EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Remediation Plan Guidance

January 2025

Contents

1 Introduction

The Remediation Plan (RP) provides an overview of the measures planned by an entity having completed a TIBER-EU test to mitigate the vulnerabilities found during the test. The RP is a document assisting the financial entity in planning its remediation measures as well as respective supervisors and overseers in following up on those mitigations, taking into account the special nature of the test as a 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 RP. It also aims at providing guidance on important aspects to be considered during drafting.

1.2 Target audience

This TIBER-EU Remediation Plan Guidance is mainly aimed at the control team (CT), which is in charge of creating the RP 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.

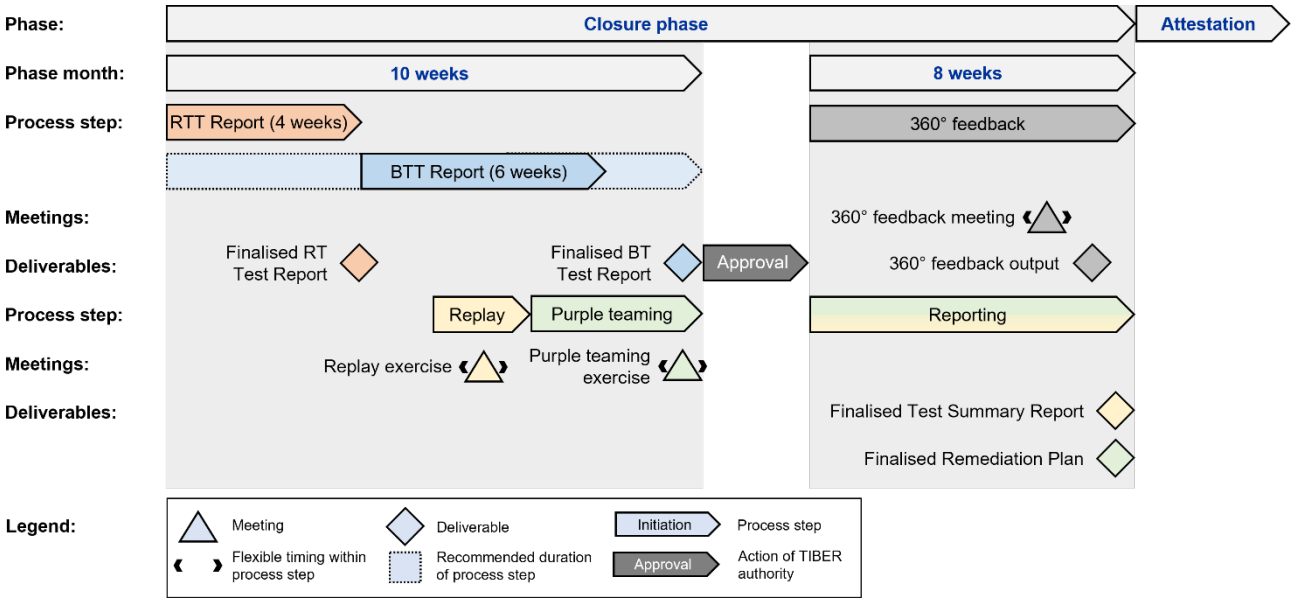
1.3 Location within testing process

The RP is typically drafted during the reporting process step, after the Blue Team Test Report (BTTR) and Red Team Test Report (RTTR) have been assessed 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.

Figure 1[2]

Reporting process step & Remediation Plan



[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 Requirements for the Remediation Plan

The RP must include for each observed vulnerability of the test:

- a description of the identified shortcomings;
- a description of the proposed remediation measures and of their prioritisation;
- the expected completion of the remediation measures, including where relevant measure to improve the identification, protection, detection and response capabilities;
- a root cause analysis;
- the entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements;
- the risks associated to not implementing the measures;
- where relevant, risks associated to the implementation of such measures.

3 Considerations when drafting the Remediation Plan

The entity is expected to acknowledge the findings and consider the recommendations offered by the RTT in the final RTTR, as well as the findings identified by the blue team (BT). Consecutively, the CT drafts a Remediation Plan in order to address the following:

- assign overall ownership of the RP to an individual at management level;
- list findings by criticality and assign ownership for each;
- have a detailed action plan;
- set timeframes and closure dates to remediate the findings based on their criticality.

Since cyber security is a risk-based approach, an entity has the freedom to decide not to mitigate a certain finding of the RTT immediately, if the associated risk is within the entities' risk appetite and/or the cost of remediation measures would greatly outweigh its benefits. In that case, the entity needs to justify the decision.

It is important that the RP focuses and addresses all findings, in addition to the root causes of the findings, which may encompass aspects related to people, process and technology used. For example, specific unpatched systems (as identified in the test) must be patched. Furthermore, the overall patching process must also be strengthened as needed, to ensure that systems are patched in a consistent and routine manner across the entity as a whole.

4 Drafting format

The TIBER-EU RP 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