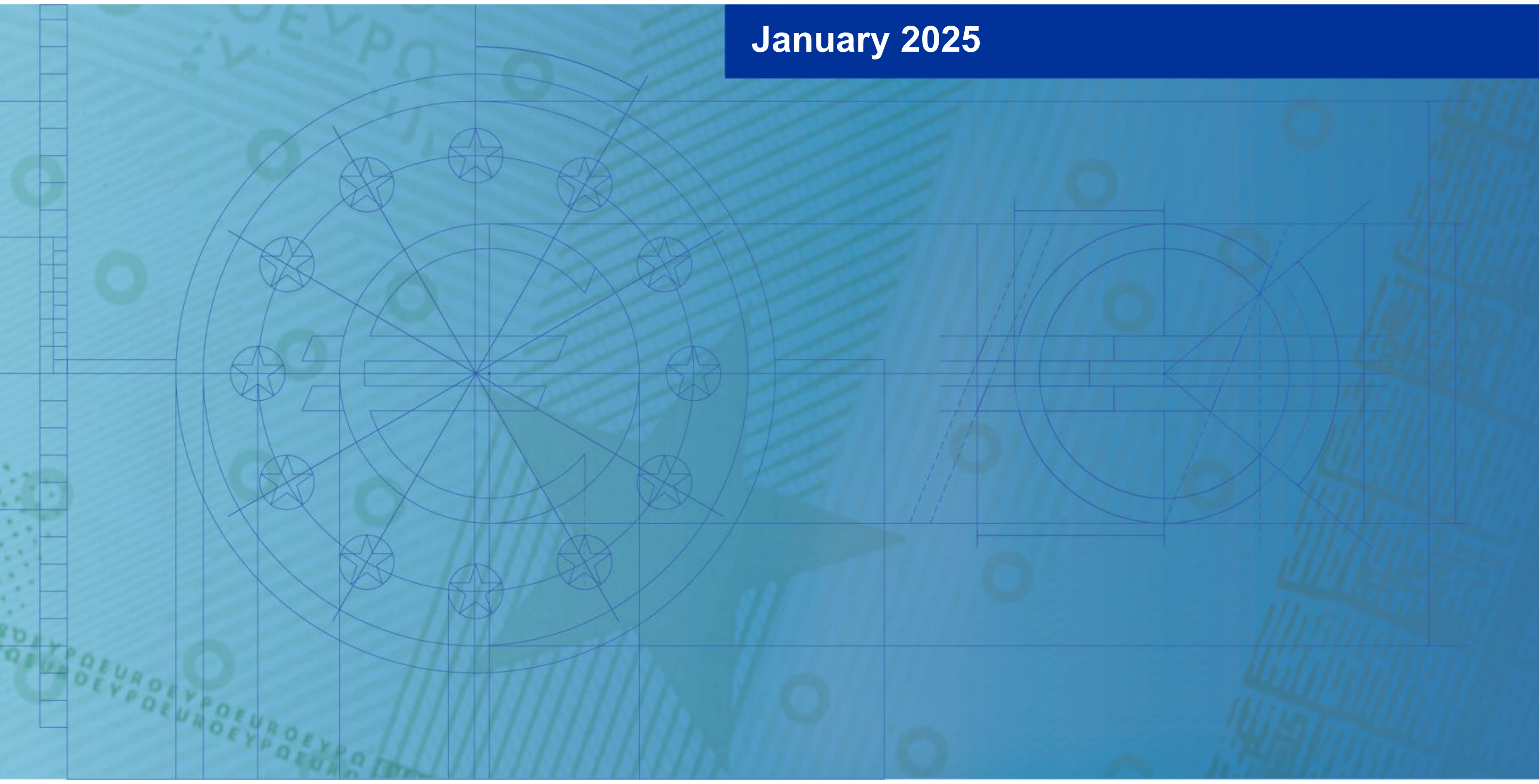
EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU

Red Team Test Report Guidance



January 2025

Contents

1 Introduction

The Red Team Test Report (RTTR) summarizes the test conduct and its results on a detailed technical level. As such, it includes all the information about all attack actions performed by the red team testers (RTT), weaknesses identified and detections by the blue team (BT) as well as specific analyses of root causes and recommendations for remediation and improvement. It therefore serves as a basis for all the activities conducted during the closure phase.

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 RTTR. It also aims to provide guidance on important aspects to be considered during drafting.

1.2 Target audience

This TIBER-EU RTTR Guidance is mainly aimed at the RTT involved in the testing of the financial entity creating a RTTR 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.

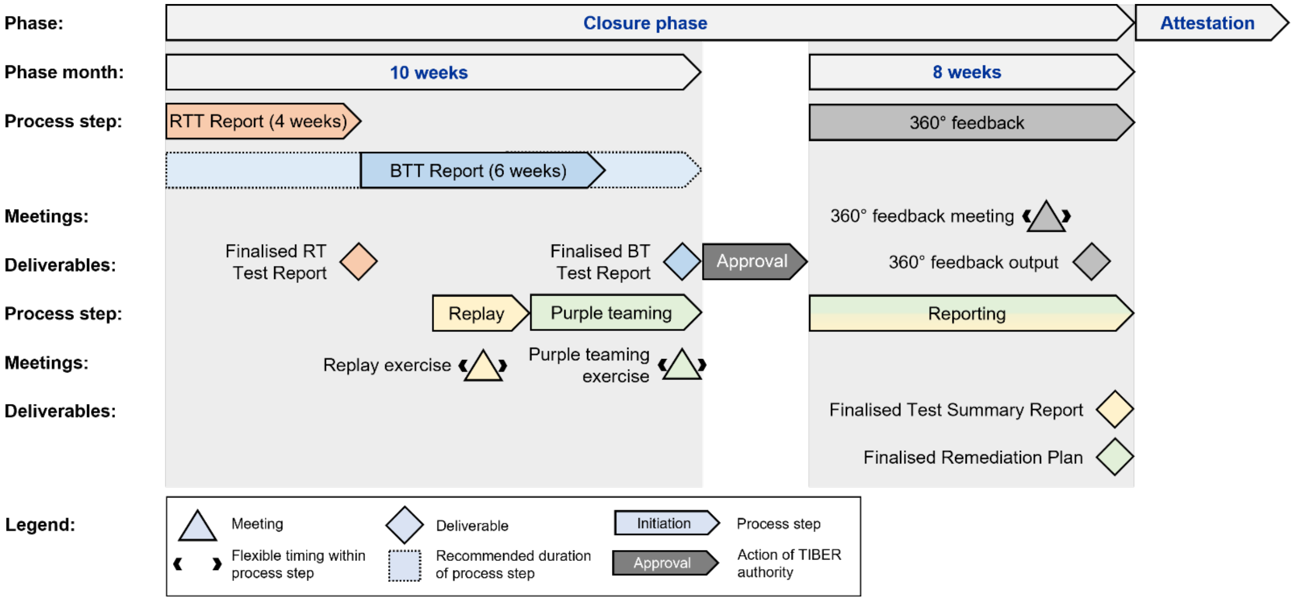
1.3 Location within testing process

The RTTR is created by the RTT at the beginning of the closure phase during the Red Team and Blue Team Test Report (BTTR) creation process step. It serves (together with the BTTR) as the basis for the later conducted replay and purple teaming exercises (in terms of timeline of events and potential discussion points) as well as for the Test Summary Report (TSR) and Remediation Plan (RP).

[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]

Closure phase: Red Team Test Report 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 RTTR

The RTTR shall include information on at least all of the following:

- Information on the performed attack, including:
  - the targeted critical or important functions (CIF) and identified ICT systems, processes and technologies supporting the CIF, as identified in the Red Team Test Plan (RTTP);
  - a summary of each scenario;
  - flags reached and not reached;
  - attack paths followed successfully and unsuccessfully;
  - tactics, techniques and procedures (TTP) used successfully and unsuccessfully;
  - deviations from the RTTP, if any;
  - leg-ups granted, if any;
- All actions that the testers are aware of that were performed by the BT to reconstruct the attack and to mitigate its effects;
- Discovered vulnerabilities and other findings, including:
  - vulnerability and other finding description including their criticality;
  - root cause analysis of successful attacks;
  - recommendations for remediation including indication of the remediation priority.

3 Considerations when drafting the RTTR

3.1 Management summary

The RTT should draft a short narrative in layman's terms, suitable for consumption by senior management and higher-level governance bodies (such as a Board of Directors), in order to:

- explain what critical or important functions and underlying systems were tested;
- give a high-level timeline of the test and provide an overview of the scenarios tested, including references to mimicked threat actors from the Targeted Threat Intelligence Report (TTIR), and context of the successful and unsuccessful attack methods employed, including the usage of leg-ups;
- highlight the main findings (based on criticality), including strengths and challenges, and possible root causes based on the attack methods used;
- give insight into the main categories of recommendations to address the findings and possible root causes;
- note any significant observations and exceptions in the test.

3.2 Storyline

The RTT should draft a storyline of the test, for each scenario, end-to-end, and where relevant divided into in, through and out phases, to be used by the relevant staff at the tested entity, outlining:

- The CIFs and underlying systems that were targeted, including the identified ICT systems, processes and technologies supporting the CIF as identified in the RTTP.
- Any deviation from the RTTP.
- A summary of the attack scenarios that were utilised, in line with the MITRE ATT&CK framework, including the flags and objectives reached and not reached (linked to the relevant aspect(s) of the CIA triad).
- Any leg-up[3] or allowance made by the control team (CT) of the entity undergoing the test to facilitate the test and/or action by the BT of the entity affecting the test.

[3] 'Leg-up' means the assistance or information provided by the CT to the RTT to allow the RTT continue the execution of an attack path where they are not able to advance on their own, and where no other reasonable alternative exists, including for insufficient time or resources in a given TLPT.

- What was compromised, the attack path, both successful and unsuccessful, the successful and unsuccessful TTPs used, the main findings and associated recommendations.
- Stealth-based techniques used across the attack life cycle. Assessment of whether the detection capabilities of the entity were adequate. If not, provide recommendations for improvement.
- Main root causes leading to the findings.
- Threat actor sophistication level that was actually needed for the attack. For example, the simulated threat actor is a nation state but for the actual attack it would have been enough with an intermediate hacker using existing attack toolkits.
- Any insight the RTT wishes to provide on the cybersecurity posture of the entity undergoing the test, including further exploitation that could have taken place if the RTT had more time and resources like an actual attacker, and areas of strength and/or weakness.
- All actions that the RTT are aware of that were performed by the BT to reconstruct the attack and to mitigate its effects.
- A timeline with the relevant logs and details for the BT to create an accurate BTTR.

3.3 Findings

The RTT must extensively document the findings identified in the testing process, and must categorise each finding in accordance with the NIST functions (i.e. Identify, Protect, Detect, Respond, and Recover); each finding must be categorised by criticality and complexity; and each finding must contain a clear description on how the entity was compromised and the impact of the compromise (including also the real impact if there were no limitations of a test). The findings should describe both technical and non-technical elements, if applicable.

This categorisation does not need to be based on a single dimensional technical aspect only, such as the Common Vulnerability Scoring System (CVSS) rating, but should also take into account multiple factors, including but not limited to the “location” of the finding in the infrastructure and proximity/effect on a critical system, the impact on the CIF if compromised and what further compromise this can lead to.

3.4 Provisional root cause analysis

The RTT must use their experience and expert judgement to determine whether they can draw conclusions on root causes of the findings outlined above. In order to do this the RTT needs to consider people, processes and technology holistically and not limit their view on the technological aspect alone.

Using these root causes, the RTT must also extrapolate from their actions what could have been further done to advance the attack on the entity and what the possible impact could have been. Based on this analysis and the findings from the root cause, as well as the RTT's expert opinion, the root causes also need to be categorised per criticality.

It should be noted that the provisional root cause analysis will be judgement based and only preliminary; the aim of such preliminary analysis is to provide the basis for the BT to reflect and to facilitate a robust discussion in the replay exercise. This section of the RTTR should be more analytical in nature, and aims to facilitate the replay exercise being more forward thinking, rather than solely technical and retrospective.

3.5 Recommendations for remediations

The RTT should develop clear conclusions and identify concrete recommendations for remediations, which can lead to future action. The RTT must extensively document the recommendations for remediations on the findings in the following manner:

- the prioritisation of recommendations for remediations must be commensurate to the finding it aims to address; and
- the recommendations for remediations must be adequately described to determine the entity's objective and to be able to implement the actions under each recommendation.

The RTT must extensively document the recommendations for remediations on the root causes in the following manner:

- the recommendations for remediations of root causes must be separate from those of the findings;
- the prioritisation of recommendations for remediations must be commensurate to the root cause it aims to address; and
- the recommendation for remediations on root causes should be drafted at a level that provides options and guidance to the entity undergoing the test, given that there may be alternative ways to address the root cause.

3.6 Artefacts

The RTT must include any artefacts that could plausibly remain on the systems of the entity having undergone the test, in the main body of the RTTR or in appendices to the report. These artefacts are, for example, toolsets that may remain on compromised hosts/systems. This section should list and allow these remaining artefacts to be removed by the entity as they may pose a risk to the systems or interfere with any future incident investigations or security assessments. Typically, these artefacts are described using filenames, paths, hashes, hostnames, IPs, email addresses, email subjects, email domains and web domains.

The RTT must substantiate all of the above with clear evidence (e.g. log files with timestamp, screenshots, etc).

3.7 Confidentiality

The RTT should be aware that the RTTR (including the annexes) is highly sensitive and therefore must be treated with the highest level of confidentiality in line with the TIBER-EU framework. Consequently, the RTT must ensure the following:

- strict control of the production of any copies and a register of all and any copies with the recipients;
- restricted access control to any copies;
- use of the allocated codename throughout the report;
- removal of any mention of the entity in the RTTR contents;
- very clear labelling in electronic and physical copies of the security label (e.g. highly confidential);
- where appropriate, requirements from national security legislations.

Due to the sensitive nature of the information contained within the RTTR, it should be handled and treated in a manner commensurate with this classification (e.g. TLP Red). It is the responsibility of the entity to retain the RTTR, and to share the report with the TM. At the very least, the TM must be permitted to visit the entity onsite to review the entire report.

The TM may request to receive a report without any sensitive information[4].

[4] Sensitive information is defined as information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the financial entity and its ecosystem would it fall in the hands of malicious actor.

4 Drafting format

The TIBER-EU RTTR 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