HADRIAN

The Quick Guide to Preparing for the Digital Operational Resilience Act

What is the Digital Operational Resilience Act?

Marking a pivotal moment in cybersecurity and financial regulation, the Digital Operational Resilience Act (DORA), officially came into play on January 16th, 2023. With a laser focus, DORA spearheads the mission to elevate and unify risk protocols across the Information Communication Technology (ICT) spectrum within the European Union's financial arena. The primary focus is on unifying and strengthening the digital operational resilience framework.

DORA establishes consistent criteria for securing the network and information systems of businesses and entities within the financial sector, along with essential third-party providers offering ICT-related services like cloud platforms or data analytics services. It constructs a regulatory structure focused on digital operational resilience, mandating that all enterprises ensure their ability to endure, respond to, and recover from various disruptions and threats related to ICT. These requirements are standardized across all member states of the European Union, with the primary objective being the prevention and mitigation of cyber threats.

The quick answer

How can security and risk management (SRM) leaders prepare for the EU's Digital Operational Resilience Act?

- Determine whether your organization needs to meet DORA's requirements
- First focus on ICT risk management, third-party risk, information sharing, incident reporting and operational resilience testing
- Develop a comprehensive plan to close any compliance gaps

Elevating Security Practices

DORA's broad applicability is prompting inquiries from entities both within and outside the EU. The resilience demanded by DORA extends its reach across various departments and managerial roles, including the Chief Information Security Officer (CISO), Chief Information Officer (CIO), and Enterprise Risk teams. Factors such as Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for Service Level Agreements (SLAs) are coming into focus.

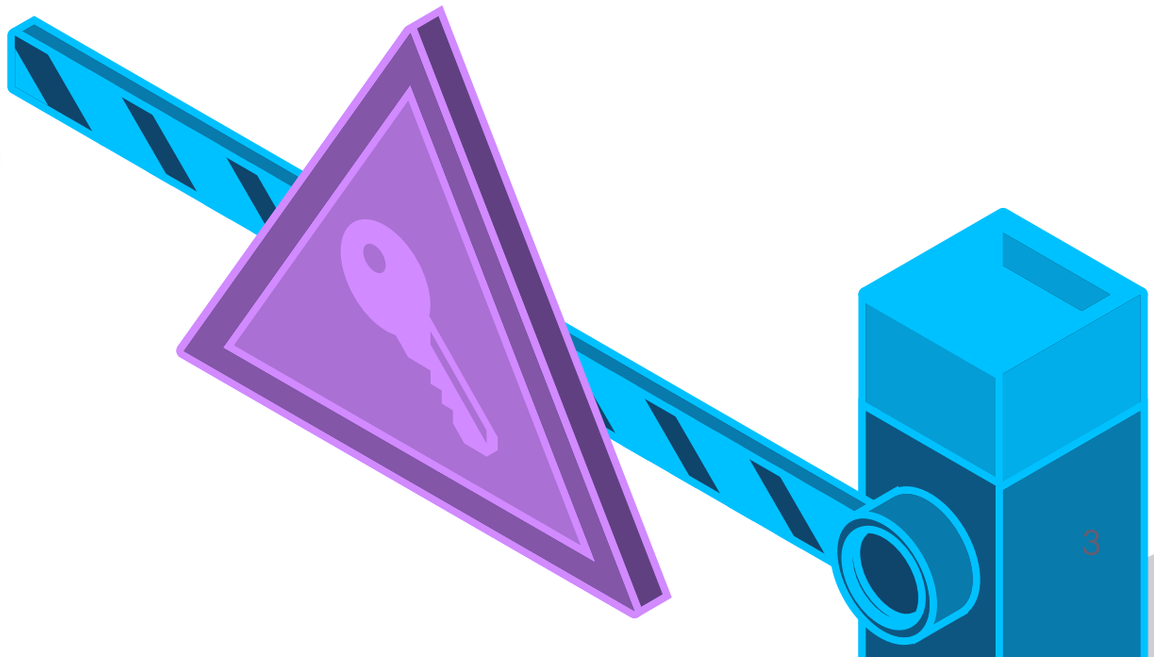
In the last decade, ESAs provided guidance on ICT risk management, influencing regulators like the European Central Bank (ECB) and De Nederlandsche Bank (DNB). Now, with DORA in effect, it's time to assess your ICT risk practices. Dive into your current posture, identify gaps, and align with DORA. This isn't a bureaucratic checkbox; it's a chance to strengthen controls. Standardize and automate for cost-effective ICT risk management. Prepare for DORA-initiated audits and inspections.

For some, DORA marks the start of a fast-tracked maturity journey; for others, it's an opportunity to enhance capabilities. In a world valuing digital resilience, DORA guides you. It's beyond compliance—it's about crafting a resilient financial ecosystem.

Why is the Digital Operational Resilience Act a game-changer?

2 minute read

Read blog post



Who's In and Who's Out: DORA's Scope of Application

Dive into Article 2 of DORA to understand its reach.

In Scope:

- Credit institutions
- Payment institutions
- Account information service providers
- Investment firms
- Crypto-asset service providers
- Insurance and reinsurance undertakings

...and many more, totaling 21 types of entities. (See Article 2 for the full list.)

Out of Scope:

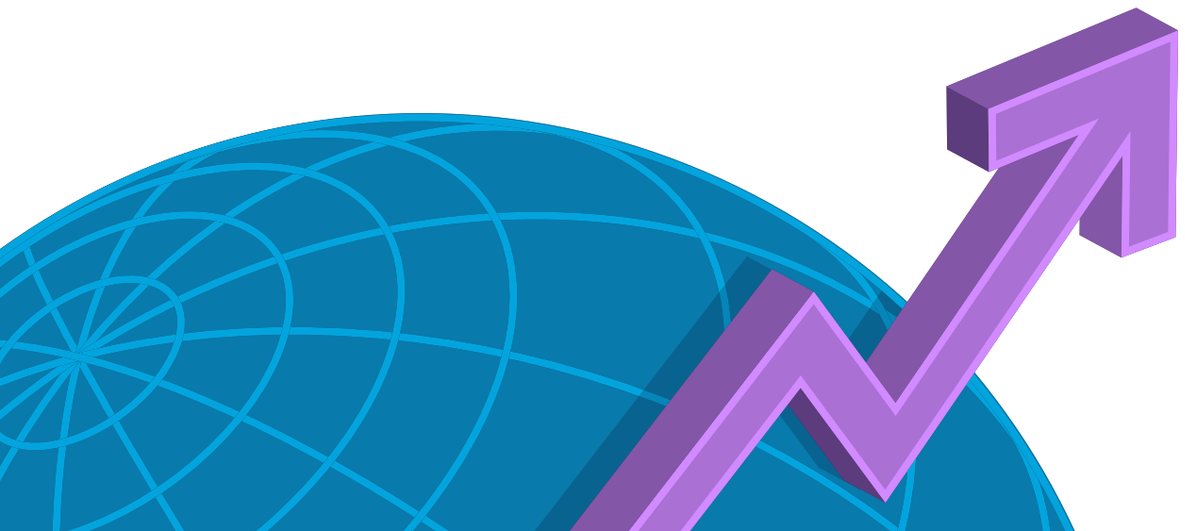
- Managers of specific alternative investment funds
- Certain insurance and reinsurance undertakings
- Small-scale pension schemes
- Microenterprises or small to medium-sized insurance intermediaries
- Post office giro institutions

> **Note**
> Member States might have specific exclusions. Always refer to the original directives for precise details.

The Role of ESAs in Market Resilience

As you delve into the 64 articles of DORA, the increased role that European Supervisory Authorities (ESAs) will play in overseeing local enforcements becomes essential. Companies should anticipate heightened supervision and robust controls, including obligations such as:

- Crafting a sound, comprehensive and well-documented ICT risk management framework (article 6(1)) that must include at least the strategies, policies, procedures, ICT protocols and tools that are necessary to protect all information and ICT assets
- Sharing mandatory reports on major ICT-related incidents
- Developing resilient Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs)
- Testing ICT business continuity plans and ICT response and recovery plans at least once a year



What are ESAs?

European Supervisory Authorities (ESAs) are integral components of the European System of Financial Supervision (ESFS) established in 2011.

Consisting of entities like the European Banking Authority (EBA) in Paris, European Securities and Markets Authority (ESMA) in Paris, and European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt, ESAs play a crucial role in microprudential oversight at the European Union level.

They were proposed by the European Commission in 2009 as a response to the financial crisis of 2007–08.

Fines and Implications

Financial institutions failing to adhere to the regulation may face several consequences, including:

Administrative fines
Serious infringements can lead to fines of up to 10 million euros or 5% of the total annual turnover, whichever is higher.

Remedial measures
Supervisory authorities may mandate institutions to take corrective actions to address operational resilience weaknesses.

Public reprimands
Supervisory bodies can publicly call out financial institutions that don't meet the regulation's demands.

Withdrawal of authorization
Repeated failures to comply may lead to the withdrawal of the institution's authorization.

Compensation for damages
Institutions may be obligated to compensate customers or third parties for damages arising from non-compliance.

Identifying Hurdles on the DORA Horizon

The Act approved, granting companies until 2025 for DORA implementation. During the two-year preparation (2023 & 2024), align governance with DORA's pillars. Conduct a gap assessment for a digital resilience strategy. From 2025, mandatory reports, testing, and annual evaluations are required. Penetration testing and ESA certification become mandatory by end-2025.

September 24, 2020: Publication of DORA proposal by the European Commission

July 23, 2022: Provisional agreement on DORA reached

November 10, 2022: DORA regulation ratification by the European Parliament

Q4 2022 (Nov/Dec): Publication of DORA in the Official Journal of the EU

January 17, 2023: Adoption Day
DORA comes into force

Q3 2023 - Q4 2024: Submission of technical standards by the ESAs

January 17, 2025: DORA Applicability
Full compliance with DORA and its technical standards required

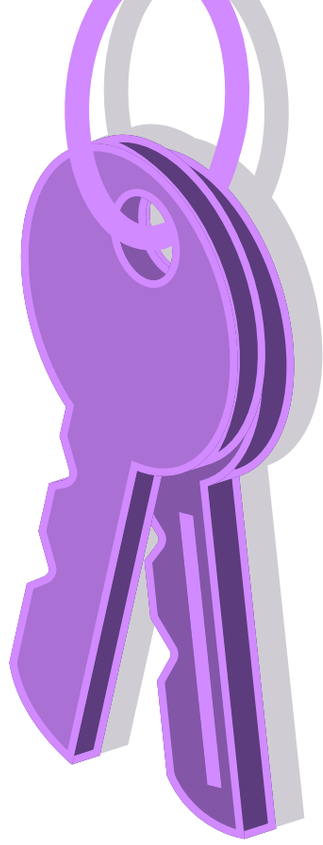
Beware!

DORA takes precedence over overlapping texts like NIS or ESA guidelines, making it the primary reference for regulatory compliance checks to avoid gaps when it becomes effective in 2025.

Navigating DORA - Key Components

DORA's legal text, outlined by the European Union, delineates the legislation's provisions and targets five core pillars of cybersecurity for enhancement.

From cybersecurity requirements to risk management, each element plays a pivotal role in shaping the future of financial cybersecurity.



5 Core Pillars

ICT Risk Management

Establish evidence of internal governance and control frameworks that ensure the effective management of all ICT risks.

ICT Third-Party Risk

Effectively manage third-party ICT risk, including risks arising from contracting third-party ICT service providers.

Information Sharing

Facilitate the exchange of cyber threat information and intelligence among financial entities.

ICT-Related Incident Reporting

Develop the capability to report major incidents to competent authorities and inform service users and clients.

Digital Operational Resilience Testing

Implement, maintain, and review digital operational resilience testing programs.

Requirements for Successfully Becoming DORA Compliant

The introduction of the Digital Operational Resilience Act (DORA) marks a pivotal moment for the financial sector, shifting institutions from primarily managing operational risk through capital allocation to now also adhering to rules for comprehensive ICT-related incident protection, detection, containment, recovery, and repair capabilities. However, this regulatory shift poses compliance challenges for targeted organizations:

Expansive Applicability: DORA's broad scope covers diverse financial institutions and Critical Third-Party Service Providers (CTPSs), making precise delineation of its applicability challenging.

Complex Requirements: The intricate mandates of DORA require a detailed understanding and strategic planning, adding complexity to both comprehension and execution.

Financial Strain: Compliance with DORA comes with palpable financial implications as institutions invest in bolstering ICT systems and restructuring processes.

Cultural Shift: Operational resilience requires a mindset shift, presenting a significant challenge in transitioning from conventional operations to a resilience-focused approach.

Strengthen
ICT Risk Management Rules

Extend
ICT regulation to all parties

Harmonise
Reporting & Information Sharing

Standardise
Resilience Testing & Monitoring

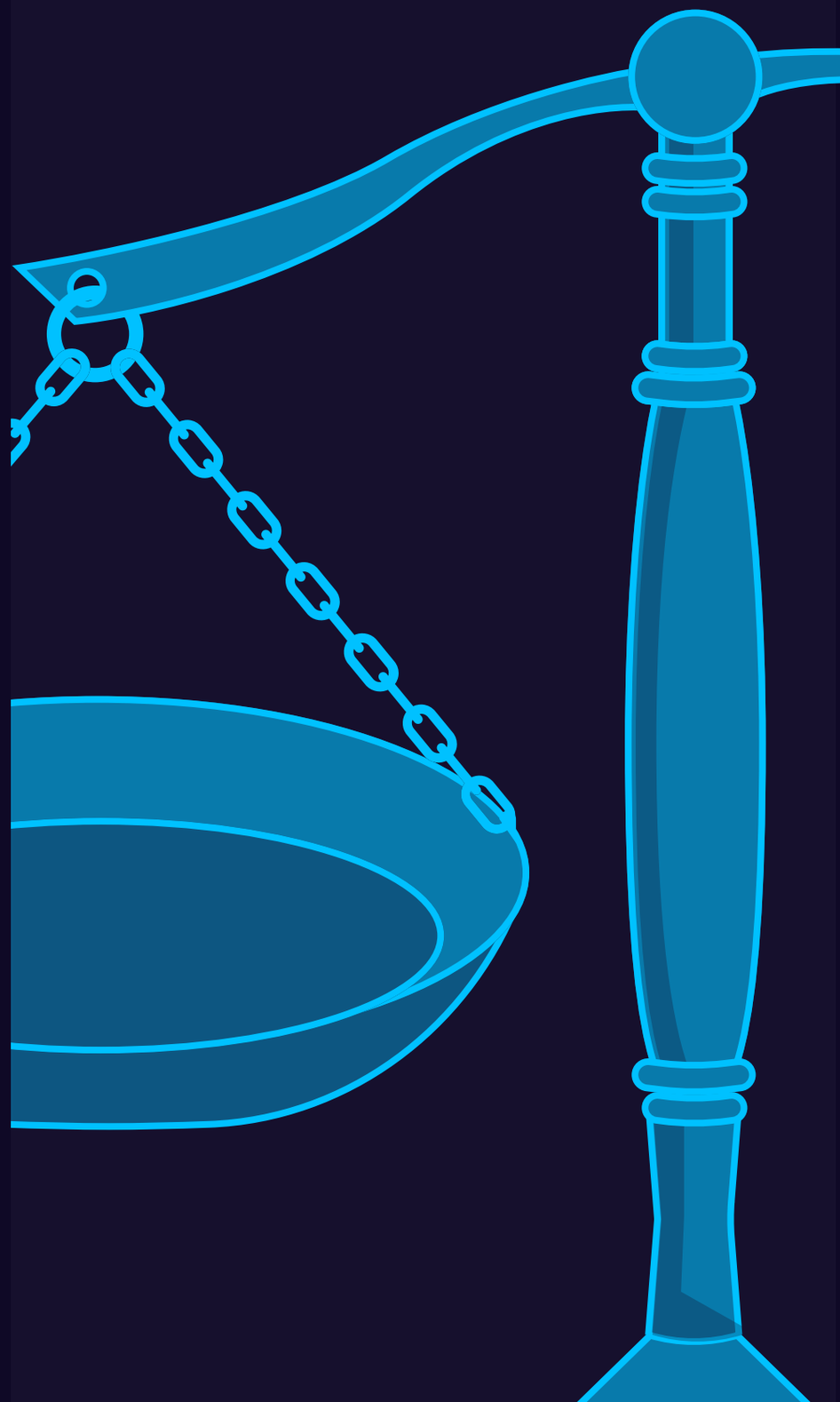
Requirements for Successfully Becoming DORA Compliant (Cont.)

Resource Limitations: Resource constraints, including budget limitations, skill deficits, and staffing shortages, can impede full-scale DORA implementation, especially for smaller entities.

Collaboration Challenges: Cooperative efforts, particularly with third parties, are often necessary under DORA. However, eliciting consistent cooperation, especially from entities beyond DORA's jurisdiction, can be arduous.

Dynamic Regulatory Landscape: The ever-evolving regulatory landscape in the financial sector poses a persistent challenge in maintaining continuous DORA compliance.

Despite these hurdles, embracing DORA compliance promises to pave the way for a more resilient, secure, and dependable financial ecosystem in the EU.



Adapting to DORA Compliance

ESAs anticipate a new era of reporting and communication from financial institutions, providing valuable insights to enhance the EU's cyber intelligence. ESAs will refine RTSs during this time, requiring companies to align governance and practices with DORA's resilience pillars.

To materialize a digital resilience strategy, companies can conduct an initial gap assessment, analyzing their maturity level. This involves evaluating compliance with existing guidelines (ESA, NIS, CROE) and IT risk management standards (ITIL, COBIT, NIST CSF, ISO). By identifying deltas, a roadmap can prioritize efforts for DORA requirements. During this phase, regulators will define new RTSs and ITSs, necessitating an agile strategy.

A significant change introduced is the Digital Operational Resilience Testing, based on Threat Led Penetration Testing (proposal of the article 23), featuring two categories:

Mandatory Annual Internal Testing	**Advanced Testing (Every Three Years)**
Applicable to all financial sector entities	Applicable to companies meeting regulator-defined criteria
Requires submitting results to ESAs in a specified format	Conducted by an external entity, with ESAs issuing compliance certificates
	Non-compliance could lead to a potential halt of company activities

Navigating the Road to DORA Compliance

Prepare for DORA's full enforcement in January 2025 by initiating projects, assessing budget requirements, and implementing organization-wide initiatives. Build resilience and achieve DORA compliance with the following steps:

Risk Identification through Network Mapping:

- Initiate risk identification by mapping application dependencies across entire infrastructure.
- Leverage security solutions like Hadrian to facilitate this mapping process, revealing critical and non-critical processes, and identifying third-party dependencies.
- Address previously unknown risks promptly upon discovery.

Enhance Detection Capabilities:

- Utilize the improved understanding of your environment to enhance detection capabilities.

Proactive Breach Containment:

- Recognize breach containment as a crucial aspect of resilience according to DORA.
- Implement technologies like micro-segmentation (Zero Trust Segmentation) to separate the network into zones, allowing controlled communication between workloads and devices.
- Proactively isolate high-value assets or reactively contain compromised systems during an active attack to halt the spread of a breach.

Read blog post

Understanding the DORA Framework

DORA goes beyond a mere compliance mandate; it presents a chance to future-proof your business, enhance cybersecurity practices, and equip your organization for the upcoming challenges and opportunities in the digital finance landscape. Here's how you can do it:

Download the Datasheet

Manage risk by proactive offensive security

Establish evidence of internal governance and control frameworks that ensure the effective management of all ICT risks.

How Hadrian can help

Hadrian's Continuous Automated Red Teaming (CART) provides ongoing and automated simulated attacks on your system to identify vulnerabilities and weaknesses. Because it is continuous, we can identify new threats and vulnerabilities as they emerge.

Effectively manage third-party risk

When it comes to third parties, the appropriate legal agreements to protect cybersecurity are essential. But in the end, you'll have to police any vulnerabilities your third parties bring to your attack surface. That's a tall order, and virtually impossible to monitor by hand.

How Hadrian can help

Hadrian's intelligent security platform assesses your entire attack surface, identifies vulnerabilities from third-party sources, evaluates the likelihood and impact of exploitation, suggests remediation, and validates post-remediation security.

Prepare for fast & accurate incident reporting

DORA is intended to harden cybersecurity across the European Union through the use of fast and effective incident reporting. Information sharing contributes to creating increased awareness of cyber threats and helps to contain ICT-related incidents, DORA says.

How Hadrian can help

Traditional compliance reports lack real-time updates, potentially leading to delayed awareness of issues. Hadrian provides accurate and clear reports, meeting DORA requirements for external stakeholders and ensuring confident communication with executives and board members.

About Hadrian

Defensive security should be validated by offensive security. Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously. Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

> ‘What's exciting about what Hadrian is doing is they solved a seemingly impossible puzzle: finding weaknesses in a complex network with human-like detail, at scale, from the outside and continuously. What usually takes a dedicated team of security engineers a few weeks to figure out for one system, they can do in minutes for thousands of systems.’
>
> **Tiago Teles - Security Lead, ABN AMRO**

Trusted by

ABN·AMRO · SHV ENERGY · macmillan education · CTC GLOBAL

WeatherTech · LEROY MERLIN · LOTTOMATICA · Crédit Agricole

RITUALS · BIOLANDES · nedap · Van Oord

DORA Compliance Printable Checklist

Download Checklist

DORA Essential Terms to know

Account Information Service Provider: An account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;

Crypto-Asset Service Provider: A crypto-asset service provider as defined in the relevant provision of the Regulation on markets in crypto-assets;

Cyberattack: A malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorized access to, or make unauthorized use of, an asset;

Digital Operational Resilience: The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions;

European Supervisory Authorities: The regulatory agencies established under the European System of Financial Supervision in order to ensure financial stability;

ICT Asset: A software or hardware asset in the network and information systems used by the financial entity;

ICT Risk: Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment;

ICT-related Incident: A single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity;

Insurance Undertaking: An insurance undertaking as defined in Article 13, point (1), of Directive 2009/138/EC;

Implementing Technical Standards (ITS): A technical implementing act providing for the uniform application of certain provisions in the basic legislative act;

Manager of Alternative Investment Funds: A manager of alternative investment funds as defined in Article 4(1), point (b), of Directive 2011/61/EU;

Medium-sized Enterprise: A financial entity that is not a small enterprise and employs fewer than 250 persons and has an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million;

DORA Essential Terms to know (cont.)

Microenterprise: A financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million;

Network and Information System: Network and information system as defined in 2022/2555;

Payment Institution: A payment institution as defined in Article 4, point (4), of Directive (EU) 2015/2366;

Regulatory Technical Standards (RTS): A delegated act, technical, prepared by a European Supervisory Authority;

Reinsurance Undertaking: A reinsurance undertaking as defined in Article 13, point (4), of Directive 2009/138/EC;

Small Enterprise: A financial entity that employs 10 or more persons, but fewer than 50 persons, and has an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but does not exceed EUR 10 million;

Threat-led Penetration Testing: A framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.