TIBER-NL

Format TIBER Test Summary

February 2022

Contents

1. Introduction

1.1. Purpose of the Test Summary

This format has been developed by the TCT (TIBER Cyber Team) from the Dutch Central Bank in cooperation with the Dutch entities taking part in the TIBER program and based on input from the EU TIBER knowledge centre. It will be periodically reviewed based on new insights.
The format mentions the topics to be summarised and gives guidance on what known information already available in other documents can be used. The level of detail to be added is up to the Dutch entity.

NOTE: Although sharing valuable details and actionable advise increasing the cyber resilience of the financial sector is encouraged, 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.

The purpose of the Test Summary is to serve:

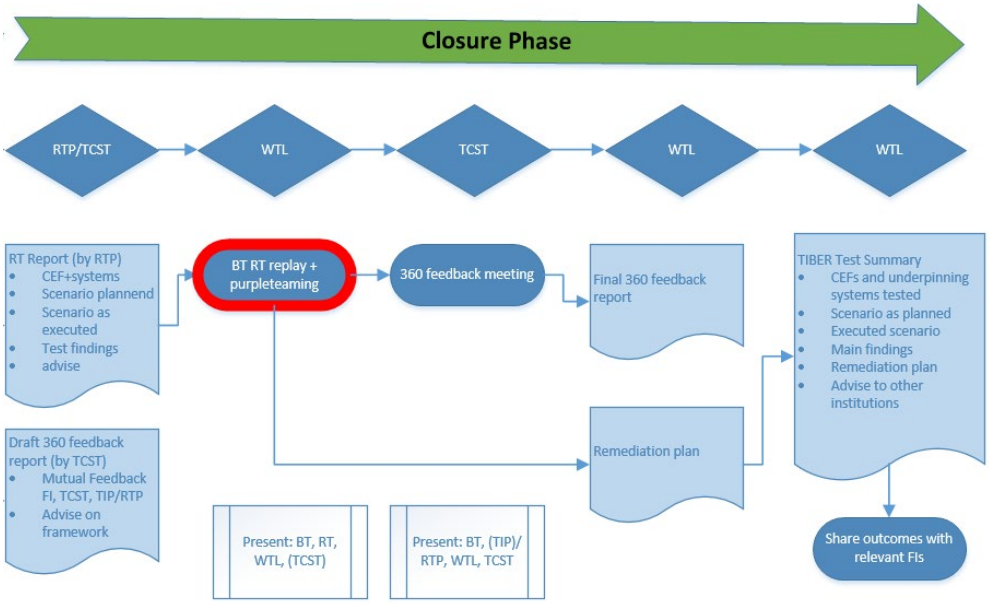
- as mutual recognition for an entity located in more than one jurisdiction;
- to inform the supervision department related to the entity;
- to facilitate analyses by the TCT on sector trends and learnings. The TCT aims to use the outcomes of tests for broader analysis of best practices that it can serve back to the TIBER-NL community;
- as a means to facilitate learning from the test by other entities in the TIBER community;
- as an overview of the test for later reference by the entity.

The 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;
- Entities part of the national TIBER program;
- Other relevant authorities.

1.2. Requirements

The WTL is responsible for delivering the Test Summary. The document will be shared with the TCT and could also be shared by the entity with the other entities within the TIBER community. The WTL finalises the document after the 360 feedback meeting.



The Test Summary is based on documentation delivered during the test process, such as the Scoping document (CF's), the Targeted Threat Intelligence (TTI) report, the Red Team (RT) Test Plan (scenarios planned), the RT report (scenarios executed and main findings), the Remediation Plan (RMP) followed by a final advice to other TIBER participants.

The TIBER Test Summary consists of three main elements:

1. A debrief to prove the TIBER test met the TIBER standard by successfully following the TIBER test process, and meeting the minimum requirements for each phase;
2. A complete overview of the test;
3. Advice to other TIBER participants.

1.3. Legal disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

All TIBER parties will exchange information using the Traffic Light Protocol (https://www.us-cert.gov/tlp).

2. Debrief

Include here the TCT opinion about the complete test, as explained during the board meeting, to confirm whether the TIBER test process was followed successfully and all documented output as shared with the TCT, met the minimum requirements. This text will be provided by the TCT to the WTL.

For example:
<The TCT confirms all required TIBER test phases and its sub activities have been applied correctly. Output as delivered during the test complies to the TIBER Framework, its required guidelines and formats. No (insuperable) omissions have been observed and therefore this test has been debriefed as a valid TIBER test.>

When omissions have been observed, describe in what phase and why it was an omission, what was done and explain the impact on the test results.

3. Complete overview of the test

3.1. Scope

Give a short description of the organisation, its Critical Functions (CF's) and underpinning systems and services. Please re-use the information from the Scoping Document as defined earlier in the TIBER process.

Please include elements that are crucial for the understanding of the total TIBER test, such as:

- The organisation's function and main characteristics;
- Geographies concerned with the delivery and use of the targeted CF's;
- Brands of the operating company involved;
- Third parties involved in the delivery of the targeted CF.

3.2. Targeted Threat Intelligence

This section gives an overview of the main Target Threat Intelligence findings. It includes the main finding of the business overview form an intelligence perspective, the threat actors deemed most relevant and a justification of why they are most relevant and findings on the digital presence. Also this section gives a reflection of the high level scenarios produced by the Threat Intelligence Provider, including the mapping to the MITRE ATT&CK Framework.

3.3. Attack scenarios

The Test Summary is used as a basis for adding the test to the scenario overview that is collected in TM for later reference by the entity's blue team/internal intelligence team/internal red team and other security professionals which the entity granted access to TM.

3.3.1. Test Plan Scenarios

Based on the Targeted Threat Intelligence and the CFs, three scenarios (1, 2 and x) have been *planned* and described by the Red Team Provider using the MITRE ATT&CK

Framework. These scenarios should be documented (copied from the RT Test Plan) in this paragraph.

3.3.2. Scenarios executed

This paragraph highlights scenarios as *executed* during the RT test. The executed test scenarios can differ from the planned test scenarios, for example the planned techniques, tools or procedures (TTPs), a leg up could have been given or other unforeseen deviations which can be found in the Red Team Test Report. As in the previous paragraph, these final executed test scenarios are described using the MITRE ATT&CK Framework. These scenarios should be documented (copied from the RT Test report) in this paragraph.

3.4. High level findings and recommendations

This paragraph is the most sensitive part of the Test Summary Report. It is therefore critical that the entity takes due care when drafting this paragraph, ensuring that no sensitive or overly technical details are revealed, which may compromise the security of the entity. 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.
The entity should re-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:

- 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;
- Any insight from the RT provider on the cybersecurity posture of the entity.

3.5. Remediation plan

The chapter should also set out, at a high level, the Remediation Plan that the entity has agreed to implement. This should include the following information:

- Who has overall ownership of the remediation plan;
- List of findings by criticality and assigned ownership for each;
- High level action plan;

- Timeframes and closure dates to remediate the findings based on their criticality.

4. Advise to other TIBER participants

The goal is to not only learn from a TIBER test per entity, but to also learn from TIBER tests by others. In order to facilitate this learning, please share whatever advise you have to other entities regarding mitigations, best practices etc. apart from what is mentioned in the former chapter. For your audience think of other WT's, CISO's, Blue Teams and intelligence teams.

5. Metrics

<this chapter will be added as soon as the proposal incl. best practices for metrics has been shared and approved by the TIBER community.