EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Guidance for the TIBER-EU Test Summary Report

August 2020

Contents

1 Introduction

1.1 Purpose of this document

Following completion of the replay and the 360-degree feedback workshops, the entity should draft its Test Summary Report. The Test Summary Report summarises the overall test process and results (including the Remediation Plan) and should draw on the test documentation, such as the Red Team Test Report, the Blue Team Report, the Target Threat Intelligence (TTI) Report, the Red Team Test Plan and the Remediation Plan.

The entity must share the Test Summary Report with the lead authority, and may share it with other relevant authorities. The signed attestation and the Test Summary Report are the two key outputs from the test, to demonstrate that the entity has conducted a TIBER-EU test that has been recognised by the lead TIBER authority, and both documents form the basis for mutual recognition amongst other relevant authorities. Following the completion of the test, if a relevant authority seeks assurance that the entity conducted a recognised TIBER test, the entity may share the Test Summary Report and attestation with the relevant authority. The relevant authority should take these outputs into consideration, to avoid requiring the entity to conduct another TIBER test immediately.

The Guidance for the TIBER-EU Test Summary Report aims to provide entities undertaking a TIBER test with a standardised approach and structure for producing the Test Summary Report. The key purpose of the Test Summary Report is to provide authorities with a sanitised, high-level overview of the TIBER test. **It 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. It is critical that this report is highly sanitised.** Furthermore, the Test Summary Report should be drafted in language that is accessible to senior management, providing a sufficiently account of the end-to-end test, its conclusions and the way forward for the entity to improve it cyber posture.

It is clear that there will be several possible iterations of the Test Summary Report, and the final Test Summary Report should be fully accurate and reflective of the overall end-to-end conduct of the test. The Test Summary Report has to be agreed by the White Team of the tested entity and by the TIBER Cyber Team (TCT). For more detail on the overall processes in a TIBER test, please consult the TIBER-EU Framework[1] and related TIBER documentation, and the relevant TIBER-XX Implementation Guides.

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

1.2 Who is this document for?

This TIBER-EU Guidance for the TIBER-EU Test Summary Report is aimed at:

- The entity undertaking the TIBER test;
- Threat intelligence (TI) provider and red team (RT) provider.
- TIBER Cyber Teams (TCTs) involved in the TIBER test;
- Lead authority; and
- Other relevant authorities.

1.3 Structure of this document

This document is structured as follows:

- Section 2: Background information;
- Section 3: Scope;
- Section 4: Attack scenarios; and
- Section 5: High level findings, recommendations and remediation.

Due to the sensitive nature of the information contained within the TIBER-EU Test Summary Report, once complete, it should be handled and treated as highly confidential and stored in a manner commensurate with this classification (e.g. Traffic Light Protocol Amber).

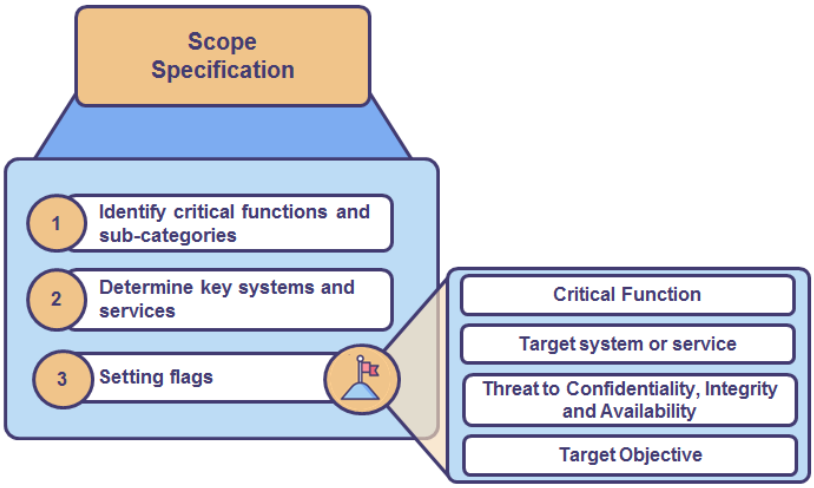
2 Background information

In this chapter, the entity should provide background information on the end-to-end test conducted. This section should include the following information:

- The TIBER authorities (lead and relevant) involved throughout the test;
- The names of the TI and RT providers that conducted the test;
- The third-party service providers included in the scope of test, if applicable;
- The timelines of the end-to-end test; and
- Confirmation that the test was conducted in line with the TIBER-EU Framework and that an attestation has been signed accordingly.

3 Scope

The entity should use the final and agreed TIBER-EU Scope Specification document as inspiration for this chapter in the Test Summary Report. The core of the Scope chapter is to provide the reader with a concise overview of the scope of the test. When agreeing the Scope of the test, the entity underwent the following conceptual process:

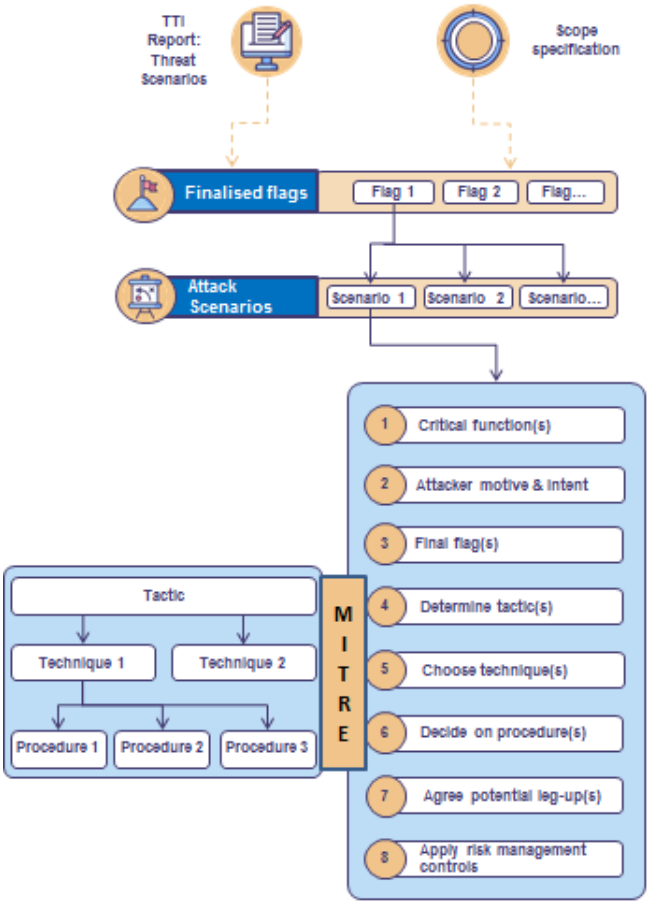


This chapter should summarise the critical functions and sub-categories that the entity included in the scope of the test; the justification for their inclusion; the key systems and services that are used to deliver the critical functions; and the flags that were finally set for the test. When listing the flags, the entity should also cite the objectives of the flags, i.e. the specific attempts to compromise the Confidentiality, Integrity and/or Availability (CIA) of the disclosed systems and services. As a summary, the entity may tabulate the chapter with the information above, as follows:

Critical function *(sub-category)*	
Target System / Service name	
Information Assurance threat category (Confidentiality, Integrity, Availability)	
Description of system/service function	
Objective - i.e. testing activity required to demonstrate compromise (e.g. Exfiltration, Insertion, Privilege Escalation)	

4 Attack scenarios

In this chapter, the entity should use the TTI Report and the Red Team Test Plan to summarise the attack scenarios that were employed during the red team test. When developing the attack scenarios, the RT provider used the following conceptual model:



In this chapter, the entity should summarise: the key points from the TTI Report, providing any high level issues that were raised by the TI provider regarding the entity; the specific attack scenarios that were developed by the RT provider; the leg-ups that were agreed; and the risk management controls that were applied in advance and during the test. The entity should ensure that the summary in this chapter clearly links the agreed critical functions, 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 and modus operandi, and how they would seek to attack the critical functions of the entity and achieve the flags and objectives in real life.

Finally, the reader should gain a clear assurance that the White Team and TI/RT providers had put in place adequate risk management controls, to ensure that the test was conducted in a controlled manner.

5 High level findings, recommendations and remediation

This chapter is the most important, and also the most sensitive part of the Test Summary Report, and therefore it is critical that the entity takes due care when drafting this chapter. It 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 final Red Team Test Report and the Blue Team Report 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 leg-up or allowance made by the White Team of the entity undergoing the test to facilitate the test and/or action by the Blue Team of the entity affecting the test;
- Highlight the main findings (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 RT provider was unable to circumvent.
- Provide the views of the Blue Team and their post-test reflections;
- Give insight into the main categories of recommendations to address the findings and their root causes;
- Note any significant notable observations and exceptions in the test; and
- Any insight from the RT provider on the cybersecurity posture of the entity.

The chapter should also set out, at a high level, the Remediation Plan that the entity has agreed to implement. The Board of the entity is accountable for the Remediation Plan. The Remediation Plan should have been finalised prior to the Test Summary Report, following the Replay, and have been approved by the relevant overseer/supervisor. In the Test Summary Report, the entity should include the following information related to the Remediation Plan:

- Who has overall ownership of the Remediation Plan;

- List of findings by criticality and assigned ownership for each;
- High level action plan; and
- Timeframes and closure dates to remediate the findings based on their criticality.

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