this category, meaning you have no critical gaps. As a next step and look to improve towards best practice across all topics.

Security: 53%

Company Alignment to Best Practice

- Anomalous Activities' Detection**
Best practices include continuous monitoring and real-time alerts for unusual behaviours and red flags. Threat intelligence should be kept up to date, and audits conducted on a regular basis, with a robust incident response plan.
- Cryptographic Key Management**
Systems must generate unique keys and store them in hardware security modules. Keys must be rotated and updated, with strict access controls. There also must be proper key lifecycle management, regular audits and secure physical transportation of keys.
- Data & System Security**
Multi-layered security measures such as firewalls, intrusion detection systems and encryption must be in place. Patch systems must be regularly updated, and access controls must be enforced and regularly audited.
- Cryptographic Controls**
Strong encryption algorithms and key management processes include generation, storage, rotation and destruction. Access controls should include multi-factor authentication, regular audits and simulations of intrusion attempts by a third party specialist.
- General ICT Security Policies**
These policies include password management, multi-factor authentication, regular software updates, data encryption and secure backup. An inventory of IT assets should be maintained, and systems should be monitored for vulnerabilities.
- Information Security Policies**
Good practice includes data encryption, access control and secure network configurations. Security training, incident response and risk assessments should be mandated, covering data handling, remote work and third party vendor management.
- Network Security Management**
Companies must implement firewalls, intrusion detection and prevention systems, and VPNs for secure remote access. Patch network devices should be regularly updated, and the network should be monitored for anomalies and assessed for vulnerabilities.
- Physical & Environmental Security**
Facilities should be secured with surveillance and alarm systems. Fire suppression, climate control and uninterruptible power are key to protect equipment. Access to critical areas must be controlled and sensitive materials must be securely disposed of.
- Securing Information In Transit**
Strong encryption protocols like TLS/SSL, VPNs for secure remote access and secure email communication with end-to-end encryption are vital. All messages and passwords should be encrypted, physical security must be adhered to.

Recommended Next Steps

Anomalous Activities' Detection: Speak to your hosting provider and ask what protection, alerting or recording they provide to detect and respond to anomalous incidents e.g. hacking. Document your response to detected breaches or attacks, align this with your hosting partner. Record all incidents, impacts and responses. Execute penetration tests. [Download our Red Flag Report Sec 27 Art 33 - Anomalous activities' Detection and criteria for ICT-related incidents' detection and response](#)

After addressing red flags, start with your lowest scores and look to improve towards best practice across all topics.

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.

What to do next

Step 1 Address Your Red Flags

Address any red flags indicated in this report to mitigate the risk of exclusion from the supply chain of DORA-licensed entities. Red flags are based on the assessment questions, which have been derived from the 29 articles in the DORA legislation. 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.

Step 2 Take Action to Improve Your Scores

Review your score data per topic in this report and look to improve coverage, policies, procedures or practices across all the areas that are covered. Ensure you align with industry standards relevant to your sector and where applicable, reference the DORA legal text to ensure your firm aligns with the latest version of legislation. The report will highlight legal references for any red flags, but you can also align versus topic areas, as summarised per table in each category.

Step 3 Collect Your Documentation

Based on your answers, any red flags are items preventing you from meeting the requirements to trade with a company assessed by DORA. In order to evidence your practices, you will be asked for the following documentation:

<ul style="list-style-type: none"> Documentation of ICT security procedures and practices Documentation of ICT risk management procedures ICT asset management policy Evidence of criticality assessments for information and ICT assets supporting business functions Policy covering encryption and cryptographic controls Documentation of techniques for managing cryptographic keys through their lifecycle Documentation of procedures for monitoring, controlling and restoring ICT assets when needed Evidence of procedures for identifying capability requirements and resource optimisation of ICT systems Documentation of patch management procedures Documentation of use of vulnerability management to protect your firm's operational resilience Documentation of data and ICT system security procedures Documentation of system logging standards Documentation of network security and log-upon authentication of ICT systems 	<ul style="list-style-type: none"> Evidence of procedures to preserve the availability and authenticity of your data Evidence of procedures to secure information in transit ICT Project Management policies Documentation of ICT system development and maintenance practices Documentation of ICT change management procedures Physical and environmental security policies Requirements regarding staff usage of ICT devices Identity management policies and procedures Access rights policies for ICT systems Procedures for ICT-related incident management Procedures for defending against anomalous ICT activities ICT business continuity policies, procedures or mechanisms Procedures for testing ICT business continuity plan ICT support and recovery plans Procedures for reviewing the results of your risk management framework Procedures for internal governance of your risk control framework Documented security policy
--	--

For assistance in the creation and management of policies, security checklists, and other compliance support, we recommend partners from our network such as [Adaptica](#).



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