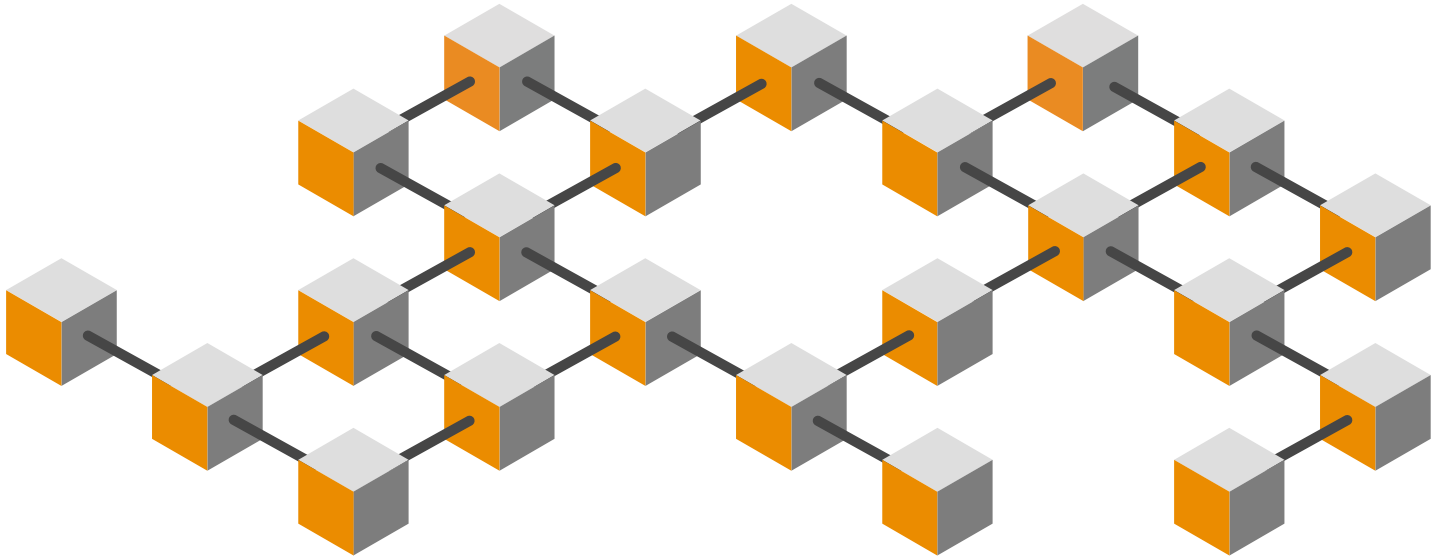
pwc



Digital Operational Resilience Testing

DORA

#5

Digital Operational Resilience Testing (1/2)

DORA requirements

- Financial entities, taking into account their size and respecting their business profile, establish a robust and comprehensive digital operational resilience programme with the aim of assessing ICT incident preparedness, identifying weaknesses and shortcomings. In addition, they shall ensure that such testing is carried out by independent parties, internal or external.
- Financial entities have policies and procedures in place to prioritise and remediate issues identified during testing. They establish internal validation methodologies to ensure that all deficiencies are identified and fully addressed.
- All ICT applications and systems are tested annually.

The Digital Operational Resilience Testing Programme

In order to adequately manage ICT risks, a key priority for financial entities is to **establish a** digital operational resilience **testing programme** to properly **monitor** the effectiveness of **the resilience strategy.**

Digital operational resilience testing must be conducted taking into account the **evolution of cyber threats** in order to understand the levels of exposure to ICT risks to which the financial entity may be exposed.

Financial entities subject **all critical ICT applications and systems** to digital operational resilience testing.

Financial entities conduct digital operational resilience testing **at least annually.**

Financial entities use **independent and qualified parties** to perform these tests.

Financial entities **analyse and integrate lessons learned** from testing into their risk assessment process, with a view to **continuous improvement.**

Digital Operational Resilience Testing (2/2)

DORA requirements

The Digital Operational Resilience Testing Programme involves performing a comprehensive set of appropriate tests, including:

- identification and assessment of vulnerabilities;
- open source analysis;
- network security assessments;
- gap analysis;
- physical security examinations;
- questionnaires and scanning software solutions;
- examinations of the source code (where feasible),
- compatibility tests;
- scenario-based testing;
- performance tests;
- end-to-end testing;
- penetration tests.

Types of Digital Operational Resilience tests

		Typology	Periodicity
1	Vulnerability Assessment	Technological	
2	Wireless Assessment	Technological	
3	Source Code Analysis	Technological	At least annual
4	Penetration Test	Technological	
5	Cybersecurity & Privacy Assessment	Document	
6	Physical Penetration Test	Document	
7	Threat-based Penetration Testing (TLPT)*	Technological	At least three years

* Execution required on specific instructions from the Supervisory Authorities

Types of Technology Testing

1 Vulnerability Assessment

Vulnerability Assessment is the process of **identifying** and **classifying** the **risks** and **vulnerabilities**, in terms of security, of **corporate information systems.**

The objective of this type of security analysis is to identify all potential vulnerabilities in systems and applications.

Roles involved	Test environment
• CISO • IOC	• Internal and/or exposed applications and systems

2 Wireless Assessment

Wireless Assessment is the process of **identifying** the **risks** and **vulnerabilities** of **Wi-Fi networks** deployed by customers.

This process also makes it possible to predict the effectiveness of the security measures taken in the event of an attack or threat.

Roles involved	Test environment
• CISO • IOC	• Internal Wi-Fi networks • Wi-Fi guest networks

3 Source Code Analysis

Source code analysis is a software **auditing method** consisting of using a scanner to **detect** potential **problematic points** in the source code, then manually checking these points for security issues.

Source code analysis is an essential process for **understanding** the **behaviour of applications** as well as potential code transformation.

Roles involved	Test environment
• CISO • IOC	• Internal and/or exposed applications and systems

4 Penetration Test

Penetration Testing refers to a type of test carried out with the aim of **assessing the security** of a technological infrastructure through controlled attempts to compromise and circumvent security controls. **Real attacks** are often carried out on **real** infrastructures and **data,** exploiting vulnerabilities existing within systems, applications and networks or linked to user behaviour.

Most Penetration Tests are concerned **with finding combinations of vulnerabilities** within the system in order to obtain higher levels of access than can be obtained by exploiting a single vulnerability, e.g. by privilege escalation.

Roles involved	Test environment
• CISO • IOC • COO • Control Functions	• Critical assets • Production systems

Types of Organisational and Documentary Tests

5 Cybersecurity Maturity Assessment

A Cybersecurity Maturity Assessment is a **gap analysis** and **risk assessment based** on accredited **frameworks** and **methodologies.** It is performed in order to provide a view of an entity's current **cybersecurity posture.** Its **output** can help an organisation **develop** tactics and strategies to **strengthen security programmes,** aligning them with industry best practices, thereby facilitating compliance with industry standards.

The Cybersecurity Maturity Assessment focuses on the **implementation** of **specific controls** to protect critical assets, infrastructures, applications and data and to outline an effective defence system. In addition, through this type of documentary test it is possible to assess the effectiveness and maturity of internal security policies and procedures.

Roles involved	Test environment
• CISO • IOC • COO • CRO	•

6 Physical Penetration Test

A physical security examination consists of a simulated **attempt** at **intrusion,** i.e. unauthorised access, in order to identify **vulnerabilities** in an entity's **physical access infrastructure.**

This type of test differs from a Penetration Test in that the target is not a technological system or network, but a **physical location.**

However, it is equally important as the digital resilience of an entity is also linked to the degree to which its **physical locations** are **protected** from malicious attackers. Physical security testing can involve **social engineering techniques** to gain access or attacks aimed at gaining access to server rooms or sensitive data.

Roles involved	Test environment
• CISO – Logistics • IOC	• Physical entrances / gates • Building

TLPT Threat-based Penetration Test (1/2)

DORA requirements

- Advanced testing in the form of threat-based penetration tests is carried out every three years.
- The Competent Authorities identify the financial entities that will carry out the threat-based penetration tests in a manner proportionate to the size, activity and overall risk profile of the financial entity, on the basis of the assessment of certain elements, such as the criticality of the services provided and the activities carried out by the financial entity, aspects of financial stability (e.g. systemic character of the entity at national or Union level), specific ICT risk profile and level of maturity of the ICT of the financial entity.

Performing advanced penetration tests

Financial entities required to conduct advanced threat-based penetration tests are selected by the relevant authorities, based on several factors:

Impact

Criticality of the services provided and activities carried out by the financial entity

Stability

Aspects of financial stability, including the systemic character of the entity at national or EU level

Risk Profile

ICT / Cyber relative risk profile

Maturity

Level of maturity of the financial entity's ICT or technological features in question

The periodicity of threat-led penetration tests

TLPTs are **tests** which, because of the **complexity of** the **way** they are **carried out** and the effort (involvement of different teams) involved, need to be carried out **at least every three years.**

The role of the competent authorities

Competent authorities **identify** the financial entities required to **conduct TLPTs in a** manner **commensurate with the size,** activity and overall risk profile of the financial entity.

Following the performance of these checks, financial entities send **documentation** proving that the tests have been carried out, which is **examined** by the competent authorities who, if positive, **validate** the documentation received and issue a **certificate.**

TLPT Threat-based Penetration Test (2/2)

DORA requirements

- Threat-based penetration tests address at least the critical functions and services of the financial entity and are performed on the actual production systems that support those functions.
- Financial entities determine the scope of threat-based penetration testing, based on the assessment of critical functions and services, by identifying the underlying ICT processes, systems and technologies, including functions and services outsourced or contracted out to third-party ICT service providers.

The 6 basic elements of the TLPT

1. **Scoping and Risk Management**
   The entity must implement effective **risk management controls** to avoid potential impacts on **critical** assets or **interruptions** to **critical services**. In addition, it is necessary to define the scope of the test in terms of critical functions and services.

2. **Resourcing**
   It is essential that the entity **carefully** chooses its threat intelligence and penetration testing providers (testers).

3. **Threat Intelligence**
   Threat intelligence providers develop threat profiles containing threat scenarios that help the **Red Team**, responsible for the **penetration testing phase**, to **develop** test cases.

4. **Penetration Testing**
   The Red Team plans and carries out the testing of target systems and services, as defined in the initial scope

5. **Closure and Remediation**
   At the end of the penetration testing phase, the relevant stakeholders **analyse** the **results of** the test with the aim of **implementing improvements** to **enhance** the **digital resilience** of the entity.

6. **Thematic Data**
   One of the objectives of TLPTs is to strengthen the resilience of the financial market in general, which can be achieved by **identifying** and **sharing vulnerabilities** in the sector.

Requirements for Testers

DORA requirements

- Testers must meet certain requirements such as:
  - High degree of suitability and reputation;
  - Technical and organisational skills with specific experience in the field of threat intelligence, penetration testing or red team testing.
- Testers must be certified by an accreditation body in a state.
- External testers must provide an independent assurance or audit report concerning the sound management of risks arising from the execution of threat-based penetration tests. They must also be duly and fully covered by professional liability insurance, including against the risks of negligence and fault.

* ECB opinion of June 42021 on the proposed DORA Regulation
** Tiber-EU Framework, Services Procurements Guidelines

Requirements for testers

The ECB* only recognises tests carried out by independent **third-party providers as valid** tests because they can provide an innovative and unbiased point of view. In addition, external providers may have **more resources** and up-to-date, **state-of-the-art expertise** at their disposal.

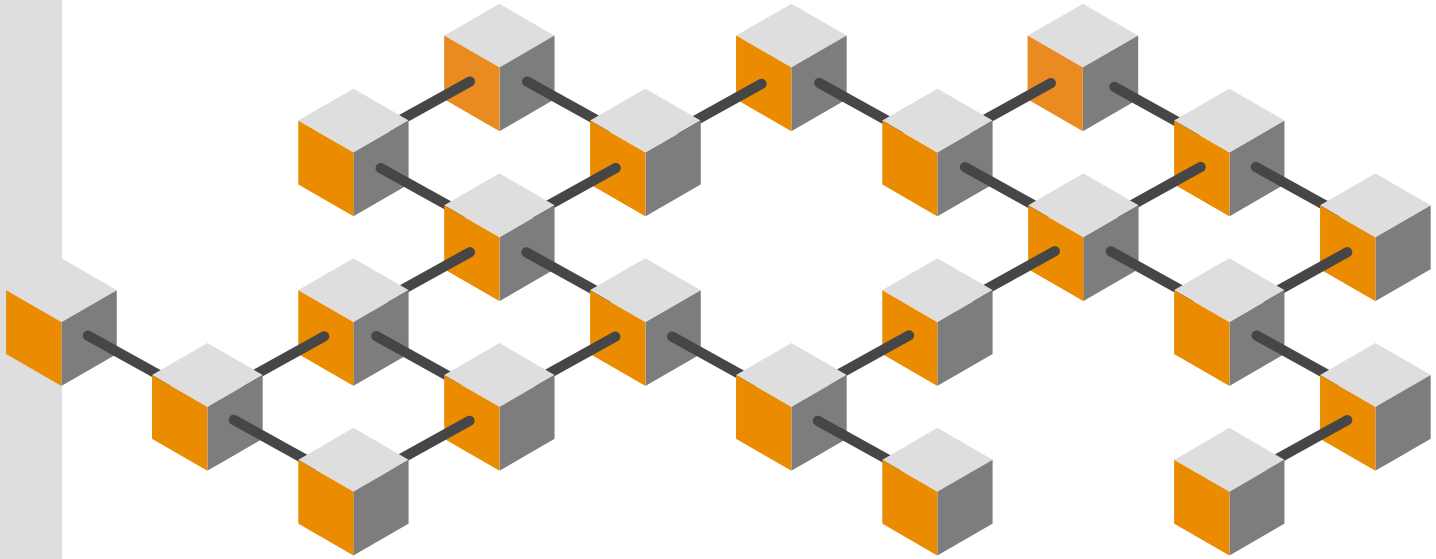
Suitability	Experience	Certifications	Independence	Responsibility
High degree of suitability and reputation	Technical skills and experience	Certification by an accreditation body	Guarantee of independence and sound risk management	Professional liability insurance

Tester certifications

Some of the certifications required of suppliers to deliver services according to the Tiber EU standard**:

	Certification Body	Qualification
Suppliers	ISO	ISO/IEC 27001, ISO/IEC 29147, ISO 30111
	NIST	NIST 800-115 for Information Security
	FIPS	FIPS 140-2-Compliant encryption for data protection
Manager	CREST	CREST Certified Threat Intelligence Manager (CCTIM)
	CREST	CREST Certified Simulated Attack Manager (CCSAM)
	Offensive Security	Offensive Security Certified Expert (OSCE)
Team	CREST	CREST Certified Simulated Attack Specialist (CCSAS)
	SANS Institute/GIAC	GIAC Penetration Tester (GPEN)
	Offensive Security	Offensive Security Certified Professional (OSCP)

Thank you



pwc.com

Contact

Philipp Rosenauer
Director

+41 79 238 6020
philipp.rosenauer@pwc.ch

Claudia Liliane Jung
Senior Manager

+41 79 779 8758
claudia.liliane.jung@pwc.ch

Lorena Rota
Manager

+41 79 305 5540
lorena.rota@pwc.ch

Anna Maria Tonikidou
Senior Associate

+41 79 388 3765
anna.maria.tonikidou@pwc.ch