# TIBER Short Read – A Joint DNB and BuBa Publication

## When Will My Entity Learn the Most from a TIBER Test?

## Introduction

The financial services sector can be characterized by its large dependency on IT systems. Historically, these systems have been protected against malfunction. In the last decade, they have also been protected against the growing threat of cyber-attacks. In order to make the financial services sector more resilient, the TIBER[1] framework has, since its introduction in 2016, been adopted by the ECB Governing Council and implemented in 13 countries.[2]

TIBER-EU is a framework implemented for critical financial entities whose potential service disruption has a significant societal impact. Additionally, a tested entity should have a base level of cybersecurity measures in place to successfully reap the benefits of such a test. A TIBER test is only a TIBER test if it is accompanied by a TIBER Test Manager from the respective TIBER Cyber Team (TCT), usually located at the respective central bank. TIBER tests are conducted on a voluntary basis in most jurisdictions, although competent authorities and/or central banks might encourage critical entities to undergo such a test.

This short read, designed by De Nederlandsche Bank and the Deutsche Bundesbank, explains when an entity has reached the required level of cyber maturity in order to get the most out of a TIBER test. The following section outlines a number of prerequisites that should be met in order to be able to: (1) test an entity's cyber defence and get tangible – and a manageable number of – findings, (2) implement the remediation plan resulting from the test.

## Prerequisites for a TIBER test

There is no formalised checklist your entity can use to determine whether it has reached an optimal level to start a TIBER test. Entities that have not yet reached a certain level of cyber maturity will likely benefit more from a gradual increase in the level of security testing, making the recommendations more manageable. Once more accessible forms of security testing have been successfully conducted, the following aspects might be taken into account to determine whether your entity is ready for a TIBER test:

- **Your entity should be of critical importance to the lives of citizens and/or the functioning of systemic entities**. Since a TIBER test requires a significant amount of resources, entities undergoing such a test should be of a certain size and/or importance for citizens and/or the functioning of their respective sector, or possess *'crown jewels'*. Without these characteristics, the most skilful actors operating in the digital threat landscape would, in general, be less interested in breaking your defence. The TIBER-EU framework is designed in a way that is sector-agnostic so that TIBER tests are by no means limited to one sector. Tests previously conducted in other sectors have proven the framework's cross-sectoral applicability.

- **The culture within your entity should be open to learning experiences**. Red teaming, especially TIBER, is primarily a learning exercise. In this learning process, it should be acceptable for the blue team (the entity's cyber-defenders) to make mistakes and learn from them. Without a fair level of openness and willingness to learn and improve, a TIBER test will likely be found to be very difficult.

[1] Threat Intelligence-based Ethical Red-teaming

[2] More information about the TIBER-EU framework can be found in a previous short read: link

- **Your entity is highly recommended to conduct traditional red teaming, scenario-based testing or other security evaluation tests before participating in TIBER**. Only external service providers with the highest skill levels are to be used to execute the attacks of a TIBER test. Therefore, a basic cyber maturity should be established within your entity to maximize the learning effect of a TIBER test. Traditional security evaluations such as smaller red teaming tests or scenario-based tests can help achieve such maturity – even if they are not TIBER tests, they might still be performed by following the steps described in the TIBER-EU framework. However, your entity should not shy away from conducting a real TIBER test with your national TCT as soon as you feel ready for it. The TCT can help you to make this decision.

- **In order to conduct a TIBER test, your entity should have sufficient resources and personnel available**. A TIBER test is demanding in terms of resources as well as staffing. It involves both sufficient qualified blue team members (employees involved with your entity's cyber defence) and white team members (employees involved in steering the test as well as risk management). Without a structured, well-functioning blue team, it will be very hard to gain enough learning experience to enhance your entity's cyber defence. Without a properly staffed white team, the safe and efficient conduct of the test might be in jeopardy.

- **If you are interested in conducting a TIBER test, you should have the support of your entity's board**. Support from at least one board member is needed for multiple reasons:
  (1) The board of your entity should take ownership of the entity's cybersecurity and should be sensitized towards related risks and weaknesses.
  (2) TIBER tests are a resource-consuming effort. Therefore, the board should allocate the resources needed to conduct this test.
  (3) Testing on live production systems poses a certain – although very limited – risk to the continuity of business processes and should therefore be authorized by the board as the risk owner.
  (4) TIBER tests will likely result in findings on the capabilities of the cyber defence of your entity. In order to properly follow up on these findings, the respective willingness and budget is required to address shortcomings. Support of your board can ensure that the necessary improvements can indeed be implemented, making the TIBER test a worthwhile exercise.

### Resources required for a TIBER test

The resources needed for a TIBER test can vary greatly depending on your entity's size, scope, the remediation measures resulting from the test as well as additional services procured from service providers. The required resources might fall into the following categories:

(1) Budget needed to procure a threat intelligence provider.
(2) Budget needed to procure a red teaming provider.
(3) The investment of work hours by your white team members and, in regard to the following replay and purple-teaming sessions, by your operational team members.
(4) The investments needed to follow up on the remediation of the test's outcome. TIBER tests identify shortcomings in your cyber defence that might require the procurement of new systems or services to mitigate them.

## Conclusion and outlook

In order for your entity to get the most out of a TIBER test, a number of prerequisites should be met. In addition to having the required criticality and traditional testing experience, your entity should have an open, learning-oriented culture and be able to procure the required resources, personnel and board involvement. Once these requirements are met, TIBER tests are a great tool to evaluate your cyber posture under realistic conditions and increase your defensive capabilities in a very practical way. If you are unsure whether to start a TIBER test, do not hesitate to contact your national TCT, which can assist you in your decision-making.