DORA Overview

Version 1.0

Digital Operation Resilience Act (DORA) - Overview

What is DORA?

DORA is a directly applicable European Union Regulation (EU) 2022/2554 designed to strengthen the digital operational resilience of financial entities across the EU by addressing ICT risk management, incident reporting, third-party dependency, and resilience testing. DORA requires these financial organisations to take measures for ICT risk management, security of ICT systems, and reporting ICT-related incidents. The overall aim is to enhance their digital resilience.

Digital Operational Resilience Act (DORA) - EIOPA

Digital Operational Resilience Act | European Banking Authority

Digital Operational Resilience Act (DORA)

DORA consists of multiple parts and one of those is mandatory Threat Led Penetration Testing (TLPT). If a financial entity has been informed by their lead authority to complete a DORA assessment, they must perform a TLPT in accordance with the TIBER-EU framework. Article 26 of DORA formalises Threat Led Penetration Testing (TLPT) as a regulatory requirement for certain financial entities. The European Supervisory Authorities (ESAs) have published Regulatory Technical Standards (RTS) specifying that TLPT under DORA must follow a TIBER-EU aligned methodology.

Why DORA TLPT Exists - The Supervisory Intent

DORA represents a fundamental shift in European supervisory expectations. Historically, cyber resilience was assessed through policies, frameworks, and documented controls. Under DORA, resilience is assessed through demonstrated operational capability.

Financial entities are no longer judged solely on the existence of governance structures or control documentation, but on whether they can detect, respond to, contain, and recover from advanced threat activity under realistic conditions.

©CREST (International) All rights reserved

What Supervisors Are Actually Testing

TLPT under DORA is therefore not simply a red team exercise. Supervisors are assessing:

- Whether detection capabilities identify sophisticated adversary behaviour
- Whether containment actions are timely and effective
- Whether escalation and decision-making processes function under pressure
- Whether governance oversight is active and informed during a crisis
- Whether remediation is structured, prioritised, and owned at senior level

The objective is to test resilience as it operates in practice, not as it is described on paper

Emerging Supervisory Focus Areas

Across Europe, supervisory feedback and thematic reviews indicate particular scrutiny in the following areas:

- Identity and access management weaknesses, including privileged access and authentication controls
- ICT third-party dependency risk, especially where critical functions rely on cloud or managed service providers
- Remediation governance, including how quickly vulnerabilities are addressed and how senior management tracks risk reduction
- Operational coordination, particularly between technical teams and executive decision-makers

DORA TLPT therefore acts as a stress test of both technical controls and organisational maturity.

What is TIBER-EU

TIBER-EU is a European framework for threat intelligence-based ethical red-teaming. It provides comprehensive guidance on how authorities, entities, and threat intelligence providers and red-team testers should work together to test and improve the cyber resilience of entities by carrying out controlled cyberattacks.

TIBER-EU has been in existence since 2018 and has a robust set of documentation and guidelines. What is TIBER-EU?

There is no intention to fully replicate the detailed documentation here but to simply give an overview of the main phases that may be useful for anyone that has not been involved in TIBER-EU previously or is now interested because of DORA.

©CREST (International) All rights reserved

DORA Phases and Timelines

Identification

Under DORA, TLPT is not automatically applicable to all financial entities. Article 26 provides that only a subset of entities deemed significant from a systemic or risk perspective will be designated by their competent authority to undergo TLPT. The determination is supervisory and risk-based, taking into account factors such as the entity's size, complexity, critical functions, ICT dependency, and potential impact on financial stability.

Entities formally designated for TLPT will receive written notification from their competent authority initiating the process. Once designated, TLPT must be conducted at least once every three years, unless the authority requires more frequent testing based on the entity's evolving risk profile or supervisory findings. The scope, depth, and structure of each engagement are subject to proportionality and supervisory discretion, ensuring that the test reflects the operational realities and systemic importance of the entity concerned.

Financial entities that are not designated may still elect to undertake a voluntary TIBER-EU aligned test to benchmark resilience, improve detection and response capability, or prepare for potential future supervisory designation

Preparation Phase – 6 months

Notification

Notification is individual to each Financial Entity (FE) and happens close to when they must start their DORA assessment. This letter starts the clock with an expectation that DORA is completed within fifteen to sixteen months. Within each European country the Competent Authority (CA) is responsible for the identification and notification process and the TIBER Cyber Team (TCT) is responsible for the operational and delivery aspects. There may be multiple regulatory and oversight entities involved or just one completing all aspects. This will be a decision for each country within the European Union (EU).

Scoping

The FE creates their Control Team (CT), performs a scoping assessment and produces a scoping document presented to the TCT for their approval.

TIBER-EU Scope Specification Document Guidance

©CREST (International) All rights reserved

Procurement

The FE looks to procure the services of a TIP and RTT who can be separate companies or a single provider, if the two teams do not have the same people as members. Where a single provider is used, it is best practice to be able to demonstrate that appropriate separation is in place between the two teams to prevent influencing the outcomes of either phase. There are procurement guidelines defining what qualifications and experience is recommended. CREST TLPT accredited companies meet the qualification criteria by providing CREST Certified Red Team Specialist, Red Team Manager and Threat Intelligence Manager resources.

TIBER-EU Guidance for Service Provider Procurement

An FE can use internal testers if they can demonstrate independence and match the criteria within the service provider guidance document. The TCT can veto a provider or the internal team if they believe they represent a risk of not being able to deliver a successful TIBER-EU engagement.

The final part of procurement is the launch meeting which has the TIP, RTT and CT as attendees.

Testing Phase – Threat Intelligence - 4 to 7 weeks

There may or may not be a Generic Threat Landscape (GTL) report provided by the CA or TCT from the country where the FE is being tested. If one is provided, then it should form the baseline of the Threat Intelligence activities. There are two meetings scheduled during this phase; in the first all Critical Functions (CF) of the FE must be covered, in the second only the CF that are most relevant must be covered but that could still be all of them.

The Threat Intelligence phase is managed by a CREST Certified Threat Intelligence Manager throughout and is completed when the TCT approves the report.

The deliverables for this phase are at minimum typically:

- The targeting report,
- A threat intelligence report,

A scenarios report TIBER-EU Targeted Threat Intelligence Report Guidance

©CREST (International) All rights reserved

Testing Phase – Red Teaming – 15 to 16 weeks (required minimum)

The first 2 to 3 weeks are where the Red Team assess the deliverables from the Threat Intelligence Testing Phase and creates the test plan, which is discussed during a meeting before the final version is submitted and presented for TCT approval. When the approval has been received then the active testing can begin and must last for a minimum of 12 weeks. There are weekly meetings with the TCT plus meetings with the CT at a cadence agreed between them and the RTT. If for some reason, there is a need to perform Purple Team (PT) activities because it is not possible to continue in a stealthy or Red Team manner then this time does not count towards the closure phase PT requirement.

The deliverables for this phase are at minimum typically:

- The red team test plan,
- A detailed technical report,
- A purple team report,

TIBER-EU Guidance for the Red Team Test Report

Closure Phase – 19 weeks

The Red Team has 4 weeks from the last active testing day to deliver the final report. The Blue Team (BT) then has 6 weeks to deliver their final report. During the BT reporting time Replay workshops and an exercise take place with a 1-2 week gap before PT workshops and exercise. The FE chooses what activities from the Red Team phase are performed in the replay and PT exercises and provide the relevant access to facilitate this.

TIBER-EU Blue Team Test Report Guidance

TIBER-EU Purple Teaming Guidance

The TCT must approve both the Red and Blue team reports before moving on to the 360 feedback activities. This is concluded with a document following a meeting (usually in person) where all parties involved discuss what went well and areas for improvement.

TIBER-EU Test Summary Report Guidance

The FE produces a test summary for the TCT, a remediation plan for the CA and there is an attestation signed by the TCT and FE to the effect that a TIBER-EU was completed in accordance with the guidance and to their satisfaction.

©CREST (International) All rights reserved

Organisations Involved in DORA Threat Led

Penetration Tests

DORA considers all aspects of ICT used by FE and therefore Third-Party Service Providers (TPSP) to whom services are outsourced or contractually managed may also be involved as part of the test. As more entities become involved then the complexity of testing increases so different testing types have been created. There is an understanding that the time and cost required to complete a DORA for the more complex tests is going to be greater than the historic TIBER-EU engagements.

Solo TLPT

This is the standard test where the FE owns and manages all the systems. It can include cloud infrastructure where the FE is tenanted but does not include the cloud provider. This is essentially the same as the historic TIBER-EU engagements and is likely to be the most common type of DORA assessment.

TLPT with TPSP

Where a TPSP operates, manages or hosts a major part of the FE then they would form at least one scenario within the engagement. The TPSP would be involved in the CT and part of all aspects of the DORA assessment. The decision of what parts of a TPSP are included will be taken at the scoping stage and agreed by the CA and TCT.

Joint TLPT

Where an FE has operations in many countries then these may form a broader test. The decision of how many parts of the organisation will be assessed will be determined by the CA and the TCT from the relevant countries at the scoping stage. FE that have central group services that are used by operations in other countries but each have their own autonomy and regulation is a good example for this type of test. The group services and the individual countries would be a likely scope for the engagement.

Pooled TLPT

A Pooled TLPT is intended for situations where multiple Financial Entities rely on the same critical ICT Third-Party Service Provider (ICT TPSP), such that a compromise of that provider could have a significant impact across those entities. This may include major cloud service providers or other shared ICT providers. Under this

©CREST (International) All rights reserved

model, multiple Financial Entities participate in a coordinated TLPT, with the Competent Authorities and TIBER Cyber Teams working together to oversee the engagement.

As multiple Financial Entities and supervisory authorities are involved, pooled TLPTs are typically more complex than standard engagements. The scope of the assessment, including the participating entities, critical functions and third-party services, is agreed during the scoping phase. DORA does not prescribe a minimum number of attack scenarios for pooled TLPTs; instead, the number, scope and structure of scenarios are determined during scoping, taking into account proportionality, risk, shared dependencies and the objectives of the engagement. Careful consideration of the scope is therefore essential to ensure effective and proportionate testing.

TPSP only TLPT

This is not possible under DORA as the TPSP is not an FE and therefore not directly subject to the regulation. They can choose to perform a voluntary TIBER-EU should they wish to.

©CREST (International) All rights reserved