BLAZE

Blaze Information Security

DORA Essentials - Understanding Your Cybersecurity Obligations

2024

WHO WILL BENEFIT FROM THIS GUIDE?

We created this guide to bring relevant information on the topic of security requirements of the Digital Operational Resilience Act for leaders in the following audiences:

- Executives responsible for IT security in an organization (CISO, VP of security, CIO)
- Upper-level management, such as C-level executives (CEO, CTO, COO, CFO)
- Compliance managers
- Cybersecurity engineers and analysts (AppSec, SecOps, InfraSec, etc.)
- Engineering managers and product owners

TABLE OF CONTENTS

INTRODUCTION

Welcome to "DORA Essentials: Understanding Your Cybersecurity Obligations," a concise guide to help you understand the requirements of the Digital Operational Resilience Act.

Our goal is to offer a thorough yet accessible exploration of DORA's key components, including its objectives, scope and requirements, and to offer suggestions on how financial organizations should prepare for the new law.

Whether you are part of a major bank, an insurance provider, or a fintech startup, understanding and meeting DORA's requirements isn't just a legal obligation—it's essential for protecting your organization and maintaining customer trust.

We hope this guide will be a reliable resource for helping your institution meet current mandates and prepare for future challenges in the financial sector.

WHAT IS DIGITAL OPERATIONAL RESILIENCE ACT (DORA)?

The EU's Digital Operational Resilience Act (DORA), which entered into force in January 2023, aims to improve financial entities' cyber resilience levels and harmonize the cybersecurity requirements for the financial sector across the whole European Union.

It is one of a trio of EU's recent acts - next to CER (Critical Entities Resilience Directive) and NIS2 (Network and Information Security Directive 2) - aimed at improving cyber resilience levels of entities critical to the economy and society. DORA's scope is broad, as it applies to such institutions as banks, investment firms, crypto-asset service providers, insurance companies, trading venues, and ICT (Information Communication Technologies) third-party providers.

The main goals of the Digital Operational Resilience Act:
As specified in the impact assessment and European Commission's document "Shaping Europe's Digital Future," DORA will ensure operational resilience of the single market for financial services by:

- Harmonizing the rules regarding information security
- Improving ICT risk management of financial firms
- Increasing supervisors' knowledge of threats and incidents
- Improving financial institutions' testing of their systems
- Better overseeing risks from third-party ICT providers, such as cloud service providers

WHO IS IN THE SCOPE OF DORA?

- Credit institutions
- Payment institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- Crypto-asset service providers and issuers of asset-referenced tokens
- Central securities depositories
- Central counterparties
- Trading venues
- Trade repositories
- Managers of alternative investment funds
- Management companies
- Data reporting service providers
- Insurance and reinsurance undertakings
- Insurance, ancillary insurance and reinsurance intermediaries
- Institutions for occupational retirement provision
- Credit rating agencies
- Administrators of critical benchmarks
- Crowdfunding service providers
- Securitization repositories
- ICT third-party service providers

Some entities excluded from the regulation are:

- Institutions for occupational retirement provision that operate pension schemes (under 15 members in total)
- Small and medium-sized insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries
- Post office giro institutions

WILL ORGANIZATIONS OF ALL SIZES BE AFFECTED?

The final draft of DORA introduces the proportionality principle, according to which financial institutions will implement the new rules "according to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations."
Similarly, the impact assessment accompanying DORA states that incident reporting and testing measures would be less stringent for smaller financial firms.

ICT RISK MANAGEMENT REQUIREMENTS

ICT risk management framework

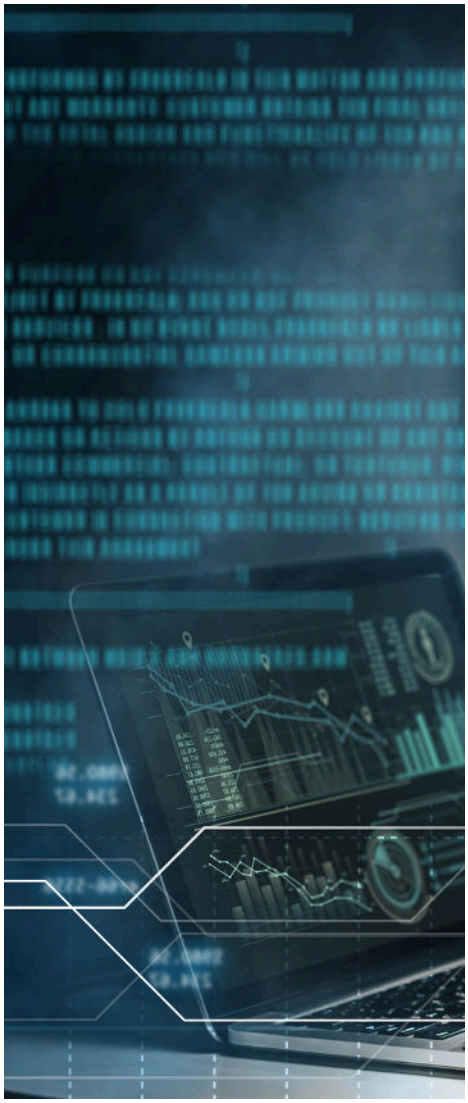
DORA obliges EU financial entities to have an ICT risk management framework, enabling them to address risks quickly and efficiently. The framework will have to include a digital resilience strategy specifying such elements as:

- The risk tolerance level of the financial entity and the impact tolerance of ICT disruptions
- Clear information security objectives
- Mechanisms used to detect, protect and prevent impacts of ICT incidents
- Recording of reported significant ICT-related incidents and the effectiveness of preventive measures
- ICT multi-vendor strategy showing key dependencies on ICT third-party services providers and explaining the rationale for using such vendors
- Implementation of digital operational resilience testing
- Communication strategy in case of ICT-related disruptions

ICT systems, protocols and tools

Financial organizations must use and maintain updated systems, protocols and tools that are reliable, technologically resilient and equipped with sufficient capacity to process the data necessary to provide their services.

→



Protection and prevention

DORA imposes an obligation on financial entities to continuously monitor and control the security and functioning of ICT systems and tools and to minimize the impact of ICT risk on ICT systems.

Financial organizations must design, procure and implement ICT security policies, procedures and tools that aim to ensure the resilience, continuity and availability of ICT systems.

The ICT solutions and processes used to achieve the above objectives will have to:

- Ensure the security of the means of transfer of data
- Minimize the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity
- Prevent the lack of availability, the impairment of authenticity and integrity, the breaches of confidentiality and the loss of data
- Ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

Detection

DORA dictates that financial entities use mechanisms to quickly detect anomalous activities, such as computer network performance issues and ICT-related incidents, and identify potential material single points of failure.
All detection mechanisms must be regularly tested.

The detection mechanisms must enable multiple layers of control and define alert thresholds and criteria to initiate incident response processes, including automatic alert mechanisms for staff in charge of incident response.
Financial entities will have to allocate sufficient resources to monitor user activity and the occurrence of ICT anomalies and incidents, in particular cyber-attacks.

THE ROLE OF MANAGEMENT

One of the main objectives of DORA is to increase the awareness and knowledge of cyber risk among management.
Management bodies of financial institutions will inevitably have to raise their awareness of cybersecurity, as they will be officially responsible for the following:

- ICT risk management
- Setting clear roles and responsibilities for all ICT-related functions
- Determining the appropriate risk tolerance level of ICT risk of the financial entity
- Approving, overseeing and regularly reviewing the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan
- Approving and reviewing the ICT audit plans, ICT audits and material modifications
- Allocating and periodically reviewing appropriate budgets to fulfill the financial entity's digital operational resilience needs, including training on ICT risks and skills for all relevant staff
- Approving and periodically reviewing the financial entity's policy on arrangements regarding the use of outsourced ICT services
- Staying informed of the arrangements with ICT third-party service providers on the use of ICT services, of any changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical functions, including receiving a summary of the risk analysis to assess the impact of these changes
- Staying informed about ICT-related incidents and their impact and about response, recovery and corrective measures.

INCIDENT MANAGEMENT, CLASSIFICATION AND REPORTING

Under DORA, financial entities will have to implement an **incident management process** to detect, manage and notify of ICT-related incidents.

The process must include early warning indicators and *"procedures to identify, track, log, categorize and classify ICT incidents according to their priority and severity and the criticality of the services impacted."*

All cybersecurity incidents will have to be recorded. Financial institutions will have to have procedures and processes for monitoring, handling and follow-up on cyber incidents to ensure their causes are identified, documented and addressed.

The management bodies of financial firms will have to be informed of at least major ICT-related incidents, with reports explaining the impact, response and additional controls regarding the incident.

Major ICT incidents will also have to be reported to the relevant national authorities.

Credit institutions classified as significant will report cyber incidents to the relevant national competent authority, which will then inform the European Central Bank (ECB).

MANAGING ICT THIRD-PARTY RISK

DORA requires financial entities to incorporate ICT third-party risk management into their risk management framework.
Rules regarding pre-deal due diligence and performing risk assessments on third-party service providers are largely not new. What DORA introduces, however, is the function of a **Lead Overseer**, appointed by ESAs, that will have the power to audit providers of third-party services supporting critical or important functions.

The Lead Overseer's main tasks will include:

- Being the primary point of contact to the critical ICT third-party providers
- Assessing whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities
- Adopting an oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider

Digital Operational Resilience Act introduces the function of a Lead Overseer, appointed by ESAs, who will have the power to audit providers of third-party services supporting critical or important functions.

DIGITAL OPERATIONAL RESILIENCE TESTING

Organizations affected by the Digital Operational Resilience Act will have to test all critical systems and applications at least yearly by an independent party. The testing program should include a full range of appropriate tests, including:

- Vulnerability assessments and scans
- Open source analyses
- Network security assessments
- Gap analyses
- Physical security reviews
- Questionnaires and scanning software solutions
- Source code reviews
- Scenario-based tests
- Compatibility testing
- Performance testing
- End-to-end testing
- Penetration testing

Threat-led penetration testing - TLPT

Financial entities will be obliged to undergo **threat-led penetration testing at least every 3 years**. Such pentesting will cover the critical functions and services of a financial entity (including those outsourced to ICT third-party providers) and will be performed on live production systems.

Threat-led penetration testing is more relevant for core financial entities such as banks and payment institutions and less relevant for other subsectors (for example, asset managers and credit rating agencies). Microenterprises are exempt from this requirement.

In July 2024, the European Supervisory Authorities (ESAs) published technical standards on TLPT in accordance with the TIBER-EU framework.

→

TLPT PROCESS

Testing methodology and process

The main participants of a Threat-Led Penetration Test (TLPT) include the financial entity undergoing the test, with a control team managing the process and a blue team defending the entity's systems without prior knowledge of the test.
Additionally, the TLPT authority oversees and validates the testing process, often through a dedicated TLPT cyber team.

External testers (red team) simulate real-world cyberattacks, and threat intelligence providers gather and analyze relevant threat data to create realistic attack scenarios. Each participant plays a crucial role in ensuring the TLPT's effectiveness in identifying and mitigating potential vulnerabilities.

TLPT authority

TLPT cyber team

Threat intelligence providers

Financial entity

Blue team

White team
(control team)

Red team
(Internal or external testers)

TESTING PHASES

The TLPT process is structured into three main phases: preparation, testing, and closure.

PREPARATION PHASE

- **Notification and initiation:** Financial entities receive a notification from the TLPT authority indicating the requirement to perform a TLPT. Within three months of notification, entities must submit TLPT initiation documents, including a project charter, control team lead contact details, intended use of testers, communication channels, and a code name for the TLPT.

- **Control Team formation:** A control team is established, including a lead responsible for the TLPT's day-to-day management. The team handles internal and external communications, risk management, and procurement of suitable threat intelligence providers and penetration testers.

- **Scope specification:** Within six months, the control team must submit a scope specification document detailing the critical or important functions to be tested. The document should be approved by the financial entity's management body and validated by the TLPT authority.

→

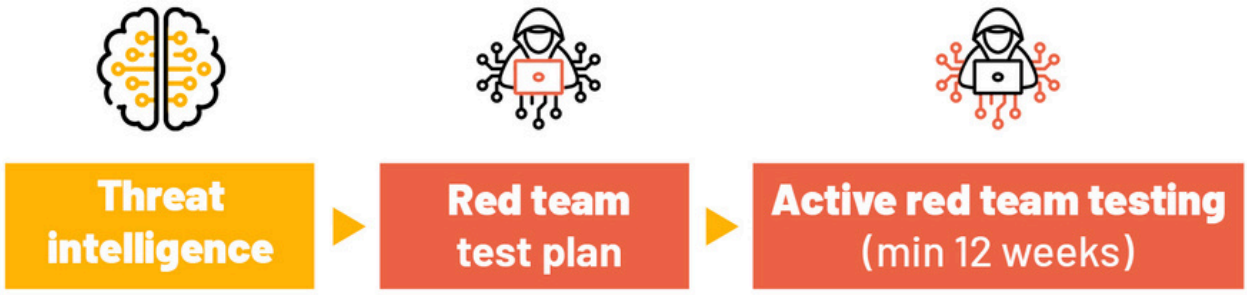
TESTING PHASE

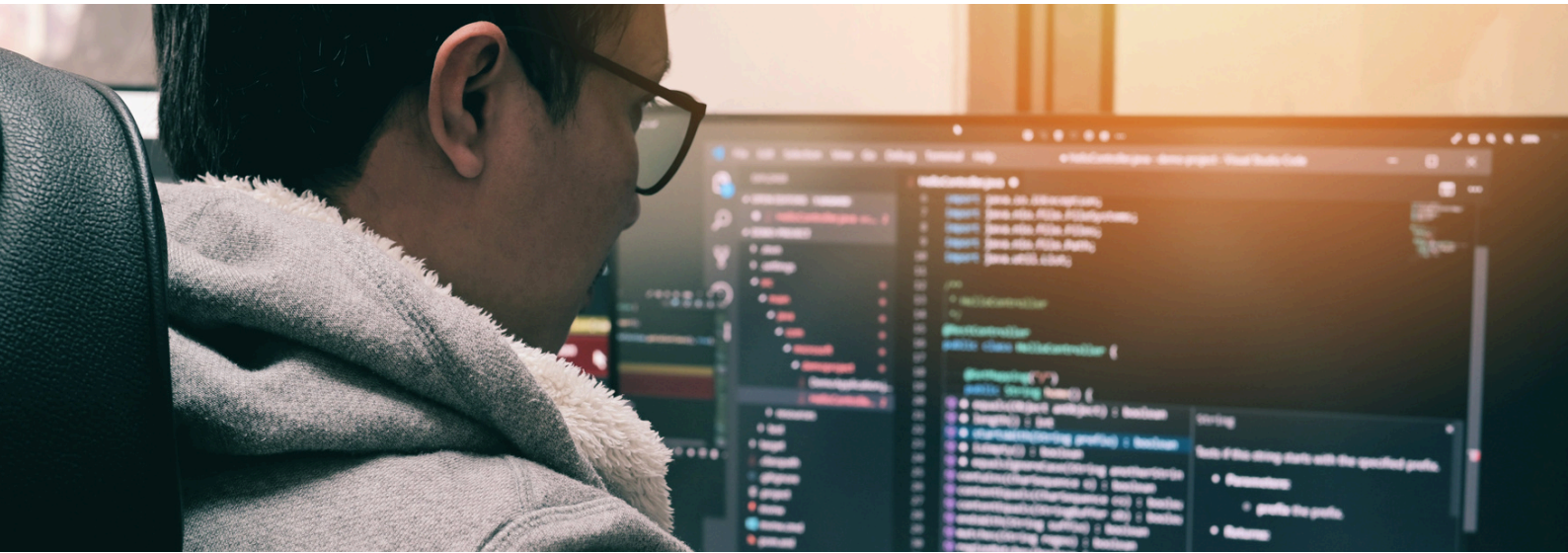
The testing phase is divided into two main activities:
threat intelligence gathering and red team testing.

- **Threat intelligence gathering:** The threat intelligence provider collects and analyzes relevant threat intelligence, identifying potential attack surfaces and threat scenarios. Next, the control team, testers, and TLPT authority select at least three attack scenarios for the test, with one scenario potentially being non-threat-led for forward-looking analysis.

- **Red Team testing:** Testers develop a red team test plan based on the scope specification and threat intelligence report that has to be reviewed and approved by the control team and TLPT authority.

The active red team testing phase lasts at least twelve weeks. During this time, testers simulate real-life cyber-attacks on the financial entity's live production systems. Testers report weekly to the control team and TLPT authority, and adjustments to the test plan are made as necessary.





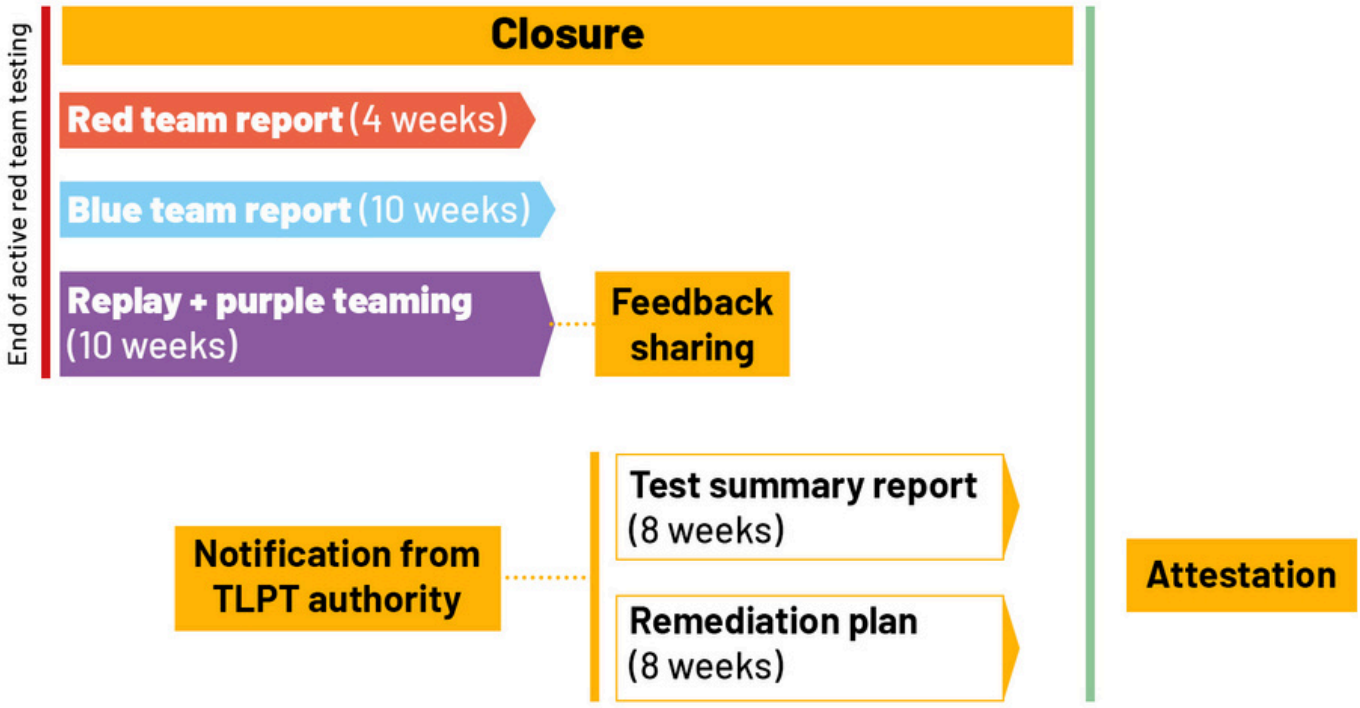
CLOSURE PHASE

The closure phase focuses on analyzing the results, replaying actions, and developing remediation plans. At this stage, the blue team is notified that TLPT has been performed. The use of the purple team is mandatory at this phase.

(1) **Reporting:** Testers submit a red team test report to the control team within four weeks of completing the active testing phase. The control team shares the report with the blue team, which then submits a blue team test report within ten weeks.

(2) **Replay and Purple Teaming:** The control team organizes replay and purple teaming exercises to review offensive and defensive actions taken during the TLPT. Purple teaming is a collaborative testing activity that involves both the red team and the blue team.

(3) **Remediation:** Based on the TLPT findings, the control team prepares a remediation plan that addresses identified shortcomings, including a root cause analysis, proposed measures, prioritization, and implementation responsibilities.



Requirements for providers carrying out TLPT

For carrying out the **threat-led penetration testing (TLPT)**, the financial entities will only use providers that:

- Are reputable
- Have technical and organizational capabilities and have specific expertise in threat intelligence, penetration testing, and red teaming
- Are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks
- Provide independent assurance, or an audit report, about the sound management of risks associated with the carrying out of TLPT, including the protection of the financial entity's confidential information and redress for the business risks of the financial entity
- Are covered by relevant professional indemnity insurance, including against risks of misconduct and negligence.

OVERLAPS WITH NIS2

The NIS2 directive already covers certain entities in the financial sector, including credit institutions, operators of trading venues, and central counterparties.

However, as the regulations of the Digital Operational Resilience Act are more specific, DORA is considered *lex specialis* and, therefore, overrides NIS2 when it comes to ICT risk management and ICT risk reporting.

Where NIS2 and DORA overlap is in the information sharing departments.

The DORA competent authorities would be able to consult and share relevant information with the Single Point of Contacts (SPOCs) and CSIRTs established under NIS2.

The SPOCs, or the CSIRTs established under NIS2 would also receive details of major ICT-related incidents from the competent authorities under DORA.

The Digital Operational Resilience Act (DORA) is considered *lex specialis* and overrides NIS2 when it comes to ICT risk management and ICT risk reporting.

WHAT WILL BE THE COSTS FOR FINANCIAL INSTITUTIONS?

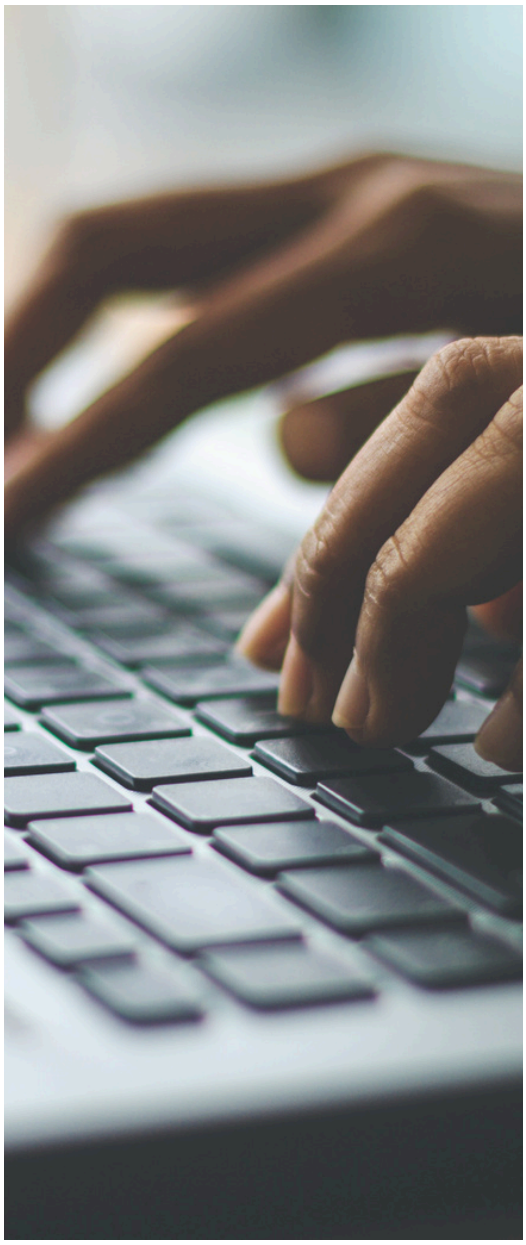
According to the impact assessment conducted in 2020, the new requirements would give rise to both one-off and recurring costs.
Some large financial firms have already made significant investments in their computer systems, and for them, the costs of implementing the measures of this proposal are likely to be low.
For smaller firms, the costs are expected to be lower as well, as they would be subject to less stringent measures proportionate to their lower risk.

When it comes to testing, the European Supervisory Authorities have estimated that the costs related to threat-led penetration testing range between **0.1% and 0.3% of the total ICT budget of affected organizations.**
Costs related to incident reporting would be drastically reduced, as there would be no overlaps with NIS in this regard.

Competent national authorities will have the power to impose penalties and establish remedial measures for any breaches of the regulation. DORA doesn't specify minimum nor maximum fines that may be imposed; it states only that those penalties and measures must be effective, proportionate and dissuasive.

STEPS TO TAKE IN PREPARATION FOR DORA

The provisions of DORA will apply from January 17, 2025. However, there are steps organizations can and should already take, starting from a review of their existing internal governance and risk management frameworks.



1. **Review internal governance and control framework and ICT risk management framework**
2. **Think about which systems to put in place to comply with detection obligations**
3. **Check if crisis communication plans are up to date**
4. **Review outsourced ICT services**

HOW CAN BLAZE HELP YOUR ORGANIZATION WITH DORA COMPLIANCE?

BLAZE

Specializing in security testing and assessments, Blaze Information Security provides essential support to financial institutions, including major international banks, ensuring their digital infrastructure meets the highest standards of cybersecurity resilience.

Our service suite, focused on in-depth security assessments and penetration testing, is designed to uncover and mitigate vulnerabilities in your infrastructure, ensuring alignment with DORA's stringent operational resilience standards.

We understand the nuances of regulatory expectations, particularly in the context of global banking, and offer targeted solutions that meet these specific challenges.

Partnering with us is a commitment to excellence in cybersecurity and operational resilience, helping your institution maintain robust compliance with DORA and stay protected against the cyber risks of today and tomorrow.

Contact us for your DORA penetration testing needs.

BLAZE

www.blazeinfosec.com

GERMANY
Friedrichstraße 114A
10117, Berlin

PORTUGAL
Praça do Bom Sucesso
131/206
4150-146, Porto

BRAZIL
Rua Padre Carapuceiro
968/2006
51020-280, Recife

POLAND
ul. Józefa Sarego 5/4
31-047, Kraków