EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Test Summary Report Guidance

January 2025

Contents

1 Introduction

The Test Summary Report (TSR) provides an overview of the entire TIBER test. The key purpose of the TSR is to provide the senior management of the entity and authorities with a sanitised, high-level overview of the TIBER test. **It should not contain detailed technical information and findings regarding the weaknesses and vulnerabilities identified during the test.** Furthermore, the TSR should provide an executive summary that is understandable to senior management, presenting the overall test scope, process and the core conclusions.

The TSR should be read in close comparison with the Remediation Plan (RP), which describes the mitigations planned by the financial entity to address vulnerabilities identified during testing. The TSR serves as a test overview to stakeholders not actively involved in the testing. In contrast, the RP is a document assisting the financial entity in planning its remediation efforts as well as respective supervisors or overseers in following up on those mitigations.

This guidance covers the TSR, taking into account the special nature of these tests as a self-learning experience.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for the content and format of a TIBER-EU TSR. It also aims at providing guidance on important aspects to be considered during the drafting of the report.

1.2 Target audience

This TIBER-EU Test Summary Report Guidance is mainly aimed at the control team (CT) creating a TSR in the scope of a TIBER test. Beyond that, it is useful to read for all stakeholders of a TIBER engagement to understand the nature of its content.

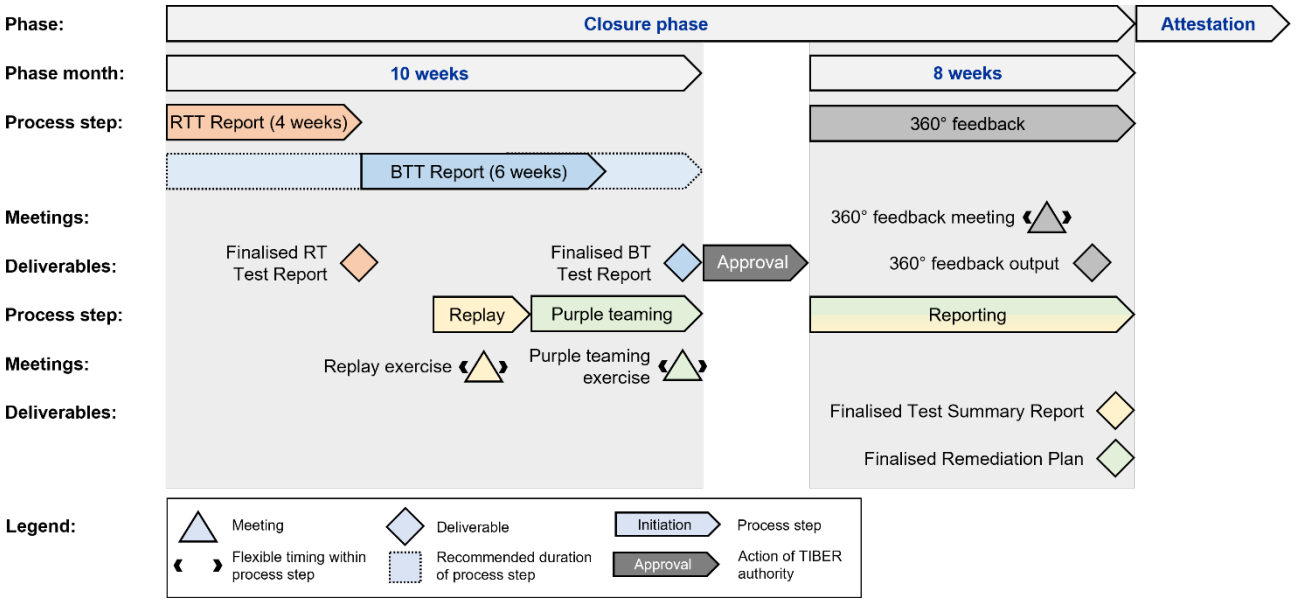
1.3 Location within testing process

The TSR is to be drafted in the reporting process step of the closure phase, after the replay and purple teaming (PT) exercises have been concluded.

[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.

Figure 1[2]

Drafting the Test Summary Report in the reporting process step



[2] 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 Required content of the Test Summary Report

The TSR shall include information on at least the following:

- the parties involved;
- the project plan;
- the validated scope, including the rationale behind the inclusion or exclusion of critical or important functions (CIFs) and identified ICT systems, processes and technologies supporting the CIFs covered by the TIBER-EU test;
- selected scenarios and any significant deviation from the Targeted Threat Intelligence Report (TTIR);
- executed attack paths, and used tactics, techniques and procedures (TTP);
- captured and non-captured flags;
- deviations from the Red Team Test Plan (RTTP), if any;
- blue team (BT) detections, if any;
- if applicable, purple teaming in testing phase, and the related conditions;
- leg-ups used, if any;
- risk management measures taken;
- identified vulnerabilities and other findings, including their criticality;
- root cause analysis of successful attacks;
- high level plan for remediation, linking the vulnerabilities and other findings, their root causes and remediation priority;
- lessons derived from feedback received.

3 Considerations when drafting the Test Summary Report

3.1 Background information

The entity should provide background information on the end-to-end test conducted. When drafting the report, this section should include the following information:

- The authorities and other stakeholders involved throughout the test.
- The names of the threat intelligence provider (TIP) and red team testers (RTT) that conducted the test.
- The project plan and timelines of the end-to-end test.
- The third-party service providers included in the scope of test, if applicable.

3.2 Scope

In this chapter, the entity may use the agreed TIBER-EU Scope Specification Document (SSD) to provide a concise overview of the scope of the test.

The validated scope should be included in the TSR, including the rationale behind the inclusion or exclusion of CIFs and identified ICT systems, processes and technologies supporting the CIFs covered by the test.

3.3 Attack scenarios

In this chapter, the entity should use the TTIR and the RTTP to summarise the attack scenarios that were employed during the red team test.

In this chapter, the entity should summarise:

- the key points from the TTIR, providing any high-level issues that were raised by the TIP regarding the entity;
- the selected scenarios and any significant deviation from the TTIR;
- the captured and non-captured flags, including any leg-ups that were used;
- the specific attack scenarios that were developed by the RTT;
- the risk management controls that were applied in advance and during the test;
- the executed attack paths and TTPs used;

- any deviations from the RTTP.

The entity should ensure that the summary in this chapter clearly links the agreed CIFs, scope, flags, and objectives to the final attack scenarios.

The reader of this chapter should have a clear and high-level understanding of the threat actors that are likely to target the entity, their motivations, intent, goals and modus operandi, and how they would seek to attack the critical or important functions of the entity and achieve the flags and objectives in real life.

Finally, the reader should gain a clear assurance that the CT and RTT had put in place adequate risk management controls, to ensure that the test was conducted in a controlled manner.

3.4 High level findings, recommendations and remediation

This chapter is the most sensitive part of the TSR, and therefore it is critical that the entity takes due care when drafting it. The chapter should not contain detailed technical information and findings regarding weaknesses and vulnerabilities, as information at that level of detail is highly sensitive and for the entity only. At the same time, it is important that the entity is able to provide enough detail to demonstrate the key findings from the test, recommendations made, and remediation actions agreed, as well an insight on unexpected difficulties and failures in the attack phase.

The entity should use information from the Red Team Test Report (RTTR) and the Blue Team Test Report (BTTR), as well as important information obtained from the replay and PT exercises, to inform this chapter. Based on this information, the entity should specifically include the following in this chapter:

- provide a high-level timeline of the test and an overview of the scenarios tested (including references to mimicked threat actors) and context of the successful and unsuccessful attack methods employed;
- any action by the BT of the entity affecting the test;
- highlight the main findings, vulnerabilities (based on criticality) and possible root causes based on the attack methods used;
- highlight the positives from the test, notably any strong control areas that the RTT were unable to circumvent;
- any BT detection identified during RTT activities;
- provide the views of the BT and their post-test reflections;
- give insight into the main categories of recommendations to address the findings and their root causes;
- note any significant observations and exceptions in the test;

- any insight from the RTT on the cybersecurity posture of the entity;
- limited purple teaming (LPT) conducted in testing phase, and the related conditions;
- lessons derived from feedback received.

4 Drafting format

The TIBER-EU TSR might be drafted in any preferred format, provided that all required information is included. All content that needs to be provided in order to complete this document is indicated in Chapter 2.

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