

Subject

TIBER-EU Implementation Document TCT-DNB

Payments, Cash & Market Infrastructure
Cyber Resilience & Crisis Management (EN)

Introduction

Since 2016, De Nederlandsche Bank (DNB), has carried out threat intelligence-based ethical red-teaming tests under the TIBER Framework. Since then, TIBER has been adopted by the European Central Bank (ECB) and by financial authorities across the European Union. It has been the foundation for Threat Led Penetration Testing in the Digital Operational Resilience Act (DORA, EU 2022/2554), which imposes obligations on financial entities to assess and enhance their digital operational resilience. These developments have led to an update of the TIBER-EU Framework in 2025, in which the experiences of the past years have been incorporated.

DNB adopts TIBER-EU for the execution of voluntary TIBER testing as well as for mandatory DORA Threat Led Penetration Testing (TLPT). The latest TIBER-EU documentation is available on the ECB’s website ([TIBER-EU](#)).

Date
March 27 2025

Reference
T019-2130844751-4387

Objectives for TIBER

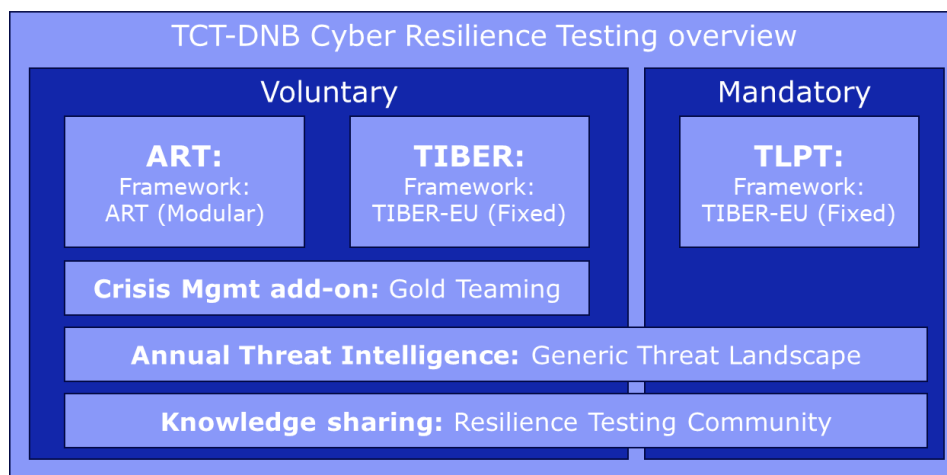
With the adoption of TIBER-EU, to be used for both TIBER and TLPT, DNB aims to:

1. Strengthen the cyber resilience of the Dutch financial sector through the execution of high-quality intelligence led cyber resilience testing.
2. Ensure harmonization in the conduct of TIBER and TLPT through the consistent application of the TIBER-EU framework.
3. Promote collaboration between financial entities and supervisory authorities.
4. Facilitate a resilience testing community, to promote knowledge sharing and enhance the learning experience for financial entities.

DNB will use TIBER-EU for the conduct of:

- DORA TLPT, for the financial entities under its supervision that are identified for TLPT.
- Voluntary TIBER tests, for the financial entities under its supervision, and in special cases, for third parties relevant to the financial sector.

Overview of TCT-DNB cyber resilience testing options



The resilience testing options coordinated by the TCT-DNB can be separated into mandatory testing and voluntary testing.

- Mandatory testing includes DORA TLPT, these tests are based on DORA article 26 and the RTS on TLPT and are carried out using the TIBER-EU framework.
- Voluntary testing is based on either the TIBER-EU framework or the modular ART framework. ART is based on the same principles as TIBER but allows for more flexibility to tailor the tests to the entity's capabilities and learning goals. Additional voluntary testing is also available to entities that are identified for TLPT. Voluntary testing can be used as part of an entity's digital operational resilience testing programme, as mandated by DORA article 24 and 25.

Besides the frameworks for both mandatory and voluntary resilience tests, TCT-DNB also offers additional products supporting these tests:

- Gold Teaming: for voluntary tests it is possible to add a crisis management exercise, based on a threat intelligence-based scenario, as proved to be realistic, during the red team phase.
- Generic Threat Landscape: describes the critical functions, the threat actors and threat scenarios relevant to the Dutch financial sector, which can be used as input for threat intelligence scenarios during cyber resilience tests.
- Resilience Testing Community: financial entities participating in cyber resilience testing activities are invited to join the Resilience Testing Community (RTC). The community aims to further improve the cyber resilience of the financial sector in the Netherlands and to enhance entities' learning experiences.

More information regarding ART and Gold Teaming is available on DNB's website, refer to: [Advanced Red Teaming](#)

The Resilience Testing Community

All financial entities participating in cyber resilience testing activities offered by DNB, are invited to join the Resilience Testing Community (RTC). The community aims to further improve the cyber resilience of the financial sector in the Netherlands and to enhance entities' learning experiences. In this trusted community members can share experiences and tips, discuss developments in testing, and give input for the further development of the different testing regimes and frameworks.

The DNB Test Cyber Team

Representatives from the DNB Test Cyber Team (TCT), will carry out the role of test manager as described in TIBER-EU.

The DNB TCT can be contacted at tct@dnb.nl and you can find us on LinkedIn: [TCT-DNB](#)