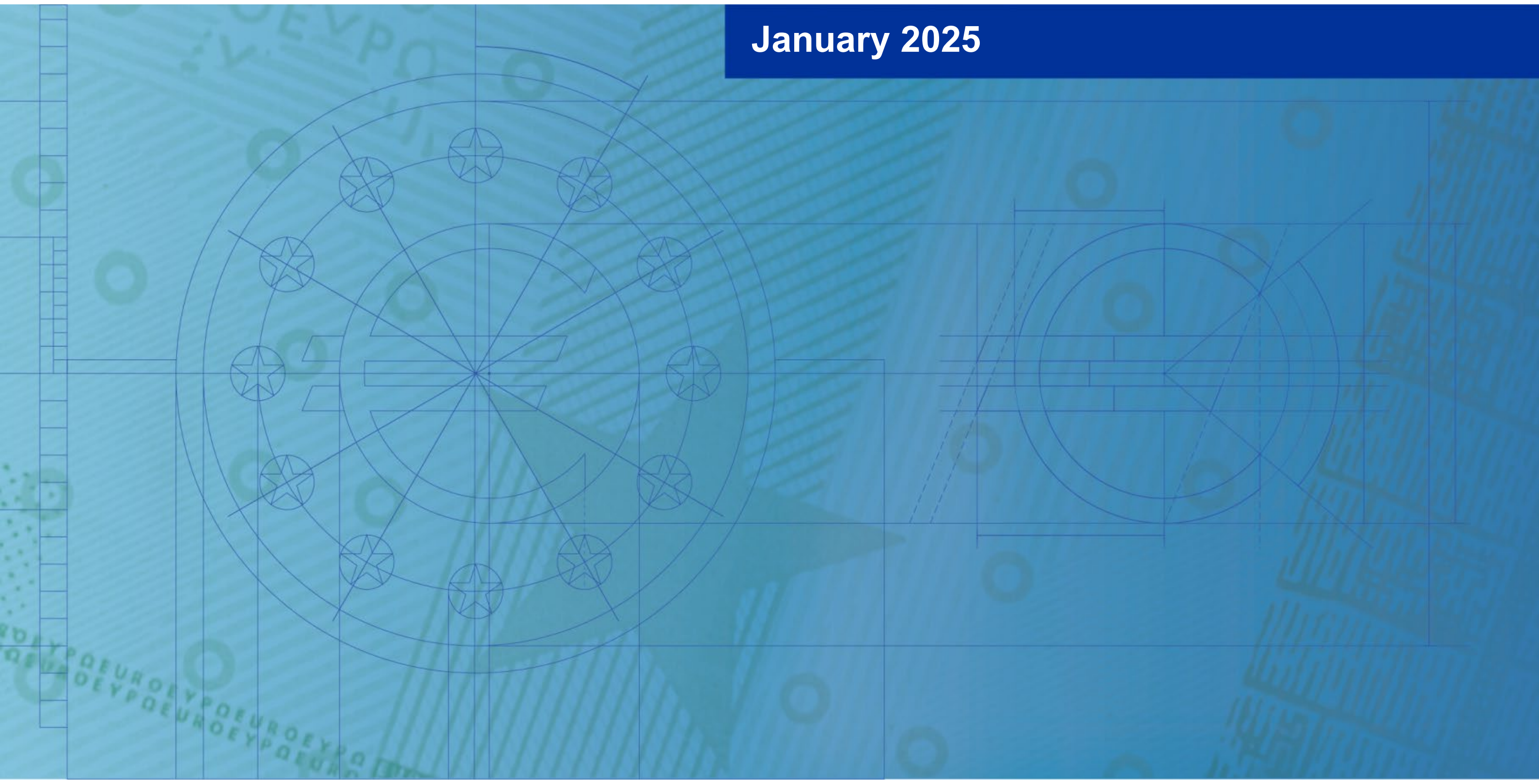
TIBER-EU

Control Team Guidance



January 2025

Contents

1 Introduction

The control team (CT) is responsible for the overall planning and management of the test, in accordance with the TIBER-EU framework. As such, it is responsible for all project management related matters, risk management, procurement and communication to and between the involved stakeholders. The CT must ensure that the TIBER-EU test is conducted in a controlled manner, with appropriate risk management controls in place, whilst maximising the learning experience for the entity. That goal in mind, the CT must closely cooperate with the test manager (TM) from the TIBER authority.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for setting up a CT. It assists in selecting the control team lead (CTL) and CT members by providing relevant selection criteria.

1.2 Target audience

This TIBER-EU Control Team Guidance (CTG) is aimed at the envisioned CTL and the CT members, serves as a practical guide for the TM to assist and challenge the selection of CT members and allows third party providers involved in a TIBER-EU test to select their own respective CT member.

1.3 Location within testing process

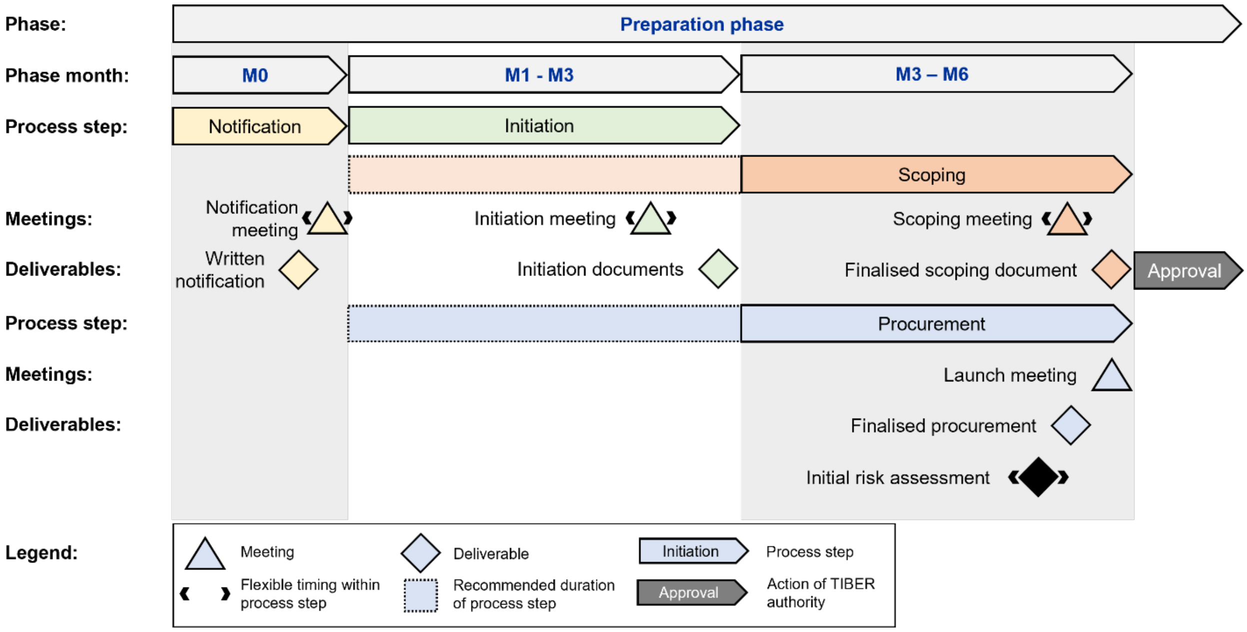
After the receipt of a written notification, the entity shall select a CTL. Once the initiation documents are approved by the TIBER authority[2], the entity will select the other CT members to support in the execution of the test. The final composition and any subsequent changes to the CT have to be validated by the TM.

[1] In addition to the minimum requirements for complying with the TLPT obligations under DORA, this document also includes operational TIBER-EU guidance based on best practices, knowledge and experience from numerous previous tests.

[2] A TIBER authority is any authority under the TIBER framework and/or its national or European implementations, conducting (regulatory) tasks within a TIBER test. When using the TIBER-EU framework for TLPT obligations under DORA, the respective “TLPT authorities” are considered as TIBER authorities for that test.

Figure 1[3]

Preparation phase process overview



[3] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

2 Requirements for setting up the control team

The CT will be responsible for the end-to-end conduct of a TIBER-EU test and managing the separate TIBER phases, to ensure the TIBER-EU test is conducted in a safe and controlled manner. However, the CT must fulfil its duties in close collaboration with the test manager (TM), and should remain in direct contact with the TM throughout the entire test.

2.1 Responsibilities of the control team

The main responsibilities of the CT are:

- Executing the test in compliance with the requirements of TIBER-EU, and informing the management body of the financial entity about the progress of the test and the associated risks.
- Ensure that all the risk management controls are in place and effective, to ensure that the test is conducted in a controlled manner, and that any business impact from the test is within the risk appetite of the tested entity.
- Involvement of all relevant stakeholders, to ensure that critical or important functions (CIF) are included within the prepared Scope Specification Document (SSD) to facilitate a realistic simulation of an actual advanced targeted attack.
- Facilitating the procurement process of the threat intelligence provider (TIP) and external red team testers (RTT) according to the TIBER-EU Guidance for Service Provider Procurement.
- If applicable, evaluate the suitability of internal RTT, ensure that all requirements for internal RTT are, met and approval from the TM is obtained.
- Liaise closely with the TIP/RTT and the TM throughout the lifecycle of the TIBER-EU test.
- Define communications channels and processes, and ensure that information protocols are in place throughout the TIBER-EU test.
- Ensure that the test is executed within the defined scope and provide guidance if the RTT wants to deviate from the agreed scope.
- Be responsible for the timely delivery of all deliverables and decisions to be taken; responsibility remains with the CTL.
- Ensure adequate insights and ability to manage potential escalations arising from the test. The CT has to ensure that there are sufficient arrangements in

place to get informed of actions taken by the blue team (BT), especially given the CT members are usually not formally part of the BT.

- Taking decisions based on subject matter expertise throughout the test.
- Maximise the learning experience for the whole entity, including through conduct of the replay & Purple Teaming exercises.
- Consult with the entity’s Board where needed.

3 Considerations when setting up the control team

The size of the CT depends on the size and complexity of the entity, its organisational structure and its business model (e.g. use of third-party providers). Hence, there is no one-size-fits all. The CT composition is likely to vary from entity to entity, while the various composition options do not alter its responsibilities.

The guiding principle should be that the CT is as small as possible, consisting of just the right people necessary to manage the test.

This implies balancing:

- the required skills to manage an end-to-end test;
- sufficient business and operational knowledge of the entity and its CIFs, systems and processes; and
- the right level of authority to make critical decisions during the test.

The CT might be composed solely of personnel belonging to the entity itself, to other group entities or to third-party providers. The CT must closely cooperate with the TM.

3.1 Control team composition

The following functions or types of personnel should be part of the CT:

- Control team lead;
- subject Matter Experts (SMEs);
- C-Level Member. C-level members are usually included in the CT in an extended composition;
- other needed expertise, e.g. project manager;
- relevant third-party provider(s).

3.2 Composition discussion with the test manager

At the start of test, the tested entity selects a CTL. It is then up to the CTL to select the other members of the CT. The composition of the CT is in principal up to the entity, but the TM should be consulted on the CT composition. The TM is not part of the CT, but will be working closely with the CT during the test. The TM must validate the final composition and any further changes to the CT.

3.3 Multiple jurisdictions

When an entity with presence in multiple jurisdictions is tested under TIBER-EU, the CT composition should take into account the scope of the test, where CIFs and their supporting systems are operated, and relevant people and processes are active. Based on these considerations, the CTL from the entity should determine the most appropriate composition of the CT, comprising of the most relevant people that can ensure a safe and controlled test is conducted. The overall accountability lies with the CTL from the jurisdiction where the TIBER authority is located.

3.4 Control team lead

The Board of the entity should delegate the responsibility for the management of the TIBER-EU test to the CTL, who is responsible for the day-to-day management of the test and the decisions and actions taken by the CT.

The CTL establishes the CT, and has the overall responsibility for the day-to-day management of the test. The CTL is the primary point of contact for all stakeholders. Due to the importance of the role of CTL, a designated back-up should be available at all times.

For the CTL to fulfil its responsibilities during a TIBER-EU test, the CTL needs to have:

- authority and a mandate within the entity to take full control of the testing process;
- direct access to senior management.

3.4.1 Skillset

As the manager of the CT and the TIBER-EU test, the following skills are essential:

- strong project management skills;
- people and process management skills;
- ability to communicate with different levels of staff, from C-level to operational teams;
- ability to work under pressure;
- be pragmatic and decisive.

3.4.2 Experience

In addition to the skills above, there are many areas in which the CTL needs experience and knowledge. If some of the attributes cannot be found in the CTL, these are ideally supplemented by other members in the CT.

The CTL should ideally possess the following experience:

- insight in and deep understanding of the entity and its infrastructure (including its IT landscape and business operations);
- experience working with other relevant departments of the entity (e.g. legal, procurement, communications, IT, business, security, fraud, etc.);
- experience in cyber resilience testing, specifically red team testing;
- experience with crisis management;
- experience with procurement processes, including knowledge of the relevant vendor market;
- general knowledge, specifically the legal aspects, of privacy and security, including ability to identify when the entity's legal department needs to be involved.

3.5 External control team lead

In some circumstances it can be beneficial or necessary to recruit an external CTL.

Given the intrusive and confidential nature of the test, the entity should take precautions like vetting, having the external CTL sign an NDA, and ensure that no sensitive data is retained after the test has concluded. If the external CTL is procured from a specialist external provider, the entity should carry out the required due diligence on this person and/or the company the CTL is hired from, ensuring the right skills, expertise, qualifications, experience and security measures to manage a TIBER-EU test.

Any such arrangements should be formalised through contracts. To avoid any conflict of interest, the external CTL cannot be employed by the TIP or RTT procured for the TIBER-EU test at the same time. The TIBER-EU Guidance for Service Provider Procurement provide further guidance on the principles of procurement.

3.6 Skills and experience of the control team members

The other CT members, or SMEs, should also have certain skills and experience to make sure they are able to fulfil the tasks of the CT. The specific skills and experience are as follows:

- extensive and specific knowledge of business processes and applications within an entity;
- extensive knowledge of the IT landscape, including the security setup of the entity;

- sufficient risk management knowledge;
- sufficient experience in project management;
- experience in cyber resilience testing, including red team testing;
- sufficient up-to-date knowledge of tactics, techniques and procedures (TTP) used by cyber threat actors.

Not every member needs to possess all of the above-mentioned skills and experience, but these should be met by the CT as a whole.

3.6.1 Subject matter experts

The SMEs should have a broad range of specific knowledge, expertise and experience pertaining to the entity and its operations, so that they can provide the requisite information and insight during the test. This will allow the CTL to make the appropriate risk-based decisions. The number of SMEs that make up or extend the CT will vary from entity to entity. SMEs with the broadest range of skills and knowledge should be selected, to limit the number of SMEs involved in the CT.

3.6.2 C-Level member

The C-level member (typically the COO or CIO, CTO CISO, or equivalent) is the most senior individual on the CT, and acts as the escalation point during the test. Although the C-level member is unlikely to be the CTL or have an active and resource-intensive role during the test, their ad-hoc presence on the CT will allow the CTL to escalate matters to the decision-makers in full confidentiality.

In any multi-jurisdictional test of group entities, the C-level member should come from the parent entity. Based on the level of involvement of third-party provider(s) in the test, the CT may include representative of the third-party providers(s); in such case, a C-level membership is encouraged (see also par. 3.6.4).

3.6.3 Other needed expertise

During the test, specific subject matter expertise might be needed. This includes, but is not limited to, procurement or legal expertise. While these SMEs will not be day-to-day members of the CT, they should be informed about the high level process of the TIBER-EU test and the need for secrecy. Such SMEs, used on an ad-hoc basis, may be requested to sign a non-disclosure agreement (NDA) to ensure confidentiality.

3.6.4 Third-party service provider(s)

If the entity being tested outsources part of its CIFs or other parts of the potential scope of the test to one or multiple third-party providers, the third-party provider(s) can be included in the CT.

It is advisable for the CTL to have an early discussion with a trusted contact from the third-party provider(s). This can be done in the early stages of the test, to indicate the intention to include third-parties/party in the test. The potential participation should be confidentially discussed with high-level management at the third-party provider. The same conditions of confidentiality apply to the third-party service provider(s) as to the entity itself. A small number of staff from the third-party service provider(s) can join the CT, depending on the defined scope of the test. These staff should have detailed knowledge about the systems that the entity uses at the third-party service provider(s).

One of the staff members from the third-party service provider(s) should be the primary point of contact for the CTL to liaise with. Regardless of the involvement of third-party service providers in the CT, the entity being tested remains accountable for the overall test.

3.7 Control team governance

The CT must operate separately and independently from the TIP, RTT and the BT.

The CTL can make decisions that have a significant impact on the test and potentially on the continuity of the CIFs of the entity. Therefore, the entity must ensure that the governance arrangements around the CT are well-considered and robust.

If circumstances require, the CTL can consult senior management (e.g. COO or CISO) to address any issues regarding business continuity of the entity or the continuity of the test. However, any such consultation must be conducted via secure communication channels to ensure the conduct of the test remains secret and confidential.

3.8 Time resources

During all the TIBER-EU test phases, the CT members must be able to dedicate enough time to their respective roles.

Figure 1 displayed below gives an indication of how much time is likely to be spent by the CTL and the other members of the CT during the different phases of the TIBER-EU test. The amount of time spent will differ per test, based on the size of the entity, the scope, the duration of the red team test and the experience of the different people involved.

Table 1
Indication of time resources for the control team

Test phase	Hours spent by CTL	Hours spent by each member of the rest of the CT
Preparation phase 24 weeks	4-8 hours per week	2-4 hours per week
Test phase TI 4-6 weeks	8-16 hours per week	4-8 hours per week
Test phase RT 14-15 weeks	10-30 hours per week	8-16 hours per week
Closure phase 18 weeks	8-12 hours per week	4-8 hours per week

3.9 Managing escalations

If actions taken by the RTT are detected during the red teaming phase, it is likely that the BT will treat them as a real-life cyber-attack and escalate corresponding incidents accordingly.

Escalation is a key part of the test, as the TIBER-EU test also aims to evaluate the entity's detection and response capabilities. However, just like all other parts of the test, it needs to be controlled. For this reason, it is important for the CT to manage all possible escalation paths within the entity. The CT should only intervene and stop an escalation if it will have an unwanted business impact or will involve external parties where this is not feasible.

An example of an uncontrolled escalation is the shutdown of critical servers by the BT to stop the attack, an incident being reported to the supervisor/overseer and/or that a police report is filed. In such cases, the CTL should intervene and pause the test, and deal with the escalation, while disclosing as little information as possible in order for the test to continue.

3.10 Confidentiality and non-disclosure agreement

To maximise the learning experience of the TIBER-EU test, no one outside of the CT should be informed about the test. If the BT is informed about the TIBER-EU test, the integrity of the test will be compromised and the entity will not learn about its capacity to detect and respond to unexpected cyber-attacks. In the case that the entity and/or the CT inappropriately discloses details of the test to the BT, the test attestation may be withheld.

However, conducting such intrusive tests secretly can be difficult. Furthermore, it may prove to be problematic for the CT members to conduct their daily responsibilities without raising suspicion. In such cases, as a form of protection for the CT members and to ensure that confidentiality is kept, the CT members should sign a confidentiality or non-disclosure agreement (NDA) at the inception of the TIBER-EU test.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).

PDF ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-N
HTML ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-Q