SUPERVISION DORA UPDATE 5

Getting ready for DORA: Testing of the digital operational resilience

In short This is the fifth edition in a series of AFM publications on the Digital Operational Resilience Act (DORA). This series is intended for all firms that will have to comply with this European regulation from 2025. This edition focuses on the testing of the digital operational resilience. In this way, firms can analyse their current status in this regard and what actions they may need to take to ensure compliance with the Regulation.

1. Introduction

DORA aims to ensure that financial firms have better control of ICT risks and are thus more resilient to cyber threats and ICT disruptions. To that effect, the Regulation details several requirements in the area of ICT, including with regard to testing the digital operational resilience. Firms are already able to analyse their compliance with the DORA requirements in this respect and take action, if needed. They are advised that it is necessary to be in the process of implementation right now in order to be DORA-compliant by 17 January 2025.

The previous editions focused on the DORA requirements for managing ICT risks, including ICT risk for third-party providers, and the management of ICT-related incidents. DORA expects financial firms to take appropriate measures and to set up processes aimed at improving information security and cyber resilience.

To ensure that these measures are adequate, it is important that ICT tools and systems are regularly tested to expose any vulnerabilities and deficiencies. Regularly testing the resilience of ICT tools and systems enables firms to ensure the continuity of critical and important functions in case of any disruptions. Articles 24 through 27 (Chapter IV) of the Regulation describe the requirements for testing the digital operational resilience.

Article 24 describes the general requirements for conducting tests. Among other things, it describes how organisations should set up a testing programme, how often tests should be performed and how findings should be followed up. These requirements apply to all firms subject to DORA, with the exception of microenterprises [1]. Microenterprises are expected to apply a risk-based approach. Article 25 describes the types of tests that can be performed for the testing of ICT tools and systems.

Articles 26 and 27 of the Regulation describe the requirements of advanced testing based on threat-led penetration tests (TLPT), which tests cover several critical or important functions on live production systems. Among other things, these Articles describe the scope of these tests, the role of the supervisory authority and the way to determine which financial firms need to perform a TLPT. They also

1 Microenterprise means 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 €2 million.

set out the requirements for testers for the performance of TLPT. The requirements for TLPT are further elaborated in the Regulatory Technical Standard (RTS)[2]. The RTS describes in more detail the criteria under which firms qualify for TLPT and the requirements for the use of internal testers. The RTS also explains the process of TLPT. This process is based on the TIBER-EU framework. In collaboration with DNB, the AFM has been supervising financial firms in TIBER-tests since 2021[3].

This DORA update offers a more in-depth focus on the general requirements for testing the digital operational resilience and the steps organisations should already be taking to be able to meet DORA. It also discusses the requirements involved in TLPT and the process of such testing

Table 1

Further elaborations	Subject	Completed
RTS for Article 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Already submitted to EC

2 See Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) (afm.nl)

3 See TIBER-NL-programme (afm.nl)

2. Getting started on testing the digital operational resilience

Testing ICT tools and systems

Firms can already start working on:
- Setting up a risk-based programme to test digital operational resilience;
- Implementing the test programme.

Article 24 of the Regulation sets out the general requirements for the performance of digital operational resilience testing. For the purpose of assessing the resilience of ICT systems and services, firms need to establish, maintain and regularly review a testing programme. This testing programme has to be part of the ICT risk management framework[4] and has to include the tests, practices, methodologies and tools regularly applied to assess the organisation's ICT systems, tools and processes. The assessment considers the processes designed to timely detect and solve any ICT-related incidents. Additionally, firms have to perform their own assessment of their ability to detect any vulnerabilities and deficiencies in their digital resilience. Finally, the tests need to provide insight into the extent to which organisations can timely implement remediation measures that minimise the length and impact of a disruption. When conducting testing programmes, firms should consider the evolving landscape of ICT risk, any specific risks to which the financial firms are or might be exposed, and the criticality of ICT systems and services provided.

Organisations are expected to conduct, at least yearly, tests on their ICT systems and applications supporting critical or important functions. These tests can be undertaken by both internal and external testers. It is important to ensure that any potential or actual conflicts of interest are avoided throughout the design and execution phases of the test. Where tests are undertaken by internal testers, financial firms need to take appropriate measures to ensure that the testers have no vested interest in the results of the tests. Financial firms will furthermore need to establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests, and ascertain that all identified vulnerabilities and deficiencies are fully addressed.

Article 25 of the Regulation describes the tests that firms can conduct to test their ICT systems and applications. Firms have to determine which tests are relevant for this purpose in accordance with the proportionality principle[5]. Examples of tests include:
- Vulnerability scans. Vulnerability scans assess the security of ICT systems and tools and identify vulnerabilities, often by means of automated scans;
- Gap analyses, which compare the current performance of the ICT systems and tools versus their desired, expected performance. Based on these analyses, it is possible to determine which systems comply and which do not;
- Assessments of physical security. Consider tests to determine whether people can gain unauthorised access to certain locations, such as offices, data centres, etc;
- Source code reviews, where persons who did not author the code perform the checking before the source code is put into production;
- Compatibility testing: compatibility testing is a type of testing that examines the functionality of the software over multiple environments such as software/hardware platforms, networks, browsers, etc;
- End-to-end testing: this type of testing checks an entire application from beginning to end to verify that all components also operate in real scenarios;
- Penetration testing: this involves testers, often external testers, searching for vulnerabilities in an attempt to gain access to the system.

4 For more information on the ICT risk management framework, see DORA update 3 (Publications (afm.nl))

5 The requirements of Chapter IV of the Regulation have to be applied proportionate to the size and overall risk profile of the firm, and to the nature, scale and complexity of their services, activities and operations.

Abovementioned requirements do not apply to microenterprises. Microenterprises are expected to combine a risk-based approach, by considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing, on the one hand, and the urgency, type of risk, criticality of the ICT system as well as any other relevant factors, on the other hand.

Advanced tests of ICT tools, ICT systems and ICT processes

In addition to the general requirements for testing ICT systems and tools, a number of firms are also subject to additional requirements with regard to testing the digital operational resilience. These firms are required to conduct advanced testing by means of a threat-led penetration test (TLPT) once every three years[6]. TLPT involves extensive testing that mimics tactics, techniques and procedures that are exploited in real life by threat actors such as hackers[7]. It checks the cyber resilience of financial firms in a controlled, firm-specific and intelligence-led manner. Such a test is a more comprehensive type of red teaming, partly owing to the involvement of the supervisory authority.

For the performance of TLPT to be successful, it is important that firms consider this type of testing as an opportunity to learn and to expose any vulnerabilities. In addition, TLPT is resource intensive, which means that it is important that firms dedicate sufficient resources and staff throughout the different phases of the test.

Each TLPT has to cover the critical or important functions of a financial firm, and it has to be performed on live production systems supporting such business functions. For this, firms first need to identify the ICT systems, processes, tools, and services, including those which have been outsourced, that support the critical or important functions. Financial firms then assess which critical or important functions need to be covered by the test. Before the precise scope of the test may be made final, it will need to be validated by the TLPT authority supervising the test. In the Netherlands, the validation will either be done by the AFM or DNB, depending on which supervisory authority issues the licence.

Where ICT third-party service providers are included in the scope of a TLPT, firms must take appropriate measures to ensure the participation of such ICT third-party service providers in the TLPT. If the participation in the TLPT will have an adverse impact on the quality of services delivered by the ICT third-party service provider to organisations falling outside the scope of DORA, the external service provider may be excluded from the scope of the TLPT of the firm. In that case, the ICT third-party service provider designates an external tester for the purpose of conducting a pooled TLPT involving several financial firms to which the ICT third-party service provider provides ICT services. This pooled testing must cover all ICT services supporting critical or important functions contracted to the third-party service provider by the different financial entities.

A number of requirements apply to the testers (or red team) to ensure that the TLPT is carried out correctly. Firms must make use of testers that are certified by an accreditation body in a Member State and/or adhere to formal codes of conduct or ethical frameworks. Testers also need to possess adequate technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red teaming. Finally, testers must be able to ensure the independent performance of the test and the confidentiality of information, such as of test results. When using internal testers, firms must have sufficient dedicated resources to avoid any conflicts of interest and the use of internal testers has to be approved by the TLPT authority supervising the test. The requirements for the use of internal testers are further elaborated in Chapter IV of the RTS.

For the designation of firms that are required to perform TLPT, the TLPT authority decides which financial entities will be designated to perform TLPT. Depending on the regulator granting the license, either the AFM or DNB will be responsible for the designation (and oversight) of TLPT. Some financial institutions may be designated by both the AFM and DNB. In such cases, it may be decided that a joint test will be conducted, involving both regulators. The criteria for identifying firms for TLPT are described in Chapter II of the RTS. The TLPT authority takes proportionality into account. Firms can be identified for TLPT

6 The supervisory authority has the power to increase or decrease this frequency.

7 The TIBER-EU framework was used as a basis for the TLPT requirements in DORA. Also see What is TIBER-EU? (europa.eu).

based on 'hard or quantitative criteria'. This for example includes trading venues having a certain market share at national or European level. Article 2(1) of the RTS describes these hard criteria. Any firms not identified based on the quantitative criteria may still be required to perform TLPT, taking into account their ICT risk profile, systemic character and impact on the stability of the financial sector. More specifically, firms can be identified based on the following (mostly qualitative) factors:

- Systemic character and impact-related factors:
  - The size of the firm;
  - The extent and nature of the interconnectedness of the firm with other financial entities in the financial sector;
  - The importance of the services provided;
  - The substitutability of the services provided;
  - The complexity of the business model of the financial firm;
  - Whether the firm is part of a group using common ICT systems.

- ICT risk-related factors:
  - The risk profile of the firm;
  - The degree of dependence of critical or important functions or their supporting business functions on ICT systems and processes;
  - The complexity of the ICT architecture of the firm;
  - Outcomes of any supervisory reviews relevant for the assessment of the ICT maturity of the financial entity;
  - The maturity of ICT business continuity plans and ICT response and recovery plans;
  - The maturity of the operational ICT security detection and mitigation measures;
  - Whether the firm is part of a group using common ICT systems.

Finally, microenterprises and firms for which the simplified ICT risk management framework[8] applies, are not identified for TLPT. The following section will focus more on the process of TLPT and the different roles of those parties involved in the testing.

Table 2

Further elaborations	Description	Completed
RTS for article 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Already submitted to EC

TLPT process

Chapter III of the RTS outlines a number of requirements related to the test methodology and the TLPT process to ensure that each TLPT is performed correctly. To begin with, firms have to assess the risks associated with the performance of TLPT. Appropriate measures must be taken to prevent these risks from materialising as a result of performing the testing activities. These involve risks relating to:

- granting external parties access to sensitive data;
- failing to meet the requirements related to TLPT;
- crisis/incident management;
- disruptions in critical activities and processes;
- loss of data due to testing activities;
- failing to fully recover any systems affected by the test.

Before any of the testing activities can be carried out, it needs to be clear to everyone involved in the performance of TLPT what their roles are. The authority supervising the TLPT, i.e. the AFM or DNB, must assign a test manager who is to coordinate the testing activities and who has to ensure that all requirements are being met throughout the performance of the test. Additionally, at least one alternate test manager has to be designated who can take over the test manager's tasks if needed. The authority supervising the TLPT is expected to participate in all phases of the testing activities and to provide feedback, validations or approvals where needed.

8 Small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of DORA; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision.

Firms are responsible for having a team of employees involved in the day-to-day management of the test (the control team or white team), with one person designated as team lead. The control team is kept informed of all detections resulting from the TLPT. This relates to any detection resulting from the TLPT by both staff members of the organisation itself or of its third-party service providers. Any follow-up actions for incidents resulting from the test should be taken up by the team itself, and information on the progress of the testing activities should be shared with test managers when requested.

Finally, appropriate measures should be taken to ensure the confidentiality of the TLPT. Thus, the access to information about the TLPT needs to be limited to the control team, the managing body of the firm, the TLPT authority, the providers of threat intelligence and the testers. The threat intelligence providers are external specialists who collect data and analyse actual threats upon which basis they develop realistic scenarios. The testers consist of external or internal ethical hackers (or red team) attempting to gain access to a firm's production systems. The blue team consists of staff members of the firm trying to protect the network and ICT systems against external attack actions. The blue team will not be involved in the test and is thus not informed about the test.

Preparation Phase

As soon as a firm receives a notification from the TLPT authority, it can initiate the preparation phase of the test. During the preparation phase, firms conduct the risk assessment, which examines the risks involved in conducting a test on the production environment of systems that support important and critical business functions. Prior to the start of the test, the TLPT authority also must receive a project charter[9], the contact details of the control team lead and information on the use of internal or external testers. Firms must furthermore share information with the TLPT authority on the communication channels to be used during the implementation of the testing activities and the code name for the test. This information must be shared with the test managers within three months from having received a notification from the TLPT authority. Firms identified by the AFM for TLPT can submit the required reports via the AFM portal[10]. As soon as this documentation has been approved by the test managers, the firm can set up the control team that is to support the team lead in the preparation of the test.

Once the TLPT authority validates the composition of the control team, firms need to determine which critical or important functions are to be included in the scope of the testing activities. In doing so, firms need to consider the importance of the function for the firm and the stability of the financial sector, the exchangeability of the function, the interconnectedness with other functions and the geographical location of the function, among other things. Once the scope of the test has been determined, it has to be approved by the managing body and submitted to the test manager[11]. This report must be submitted no later than six months from having received a notification from the TLPT authority. Once the reports submitted have been approved by the test managers, these can be shared with the testers and the threat intelligence providers. Firms must ensure that both the red team and the threat intelligence providers are contracted before the start of the testing phase.

Testing phase

The testing phase can be subdivided into two components: threat intelligence and red teaming. Following approval of the test by the TLPT authority, the threat intelligence providers have to analyse the firm and identify any threats and vulnerabilities concerning the firm. During this phase, they gather data by identifying cyber threats and existing or potential vulnerabilities that may be exploited during the test. For this step, the threat intelligence providers may consult the control team and the test managers supporting this test. Based on this analysis, the threat intelligence providers will propose a number of scenarios that can be used when conducting the test. The control team lead then selects at least three scenarios based on the threat intelligence providers' recommendation, the input of the test managers, the feasibility of the

9 See Annex I of the RTS for the contents of the project charter

10 DORA update 4 describes the process by which firms can gain access to the AFM portal as of 17 January 2025

11 See Annex II of the RTS for the contents of the scope specification report

proposed scenarios during the performance and the size, complexity and risk profile of the firm. The threat intelligence providers' analysis has to be included in a report and submitted to the test managers[12].

Following approval of the threat intelligence report by the test managers, the testers, i.e. the red team, can prepare their test plan[13]. The test plan includes the tactics, techniques, procedures, and communication channels to be used when conducting the test. Once the test plan has been drawn up, it needs to be discussed with the control team, the test managers and the threat intelligence providers before the control team and the test managers can approve the plan. Following this approval, the testers can start their testing activities. The duration of these testing activities will be proportionate to the scope, scale, and activities, amongst others. However, the test must take at least twelve weeks. During the performance of the test plan, the testers, test managers and the control team meet on a weekly basis to discuss the progress. In case of detection of the testing activities by any staff member of the firm, the control team, in consultation with the testers, will need to take appropriate measures to ensure the secrecy of the test. These measures should then also be shared with the test managers. In case the testers reach the point that continuing the test may lead to serious disruptions in critical or important business functions, the control team lead may decide to suspend the test.

Closure phase

Following the completion of all testing activities, the staff members of the blue team need to be informed about the TLPT that has taken place. Within four weeks from the end of the test, the red team has to submit to the control team a report with information on the test and the results[14]. Subsequently, this report has to be shared with the blue team and the test managers.

No later than ten weeks after the end of the testers' testing activities, the blue team has to submit to the control team a report containing a list of attack actions detected during the test (including log files)[15]. This file should then also be submitted to the test managers. In that same period, the testers and the blue team conduct a smaller test by carrying out a replay of the attack actions on the ICT systems and infrastructure, also referred to as purple teaming. They can then also conduct additional tests that could not be tested during the TLPT. After completion of this smaller test, all parties involved are given the opportunity to provide feedback to each other on the TLPT process.

Once the TLPT authority has assessed and approved the blue team test report and the red team test report, firms will have eight weeks to submit the report summarising the findings and the corrective plans to the TLPT authority[16]. Within that same period, firms also have to provide a remediation plan describing the identified shortcomings, the proposed remediation measures and the prioritisation thereof, a root cause analysis, the staff or functions responsible for the implementation of the proposed remediation measures and the risks associated with not implementing the measures. Finally, after the receipt of the required documents, the TLPT authority provides the firm an attestation confirming that the TLPT was performed in accordance with the requirements.

Table 3

Further elaborations	Description	Completed
RTS for article 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Already submitted to EC

12 See Annex III of the RTS for the contents of the threat intelligence report

13 See Annex IV of the RTS for the contents of the red team test plan

14 See Annex V of the RTS for the contents of the red team test report

15 See Annex VI of the RTS for the contents of the blue team test report

16 See Annex VII of the RTS for the contents of the test summary report

3. Outlook

At this time, the first as well as the second batch of RTSs and ITSs have both been published. The first batch and the second batch have now been submitted to the European Commission for review, after which it is expected to decide on the texts in the third quarter of 2024.

In the meantime, the AFM will continue its preparations for conducting DORA supervision. This is the final edition that addresses the substance of DORA's requirements. The next publication will anticipate the supervision of DORA as of 17 January 2025 as well as other developments. The next edition will be published in the fourth quarter of 2024.

For further elaboration on TLPT in DORA, the following pages can be consulted:

- Digital Operational Resilience Act (DORA) (afm.nl) and
- TIBER-NL-programme (afm.nl)

If you have any further questions, please contact the AFM Business Desk.