Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

TIBER-IE Framework

Threat Intelligence Based Ethical Red-Teaming - Ireland

National Guide

December 2019

Contents

PART 1 – Introduction to TIBER-IE

Introduction

In March 2018, the ECB published the TIBER-EU Framework (Threat Intelligence Based Ethical Red-teaming) with the objective of putting in place a programme to test and improve resilience of financial infrastructure and institutions, at national and European level, against sophisticated cyber-attacks.

The TIBER-EU Framework is adopted and implemented at a national level by national authorities. The Central Bank of Ireland (Central Bank) is the designated authority for TIBER-EU in Ireland and has formally adopted the TIBER-EU framework, as TIBER-IE. Participation in TIBER-IE is voluntary, therefore the framework does not constitute a regulatory requirement.

This TIBER-IE National Guide sets out how the Central Bank will implement TIBER-IE and explains the requirements of TIBER-IE and the roles and responsibilities of the key stakeholders in a test, including those of the Central Bank. The National Guide is presented in two parts; Part 1 presents an overview of the TIBER-IE test process and the roles of the TIBER Cyber Team in the Central Bank, the White Team and Blue Team in the target entity, and the third party Threat Intelligence and Red Team providers. It also discusses the interactions between the above teams and with other stakeholders, including other national authorities. Part 2 of the Guide details the requirements of each phase of the test and sets the expectations in order for a threat-led red-team test to be deemed a TIBER-test.

What is TIBER-EU?

TIBER stands for Threat Intelligence Based Ethical Red-teaming. TIBER-EU[1] is a common framework that delivers a controlled, bespoke, intelligence-led Red Team test (or 'ethical hacking') of financial infrastructures and institutions (hereafter referred to collectively as 'entities') critical live production systems, without the foreknowledge of the entities' business and IT functions. An intelligence-led Red Team test involves the use of a variety of tactics, techniques and procedures (TTPs) to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e., its people, processes and technologies).

A TIBER test mimics potential attacks by real highly advanced threat groups/actors (organised crime groups, state proxies, nation-state attackers) and tests whether the defensive measures taken by the targeted entity are effective, thus supplementing the current periodic information security audits, penetration tests and vulnerability scans conducted by the entity. It helps an entity to assess its protection, detection and response capabilities while safeguarding the integrity, confidentiality and availability of the operational processes throughout the test. The outcome is not a pass or fail; instead the test is intended to reveal the strengths and weaknesses of the tested entity, enabling it to reach a higher level of cyber maturity.

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

The TIBER-EU framework was developed by the ECB based on experience from two pre-existing methodologies, the Netherland's TIBER-NL and the Bank of England's CBEST framework. The TIBER-EU framework was published in May 2018 to put in place a programme to test and improve resilience of financial infrastructure, at national or European level, against sophisticated cyber-attacks. A number of national competent authorities in Europe have implemented the TIBER-EU framework.

Although developed for critical European financial infrastructure, it was purposely designed to be sector agnostic so that it can also be used for any type, or size, of entity across any sector and has some flexibility in how it is adopted by any authority deciding to implement it.

Why TIBER-EU?

The financial system is a complex network of participants using different environments, shared technologies and with a large volume of information flowing through their networks. Within this context, there are highly sophisticated cyber threat actors who target the most vulnerable links in this network, and so it is critical that entities reduce their vulnerabilities at every point and strengthen their overall resilience. This requires diverse, layered approaches, solutions and tools. Intelligence-led Red Team testing is one such tool to help entities test and enhance their protection, detection and response capabilities.

As the appetite grows for different jurisdictions to develop national intelligence-led red teaming frameworks, there is a risk that incompatible frameworks could emerge which could lead to an unnecessary duplication of effort. Multiple frameworks potentially represent a substantial burden for entities (financial and otherwise). They also give rise to the risk of unnecessarily exposing sensitive information, and may additionally lead to inconsistent results.

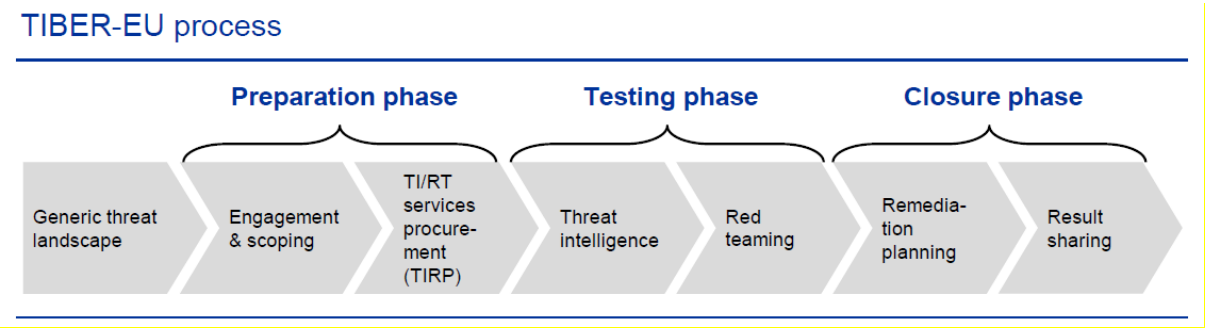
The unique aspect of TIBER-EU is the objective of facilitating testing for entities which are active in more than one jurisdiction. This promotes collaborative cross-authority testing, mutual recognition and assurance to other jurisdictions that the requirements of the TIBER-EU framework have been met.

The core objectives of the framework are to:

- enhance cyber resilience of entities, and of the financial sector more generally;
- standardise and harmonise the way intelligence-led Red Team tests are performed across the EU; while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities;
- provide guidance to authorities on how they might establish, implement and manage this form of testing at a national or European level;
- support cross-border/cross-jurisdictional testing for multinational entities;
- reduce the regulatory burden on entities and foster mutual recognition across the EU;
- create a protocol for cross-authority/cross-border collaboration, result sharing and analysis.

Overview of the TIBER Process

This section gives a high-level description the TIBER-IE test process. A step-by-step description of each of the phases in the TIBER-IE test process can be found in Part 2 of this National Guide.



The TIBER-EU framework sets out the three-phase process for an end-to-end TIBER test. The first phase, **the preparation phase**, includes engagement & scoping and procurement. The teams responsible for managing the test are established, the scope of the test is determined and attested by the entity's board and validated by the authority (i.e. the Central Bank), and the entity procures the Threat Intelligence (TI) and Red Team (RT) providers who will carry out the test.

The testing phase is made up of the Threat Intelligence and Red Teaming activities. The TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, setting out attack scenarios for the test and useful information on the entity. The report will be used by the Red Team to develop its attack approach and to try to breach the specified critical live production systems, people and processes that underpin the entity's CFs.

The closure phase includes remediation planning and result sharing. In this phase, the Red Team will draft a Red Team Test Report, which includes details of the approach taken to the testing and the findings and observations from the test. The report will also include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The Blue Team will now be aware of the test, and should replay the executed scenarios with the Red Team and discuss the vulnerabilities and findings identified during the test. Based on the findings and the replay of the test, the entity will develop and agree a Remediation Plan, in close consultation with the supervisor. The key findings from the test will be shared with other relevant stakeholders and a 360 exercise will be conducted to ensure lessons are learned from the test process.

It is critical to note that the test is scoped, managed, and paid for by the target entity and conducted by qualified third party TI and RT providers. The Central Bank's (i.e. its TCT) role is to approve the scope and oversee the test process to ensure it adheres to the TIBER-EU Framework.

TIBER-IE

The Central Bank of Ireland has decided to implement the TIBER-EU framework at a national level as described in this guide. Such a national implementation is a requirement of TIBER-EU for cross-jurisdictional recognition of tests as adhering to the TIBER framework. The national implementation of this framework is identified as TIBER-IE. TIBER-IE is a voluntary framework, adopted from a financial stability and operational resilience perspective and not a regulatory, oversight or supervisory requirement.

The outcome of a TIBER-IE test is not a pass or fail, nor is the test a silver bullet that replaces an entity's other cyber security controls or evaluations. The TIBER-IE assessment mimics potential attacks by real highly advanced threat groups/actors and tests whether the defensive measures taken by the targeted entity are effective, thus supplementing the current periodic information security audits, penetration tests and vulnerability scans conducted by the entity. The TIBER test method focuses on specified real-world threat scenarios and aims to determine, and more importantly serves to improve, the capabilities of targeted entities. It helps an entity to assess its protection, detection and response capabilities while safeguarding the integrity, confidentiality and availability of the operational processes throughout the test. Weaknesses, errors or other security issues are thereby identified in a controlled manner.

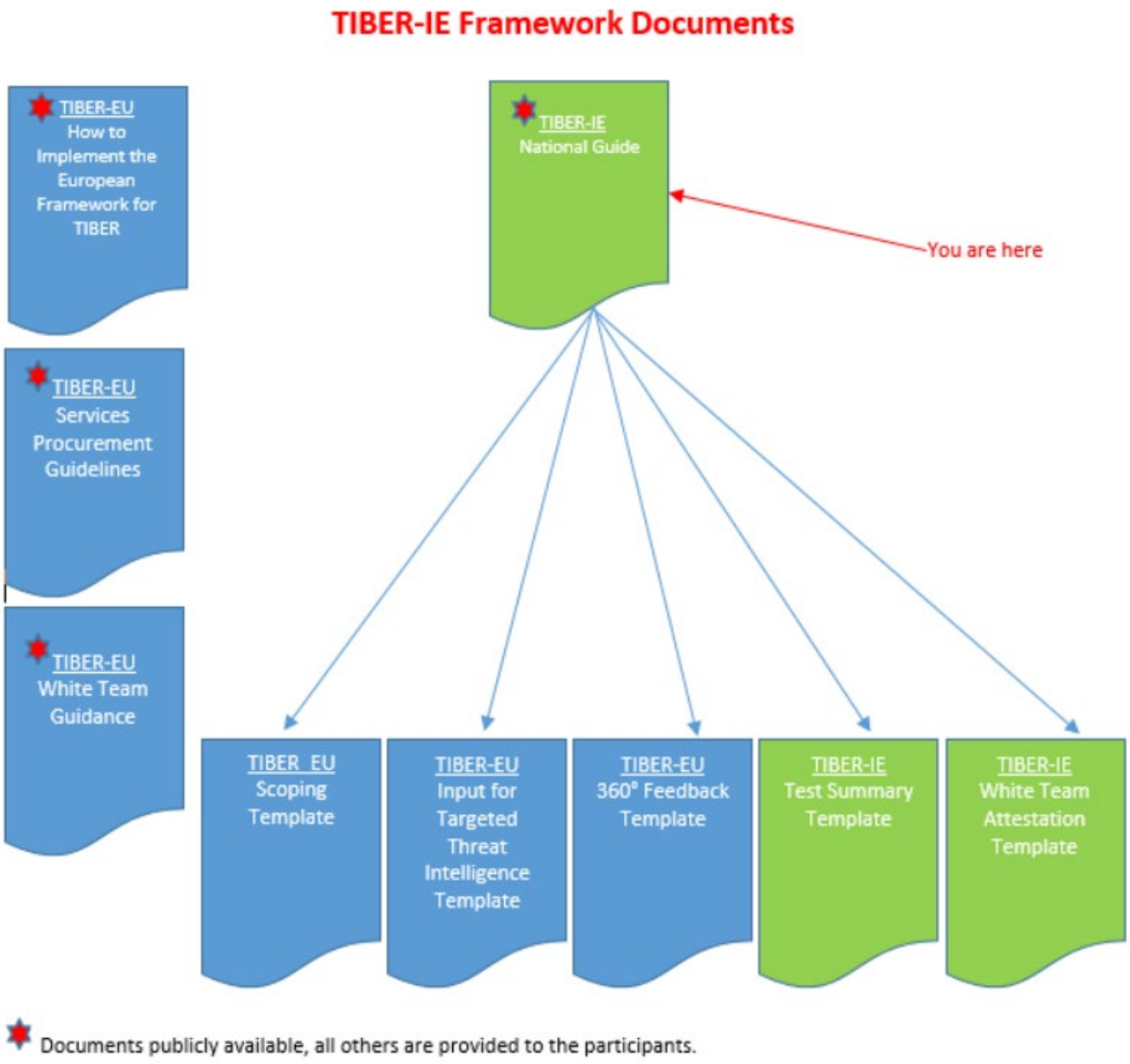
Collaboration, evidence and improvement lie at the heart of TIBER-IE. What differentiates TIBER-IE from other security tests is its intelligence-led holistic approach. This means that entities can improve their resilience based on proven relevant weaknesses rather than on perceived possible weaknesses. As such, by using TIBER-IE, a higher return on security investments can be obtained than by solely working with a compliance-driven risk framework and defending against perceived risks. TIBER-IE testing should improve the cyber resilience of individual entities and, as a result, the cyber resilience and stability of the financial system as a whole.

Purpose of this Guide

This *TIBER-IE National Guide* has been developed by the TIBER Cyber Team (TCT) at Central Bank of Ireland for the benefit of the TIBER-IE test participants and their cyber security service providers. This document details the key phases, activities, deliverables and interactions involved in a TIBER-IE assessment.

This document is a guide rather than a detailed prescriptive method. This guide should be read in conjunction with the TIBER-EU Framework and other TIBER-IE and TIBER-EU materials, detailed in the diagram below. These additional guidelines and templates will be provided to entities who engage with the Central Bank of Ireland for TIBER-IE assessments and a number are common to all jurisdictions that have implemented TIBER-EU.

The TIBER Cyber Team (TCT) is available to answer any questions that firms or service providers may have on the TIBER-IE process. The Team can be contacted at TIBER-IE@centralbank.ie.



Copyright notice and legal disclaimer

The information and opinions expressed in this document are for informational 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.

Each participant in a TIBER-IE test is exclusively responsible and liable for the execution of the tasks attributed to it by this framework, including compliance with applicable laws and regulations. It is the responsibility of each participant to conduct a review of existing laws and regulations to ensure that the execution of the tasks attributed to it does not contravene any such law or regulation.

This National Guide has been developed directly from the TIBER-EU framework to which the ECB holds all copyright. In addition, an effort has been made to align this guide with existing, published TIBER-XX guides in other EU countries to facilitate the recognition of cross jurisdictional tests. These include, TIBER-NL, TIBER-DK, TIBER-BE and similar implementations in non-EU jurisdictions such as CBEST in the UK.

Abbreviations used in this guide

Abbreviations	Explanation
FI	Financial Institution
TCT	TIBER-IE Cyber Team at the Central Bank of Ireland
WT	White Team
WTL	White Team Lead
TTM	TIBER Test Manager
RT	Red Team
BT	Blue Team
PT	Purple Team
TI	Threat Intelligence

Role of the Central Bank of Ireland

The national implementation of the TIBER-EU framework is identified as TIBER-IE and the Central Bank of Ireland is the designated national authority. As such, the Central bank has certain responsibilities to ensure TIBER-IE is implemented in accordance with TIBER-EU framework and that TIBER-IE tests meet the required expectations.

TIBER-IE Cyber Team (TCT)

The Central Bank is responsible for setting up an appropriate governance structure of TIBER-IE. This includes establishing a TIBER Cyber Team (TCT) to manage and operationalise the TIBER-IE programme. The TCT should include a Programme Manager and Test Team Managers who have experience and knowledge of the complex general IT landscape of candidate entities, technical knowledge of the tested systems and applications, risk management skills and experience, and up-to-date knowledge of the TTPs used by threat actors and of geopolitical developments and threat evolutions.

The TCT is responsible for overseeing each TIBER-IE test to ensure alignment with the TIBER-EU Framework and subsequently recognising the assessment as a TIBER test. The TCT ensures that the entities undergo tests in a uniform and controlled manner, however the TCT can in no way be held accountable or liable for the actions of the entity's White Team or third party providers or for any consequences of the TIBER-IE test for the participating entities or third parties. During a test, the TCT holds the right to invalidate a test for TIBER recognition if it suspects that the entity is not conducting the test in the right spirit and in accordance with the requirements of the TIBER-IE/TIBER-EU frameworks.

The TIBER-IE Cyber Team is responsible for continuously updating the TIBER-IE Framework in light of lessons learned from its implementation and the tests carried out. This will be done on a continuous basis in collaboration with the entities participating in TIBER-IE, but also with authorities in other jurisdictions that have adopted TIBER-EU, including the ECB.

Members of the Central Bank's TCT participate in the TIBER Knowledge Centre at the ECB, which is made up of the TCT at the ECB and those of the other EU jurisdictions that have implemented TIBER-XX at national level. This trusted community of TCTs, provides a forum for collaboration, cooperation, and support across jurisdictions that are implementing TIBER testing.

The TCT does not have a supervisory role and is segregated from the prudential and conduct supervision divisions to ensure that the tests are conducted in an open and collaborative manner without the concern that supervisory actions will be imposed on firms when weaknesses are identified. As per the TIBER-EU framework, the TCT will consult with the supervisors during the scoping phase of a test to ensure that all appropriate critical functions are captured in the scope discussions. The supervision team will not be involved in the test phases and the TCT will not share TIBER-IE related information or documentation regarding a

specific entity with the supervision team during this phase. Once the test is complete and the Test Summary Report has been finalised, the TCT will notify the supervisors that they should expect the entity to share this report in due course. The supervisors can then request to see the proposed remediation plan and can follow-up with the entity as needed. The TCT will not be involved in the remediation phase.

Cooperation with other authorities

The agreement to establish TIBER-IE was reached following a need to improve cyber resilience, cross-jurisdictional regulatory engagement and requests from financial institutions to facilitate TIBER testing which could be recognised in multiple jurisdictions. Participation in TIBER-IE is voluntary, therefore the framework does not constitute a regulatory requirement. The Central Bank of Ireland is the lead authority of TIBER-IE due to the fact that its strategy supports one of the Central Bank of Ireland's core objectives: to enhance the financial stability and resilience of the financial system. It is in the capacity of lead authority of TIBER-IE that the TCT will oversee each TIBER-IE test to ensure that the test meets the requirements in TIBER-IE and thus can be recognised as a TIBER test. This requires that the TCT is able to review and approve all the relevant material prepared in the test process. The TCT will not share information with any other authority about a TIBER test without having a specific consent from the tested entity. Furthermore, the tested entity is the legal owner of all the material being produced during the test, and is responsible for sharing the material with its competent authorities, if required.

When testing cross-border entities participating in TIBER-IE, the TCT should enter into cooperation with authorities in other jurisdictions, following discussions with the tested entity, and must be entered into in accordance with the conditions described below.

Cross-jurisdictional cooperation

The harmonised and standardised approach in TIBER-EU enables cross-border, cross-jurisdictional intelligence-led Red Team testing for multinational entities. It is therefore the responsibility of the TCT (following consultation with the entity) to liaise with authorities in other jurisdictions that are potentially relevant for the test of such a multinational entity. Before each test, the TCT, in conjunction with the tested entity, will identify such authorities and reach out to the relevant ones with the aim of either 1) establishing cross-jurisdictional collaboration for a test of the entity; or 2) explaining and documenting the procedures in the TIBER-IE test process to promote cross-jurisdictional recognition of the test results.

Generic threat intelligence

An optional first phase of the TIBER-EU framework is the development of a generic threat landscape report. This report should contain information on the geopolitical and criminal threats to the key institutions in the financial sector, including a description of relevant high-level threat groups, their motives/modus operandi, and the tactics, techniques and procedures they use in their attacks. The report should also include a description of which types of financial

institutions the threat actors are targeting, e.g., wholesale/retail banking, clearing/settlement, asset management, payment services, etc. The purpose of the report is to provide a basis for the targeted threat intelligence produced in a later phase of the test process.

This report can be prepared by a specialised third party provider or by the NCA or other government/intelligence agency, as is the case in some EU jurisdictions. The Central Bank does not yet produce a Generic Threat Intelligence report for the purposes of TIBER-IE but this option will be explored further as the TIBER-IE programme develops.

Legal and compliance

As part of the implementation of TIBER-EU in Ireland, the Central Bank has conducted a review of existing laws and regulations at a national and European level and concluded that the requirements, methodologies and processes contained in the TIBER-IE Framework do not contravene any national or European laws or regulations, and that the implementation of the framework is legally compliant. The Central Bank will revisit this opinion periodically in order to ensure legal compliance throughout the lifetime of the TIBER-IE programme.

In regard to the Red Team tests, it is important to emphasize that it is the responsibility of the tested entities, and the third-party providers to ensure that they conduct the test within the remit of all laws and regulations, and that appropriate risk management controls are in place to enforce this. Thus, the tested entities are required to carry out their own legal reviews ahead of conducting their Red Team tests and cannot rely on the legal review of the TIBER-IE Framework.

Stakeholders in the TIBER-IE test process

The direct stakeholders involved in a TIBER-IE test are:

- The Central Bank of Ireland, in particular the TIBER Cyber Team,
- The Entity to be tested, via the entity's White Team and Blue Team, and
- Third-party providers of Threat Intelligence and Red Team testing

Entity to be tested

Each entity is responsible for its own management and organisation of the test, including hiring the external third-party providers, and for implementing appropriate controls, processes and procedures to ensure that the test lives up to best practices and risks are appropriately mitigated.

The White Team (WT)

For each TIBER-IE test, the tested entity must establish a **White Team (WT)** who will be responsible for scoping and running the test, engaging with all other parties, and accountable

for management of risks during testing. The White Team should be a made up of senior executives and management of the entity who are knowledgeable of the entity's critical functions to be tested, and the team should be kept small to ensure that knowledge of the test within the organisation is minimised. This team is responsible for the overall planning and management of the test, in accordance with the TIBER-EU Framework.

The White Team is led by a dedicated **White Team Lead**. The White Team Lead coordinates all test activity including engagement with the Threat Intelligence and Red Team test providers. (More details on the roles, responsibilities and ideal composition of the White Team can be found in the TIBER-EU White Team Guidance).

The Blue Team (BT)

All other members of the entity being tested, in particular those who manage the people, processes and systems of the entity being tested, are (in the context of a TIBER-IE test) referred to as the Blue Team. It is critical that all members of the Blue Team are excluded from the preparation and conduct of the TIBER-IE test and, critically, must remain unaware of the test for the duration. In the closure phase following testing, the Blue Team is informed about the test, and the relevant, most appropriate members of the Blue Team should participate in the replay and follow-up.

Third-party providers

It is a requirement of both the TIBER-EU framework and the TIBER-IE implementation that a test will only be recognised if it is conducted by independent third-party providers. Several entities already conduct red team testing with dedicated internal Red Teams, and although the practice of internal Red Teams is encouraged, there are clear advantages in procuring an external party to conduct additional tests.

For example, an external tester provides a fresh and independent perspective, which may not always be feasible with internal teams that have grown accustomed to the internal systems, people and processes. Furthermore, external providers might have more resources and up-to-date skills to deploy, which would add value to the entity.

For each TIBER-IE test, two types of third-party providers will be involved:

The Targeted Threat Intelligence provider (TTI)

The threat intelligence provider is an external service provider procured by the White Team. This provider gathers targeted intelligence on the entity, replicating the research that would be performed by an advanced cyber attacker, and provides this information to the entity in the form of a Targeted Threat Intelligence Report. These providers should use multiple sources of intelligence to provide an assessment that is as accurate and as up-to-date as possible.

The Red Team (RT)

The Red Team is the external service provider, procured by the White Team, to attempt to breach the security capabilities of the entity using ethical hacking methods. The Red Team plans and executes a TIBER-IE test of the target systems and services based on the scenarios developed by the Threat Intelligence provider. Following the test, the Red Team drafts the Red Team test report outlining the issues identified in the test.

When hiring Threat Intelligence and Red Team test providers, the entity should make sure that there is mutual agreement on at least the following aspects of the test: the scope of the test; boundaries; timing and availability of the providers; contracts; actions to be taken; and liability (including insurance where applicable).

A key means of managing the risks associated with the TIBER-IE test is to use the most competent, qualified and skilled Threat Intelligence and Red Team test providers with the requisite experience to conduct such tests. Consequently, prior to engagement the entity must ensure that the providers meet the minimum requirements, which are set out in the TIBER-EU Services Procurement Guidelines.

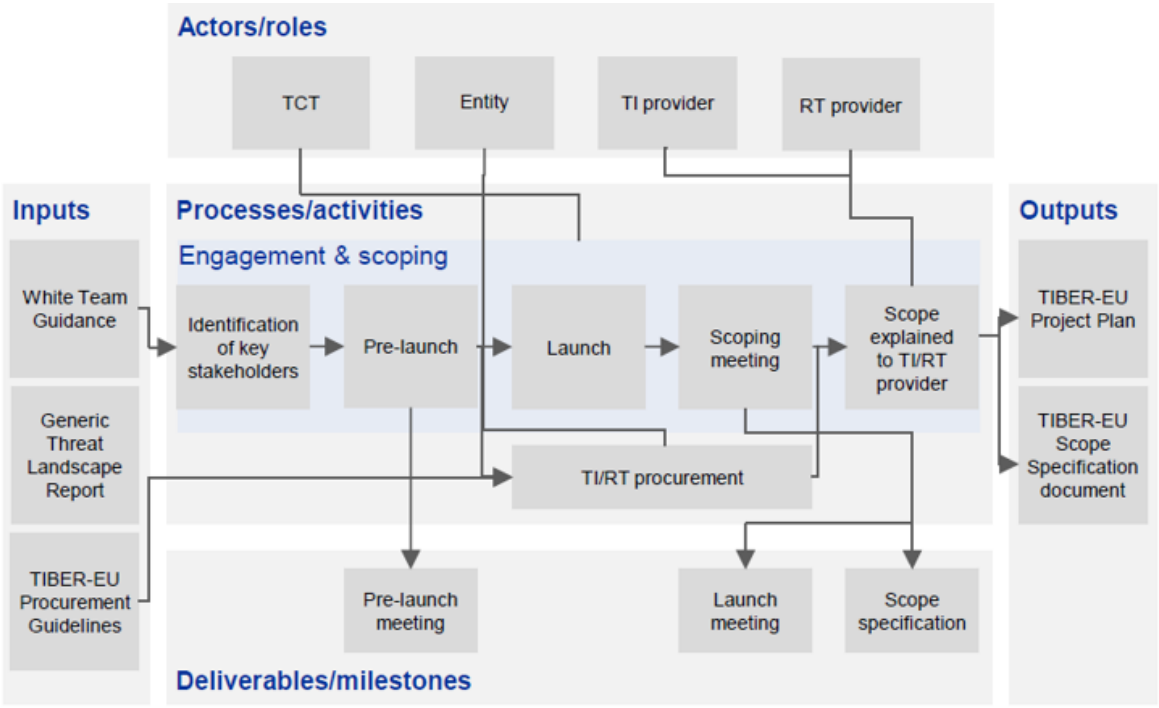
Cooperation between Stakeholders

All parties involved in a TIBER-IE test should take a collaborative, transparent and flexible approach to the work, excluding the Blue Team, which should remain unaware of the test. A prerequisite for a successful test is a close cooperation between the White Team Lead and TCT during all phases of the test. Responsibility for the overall planning and management of the test lies with the tested entity. The White Team Lead is responsible for determining and finalising the scope, scenarios and risk management controls for the test, ensuring that they have been approved and attested by the board/executive management and validated by the TCT. In addition, the White Team Lead should coordinate all test activity including engagement with the third-party providers. The White Team Lead should ensure that the TI and RT providers' project plans are factored into the entity's overall project planning for the TIBER-IE test. In the closure phase, the White Team Lead is responsible for involving relevant members of the Blue Team in the test replay and follow-up.

If there are significant deviations in the original planning, this should be discussed with the TCT. It is critical that all relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any issues, resource constraints, etc. can be addressed in a timely fashion. Although the White Team Lead is the primary contact for the TI and RT providers, the TCT should also have access to these providers as necessary. Where there are crucial decisions to be made (e.g. deviations during the test from the agreed scope), or where differences of opinion arise, both the White Team Lead and the TCT should have a formal escalation line to their respective superiors, and between the superiors.

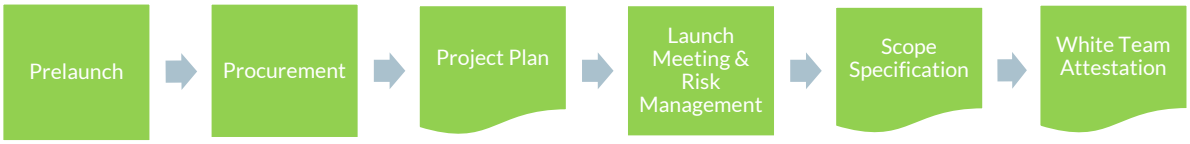
PART 2 – The TIBER-IE Test Process

The Preparation Phase – TIBER-IE



Overview

During the TIBER-IE Preparation Phase, the engagement for the TIBER-EU test is formally launched and the TIBER Cyber Team begin to liaise with the participating entity, the scope is established, and the entity procures the Threat Intelligence and Red Team providers. This phase lasts approximately four to six weeks, not including the duration of the entity's procurement process.



Prelaunch and Procurement

Objective	Deliverable	Responsible
Establish White Team and White Team Lead	Team established and TCT notified	Entity
Pre-launch meeting for familiarisation with TIBER-IE and TIBER-EU Framework and to set a launch date	Launch date set, TIBER-IE documentation/templates shared	WT/TCT
Procurement of Threat Intelligence and Red Team Service Providers	TI and RT Contracts	WT
Prepare project plan	Project plan	WT

Establish White Team and White Team Lead

The TCT requests the nomination, by the entity, of a White Team and White Team Lead. The White Team consists of a select number of senior individuals who are experts and/or are positioned at the top of the security incident escalation chain. Once established, the entity informs the TCT of the White Team members. The White Team Lead ensures that the White Team is aware of the TIBER-IE test, the requirement for secrecy and the process the team should follow in the event that the Blue Team detects and escalates a TIBER-IE related incident. All staff members of the entity who are not members of the White Team are referred to as the Blue Team. It is critical that all Blue Team members remain unaware of the TIBER Test both before and during the Test.

Pre-launch meeting and setting the launch date

The White Team Lead holds the pre-launch session with the TCT and any additional White Team members that the White Team Lead wishes to involve. The TCT can give a briefing on the requirements for a TIBER-IE test including underlying guidelines such as the TIBER-EU White Team Guidance and TIBER-EU Services Procurement Guidelines. The briefing on the requirements, should include at least the following:

- the TIBER-EU process as reflected in the TIBER-IE Implementation Guide;
- the stakeholder roles and responsibilities;
- the security protocols (including the set-up of secure document transfer);
- contractual considerations (including sharing of documentation from TI/RT providers);
- project planning.

Procurement

After the pre-launch meeting, the entity begins its procurement process. Although entities may already conduct Red Team testing with dedicated internal Red Teams, the TCT will only

recognise a TIBER test if it is conducted by independent third-party providers (i.e. external Threat Intelligence and Red Team providers).

To ensure that the Threat Intelligence/Red Team providers meet the required standards for conducting a TIBER test, the entity should take into account the specifics and minimum requirements detailed in the TIBER-EU Services Procurement Guidelines. During procurement, the entity should carry out the following activities:

- draw on TIBER-EU Services Procurement Guidelines to identify potential TI/RT providers capable of meeting the objectives of the test;
- issue an invitation to tender in compliance with the TIBER-EU framework and any relevant procurement legislation;
- assess tender responses, and then interview and select appropriate providers; and
- establish conditions governing the sharing, confidentiality and retention of intellectual property rights.

When hiring Threat Intelligence and Red Team service providers, the White Team should ensure that there is a mutual agreement on at least the following aspects: the high level scope of the test; boundaries; timing and availability of the providers; contracts; actions to be taken and liability.

The contracts with the TI and RT providers should include:

- providers must meet security and confidentiality requirements that are as least as stringent as those followed by the underlying entity for confidentiality requirements;
- a clause related to non-disclosure and confidentiality, data destruction requirements and breach notification provisions; and
- a determination of activities not allowed during the test such as destruction of equipment; uncontrolled modification of data/programmes; jeopardising continuity of critical services; blackmail; threatening or bribing employees and disclosure of results.

With regard to contractual considerations, the smooth delivery of a TIBER-IE test requires a transparent process with the appropriate information and documentation flowing freely, safely and securely between the relevant parties. To facilitate the free, safe and secure flow of information, all participating parties must sign a non-disclosure agreement. In some cases, the procurement process can be conducted in parallel to the Launch Meeting and at the discretion of the TCT.

Project Plan

Once the procurement process has been completed and all relevant contractual arrangements are in place, the White Team Lead must prepare a project plan. The project plan must include a schedule of meetings to be held between the White Team, TI/RT providers and the TCT. The project plan must be shared with all stakeholders in advance of the launch meeting.

Launch Meeting, Risk Management, Scoping, White Team Attestation

Task	Deliverable	Responsible
Launch Meeting	Physical meeting, all stakeholders	WTL
Risk Management	Applied risk controls, procedures for test	WT
Draft Scoping Document	Draft Scoping Document	WT
Scoping Meeting	Final scoping document(attested by board)	WTL
Attest to adherence of guidelines and confidentiality requirements	White Team Attestation	WTL/TCT

Launch meeting

The Launch meeting is a physical meeting with all relevant stakeholders where topics of discussions include the test process, expectations, as well as the draft TIBER-IE Project Plan, which has been prepared and distributed prior to the meeting by the White Team Lead. A code name for the entity must be chosen and used by all stakeholders when referring to the entity throughout the remainder of the test process to ensure confidentiality and secrecy of the test.

Risk management

Since the TIBER-IE assessment harbours elements of risk for all parties, it is of the utmost importance that the White Team has implemented appropriate controls, processes and procedures to ensure that the test is carried out with sufficient assurances for all stakeholders in order for risks to be identified, analysed and mitigated according to the entity's practices regarding risk management. A risk assessment must therefore be conducted prior to the test to ensure that the right risk management precautions are taken in line with the entity's existing risk management framework. It is the responsibility of the White Team to ensure that the identified precautions are taken during the entirety of the TIBER-IE testing process. In addition, the following must occur:

- protecting the confidentiality of the test is crucial to its effectiveness, and, to that end, the White Team must limit awareness of the test to a small trusted group whose members have the appropriate levels of seniority to make risk-based decisions regarding the test;
- due diligence of in-scope systems prior to any testing must be part of the preparations to ensure that backup and restoration capabilities are in place. This process should, however, be carefully carried out such that the upcoming test of in-scope systems are not revealed to employees outside of the White Team in the entity;
- code names for the entity being tested should be used by all stakeholders throughout the whole process to protect the sensitive nature of the test, and the potentially detailed findings on the weaknesses and vulnerabilities;
- escalation procedures should be defined to avoid triggering mandatory actions in the case of a real event; and

- management of risks during the test require that the White Team remain in control of the process to ensure that the test proceeds in accordance with the scope, scenario, planning and process agreed (and described in the framework documents).

Draft Scoping Document

The key objective of scoping is for the entity and the TCT to agree the scope of the red team test. The scope must include the entity's critical functions. The entity may decide at its discretion to include additional non-critical functions (i.e. people, processes and technologies) within the scope of the test, provided these do not negatively affect the testing of the critical functions.

Within the TIBER-EU framework critical functions are defined as: "the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct".

Both the TCT and the entity should have extensive knowledge of the entity's business model, functions and services. The entity may conduct a business impact analysis defining the critical functions as part of their standard operational risk management practices. It is also important to consider the relevant stakeholders of the test including the role of critical service providers. The TCT will consult with the supervisors during the scoping phase of a test to ensure that all appropriate critical functions are captured in the scope discussions, if appropriate.

A draft TIBER-EU Scope Specification template must be completed and distributed by the White Team prior to the Scoping meeting. This document sets out the scope of the TIBER-IE test and lists the key systems and services that underpin each critical function. The White Team should discuss the flags with the TCT, who must approve them.

Scoping Meeting

Although the flags[2] are set during scoping, they can be modified on an iterative basis following Threat Intelligence gathering and as the red team evolves. The final TIBER-EU Scope Specification should be agreed by the TCT during a Scoping meeting organised by the entity for all relevant stakeholders. Importantly, the scope will need to be agreed at the Board level of the entity.

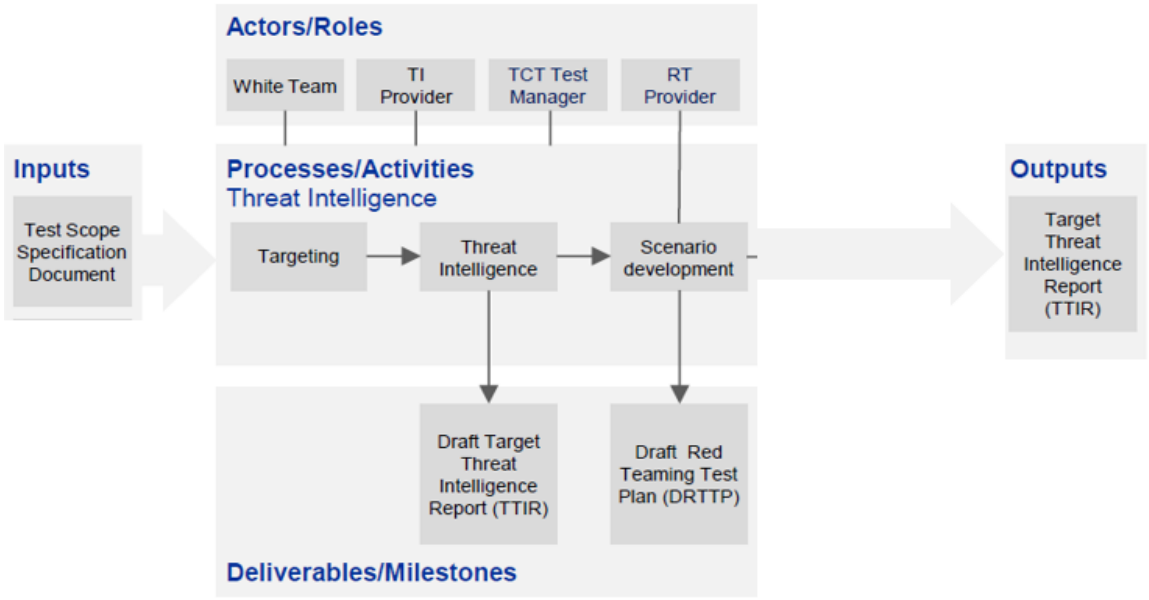
For a test to be successful, it is important that the service providers understand the business of the entity. Therefore, after scoping and in case the service providers were not already involved during the scoping, a meeting is planned with the provider(s) in which the CFs and systems underpinning them are explained.

[2] The "flags" to be captured are essentially the targets and objectives that the RT providers must strive to achieve during the test, using a variety of techniques.

White Team Attestation

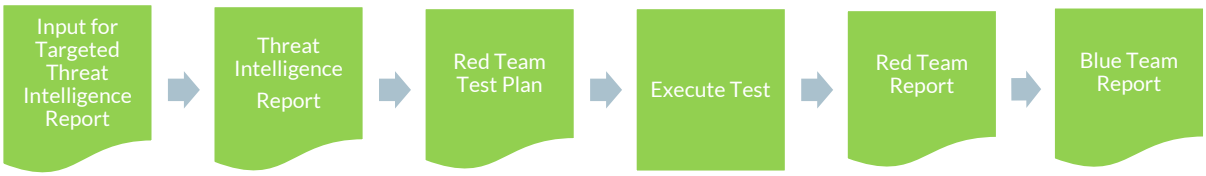
Once procurement has been finalised, the White Team attests that, to the best of their knowledge, the procurement process has adhered to both the TIBER-EU White Team Guidance and the TIBER-EU Services Procurement Guidelines using the White Team Attestation template provided by the TIBER Cyber Team.

The Test Phase – TIBER-IE



Overview

The Test Phase consists of targeted threat intelligence gathering on the FI, which result in detailed test scenarios. These attack scenarios will be expanded by the Red Team into a Test Plan prior to test execution.



Targeted Threat Intelligence and TTI Report

Objective	Deliverable	Responsible
Firm to provide information to TI	TIBER-EU Input for Targeted TI Template	WT
TI gathers TI data	TTI report	TI

TIBER-EU Input for Targeted TI Template

Threat intelligence based scenarios mimicking real-life cyber adversaries are essential to the success of testing activities. The duration of the targeted threat intelligence process in this phase is approximately five weeks.

Real-world threat actors may have months to prepare an attack. Therefore, to make intelligence gathering as efficient as possible, and to ensure the intelligence is relevant to the scope and the entity's business, the TI provider should seek from the entity and be provided with a completed *TIBER-EU Input for Targeted TI template*. Some examples of the information provided include:

- a business and technical overview of each critical function-supporting system in scope;
- the current threat assessment and/or threat register; and
- examples of recent attacks.

The TIBER process is designed to create realistic threat scenarios imitating possible future attacks against the entity. Real-world threat actors operate free from some of the constraints that TIBER-IE service providers must observe, such as the time and resources available, not to mention the moral, ethical and legal boundaries.[3] This difference can cause challenges when attempting to create realistic scenarios as knowledge about the internal network is often the hardest to gain using morally, ethically, or legally justified techniques.

A similar constraint relates to the systems underpinning the critical functions which typically do not have a large footprint on the public internet. Whether they are internal bespoke systems or external systems that span multiple organisations with common connecting infrastructure, the knowledge of the functioning of these systems with a TI /RT provider may be limited in comparison to those attackers with the capacity and time to study these extensively.

Therefore, it rests with the entity to determine how much information it is willing to divulge to ensure that the TI/RT provider has the right level of knowledge to mimic advanced attacks. This way, TIBER reflects a 'grey box' testing approach in contrast with the 'black box' approach. The TI/RT provider receives support from the entity itself in order to balance out the smaller amount of possibilities it has compared to high end attack groups. Experience shows that the more relevant information an organisation gives to the TI/RT provider the more the participating organisation will gain from the test. Of course, there will be a balance to observe. The claim should never be made in hindsight that the test was manipulated and a real attacker could not

3 It is up to the entity to set up contractual agreements with the RTP regarding e.g. the inviolability of their employees' privacy. It is, however, important to note that privacy related information is left out from test reports under all circumstances.

have gotten that information. Therefore it should be evident that the information given to the RT provider could have been obtained by an advanced attacker, given more time, using different known techniques etc. Whether this information is provided by the entity or delivered by a third party TI provider, is decided by the entity.

The Targeted Threat Intelligence Report

The targeted threat intelligence process results in the production of a Targeted Threat Intelligence (TTI) Report, which is a bespoke, focused threat intelligence report for the entity being tested. Its aim is to use specific targeted threat intelligence and reconnaissance related to the entity, taking into consideration the real-life actors within the threat landscape, to help develop realistic attack scenarios. Responsibility for the development and production of the TTI Report lies with the Threat Intelligence service provider. The RT provider becomes involved towards the end of the phase when it absorbs the contents of the TTI Report and integrates the attack scenarios into a Red Team Test Plan.

During the TTI process, the Threat Intelligence service provider collects, analyses and disseminates critical function-focused intelligence relating to two key areas of interest:

- Target: intelligence or information on potential attack surfaces across the entity; and
- Threat: intelligence or information on relevant threat actors and probable threat scenarios.

To identify targets, the TI provider should carry out a broad exercise of the kind typically undertaken by threat actors as they prepare for their attack from outside the network. The objective is to form a detailed preliminary picture of the entity and its weak points from the attacker's perspective.

With regard to threats, the TI provider collects, analyses and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence which is specifically tailored to the entity's business environment, consideration should extend to critical third party providers. This process is passive, under no circumstances should active reconnaissance be undertaken[4].

The TTI Report must at least contain a business overview from an intelligence perspective; detail on relevant actors and high level scenarios; and intelligence on the entity's digital presence.

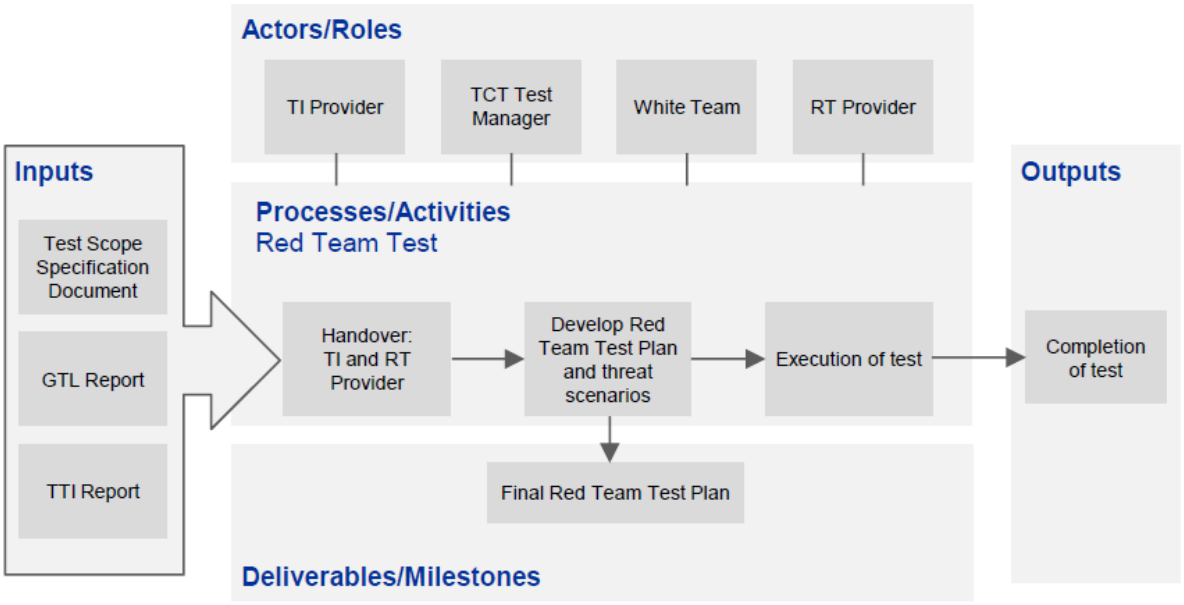
Equipped with the output from target identification and threat identification, which make up the TTI Report, the Threat Intelligence and Red Team service providers will have a firm evidential basis for the proposed red team test, which includes the attack scenarios. Three outputs are particularly relevant in this respect:

[4] Passive reconnaissance is an attempt to gain information about the target, its systems and networks without actively engaging with the target or its systems. In active reconnaissance, in contrast, the attacker engages with the target system, for example, conducting a port scan to determine open ports.

- tailored scenarios to support the formulation of a realistic and effective Red Team Test Plan;
- threat actor goals and motivations to help steer the Red Team service provider in its attempt to capture the flags agreed upon in the Scoping Phase; and
- validated evidence which will underpin the business case for post-test remediation and improvement.

Once the Threat Intelligence service provider has completed a final draft targeted TTI report, it should then be shared with the White Team, the TCT and the Red Team service provider two weeks before the TI/RT handover workshop. The targeted TI report is highly confidential and necessary precautions should be taken to protect the contents of the report from being leaked outside the group of stakeholders, including within the entity's own organisation. This high level of confidentiality applies to all the material that is produced during the TIBER-IE test process.

The Red Team Test



Objective	Deliverable	Responsible
Draft TI scenarios	TI test scenarios presented in TI/RT Handover Workshop	TI/WT
RT produces test plan	Red Team Test plan	RT

Threat Intelligence Scenarios

Scenario development represents the key transition point between the Threat Intelligence and Red Team service providers.

The TI/RT handover workshop activities are as follows:

- TI provider presents an overview of the TTI Report;
- TCT provides feedback comments on the TTI Report; and
- Red Team service provider presents the draft Red Team Test Plan, including critical function scenario mapping, flags, possible anticipated leg-ups[5], risk mitigation, escalation procedures, test start/stop dates and a draft Red Team Test Report delivery date.

Red Team Test Plan

Using the scenarios contained in the TTI Report, and in line with the TIBER-EU Test Scope Specification, the Red Team service provider should develop and integrate the attack scenarios into a draft Red Team Test Plan.

In the Red Team Test Plan, the RT will put together attack scenarios for the RT Test which:

- map onto one or more Critical Function-supporting systems;
- align Target Intelligence (Entity + RT/TI) into credible scenarios;
- provide background to the tradecraft of the type of actor that is mimicked in the attack;
- provide creative elements of what Tactics, Techniques and Procedures (TTPs) that have not yet been seen in the wild but that are, according to the professional knowledge of the RTP, to be expected for the future;
- would, if occurring in real life, have a destabilising effect on Irish financial stability; and
- provide elements that test the response of the entity, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

The scenarios are written from the attacker's point of view. The Red Team service provider indicates various creative options in each of the attack phases based on various tactics, techniques and procedures used by advanced attackers, to anticipate changing circumstances or if the first option does not work. The Red Team service provider should also indicate where a leg up might be needed if the attack is not successful. The scenario writing is a creative process. The TTPs do not only mimic those seen in the past, but combine techniques of the various relevant threat actors.

In addition to these scenarios, a Scenario X is prepared. This scenario enables a forward-looking perspective to possible attacks. The goal of Scenario X is to look forward towards what advanced attacks can be expected in the (near) future. The scenario may focus on a particular innovative tactic, not yet seen, possibly combined with societal developments that will impact the entity in the coming future. The focus of Scenario X however, remains on critical functions.

[5] During the testing process, the RT provider may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RT provider, with agreement from the WT and TTM, may be given a "leg-up", where the entity essentially gives the RT provider access to its system, internal network, etc. to continue with the test and focus on the next flag/target.

Prior to the commencement of the test, the RT provider should gain insight from the TIBER-EU Scope Specification, the GTL Report (if produced) and the TTI Report in order to finalise the Red Team Test Plan. The Red Team service provider should align its test objectives with the goals of each of the actors, map these to the critical function-supporting systems, and produce credible real-life attack scenarios for the test. The attack scenarios are designed to provide background to the tradecraft employed by each threat to conduct a successful attack. The Red Team service provider should therefore adapt its attack methodology to replicate the real-life attack scenarios.

The Red Team service provider should additionally draw upon the TTI Report, which reveals some of the entity's attack surfaces, as a basis for deeper and more focused targeting activities.

Performing any sort of Red Team test always carries a level of risk to the target system and the business information associated with it. Risks to the entity, such as degradation of service or disclosure of sensitive information, need to be kept to an absolute minimum. The Red Team service provider should therefore include an appropriate plan for managing these risks.

The output of this activity is the final Red Team Test Plan, including the attack scenarios to be followed and the risk management controls that will be applied to ensure that the test is conducted in a controlled manner.

Test Execution, Draft Red Team and Blue Team Reports

Objective	Deliverable	Responsible
Execute RT Test Plan scenarios	Test execution / draft Red Team Test Plan	RT
RT may require leg-ups	Leg-ups' should be documented	RT/WT/TCT
Provide ongoing updates	Ongoing status to WT and weekly updates to TCT	RT and WT
Issue draft Red Team report	Issued two weeks within test completion	RT
Key BT members informed	Construct a Blue Team Report	BT

Test Execution

The time-plan for the actual execution of the test should be between 10 and 12 weeks during which the Red Team service provider should perform a stealthy intelligence-led red teaming exercise against the target systems. The attack scenarios are not a prescriptive playbook which must be followed precisely during the test. If obstacles occur, the Red Team service provider should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective or flag.

Leg-up/Steers

It is possible that the Red Team service provider may require occasional leg-up/steers from the White Team to help them progress. Should this happen then these steers are duly documented. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

Ongoing updates

The TCT should be updated at least once a week by the White Team Lead and Red Team service provider, while the White Team should be kept abreast of progress on an ongoing basis. If feasible, physical meetings between the White Team, TCT and the Red Team service provider during this phase are strongly encouraged, since these discussions add significantly to the quality of the test and help build a relationship of trust. However, any such meeting should be conducted cautiously to ensure that the Blue Team is not made aware of the ongoing test.

Irrespective of the methodology used by the Red Team service provider, the test should be conducted in a controlled manner, taking a stage-by-stage approach, and in a way that does not bring risks to the entity and its critical functions. It is important for the White Team and TCT to be continuously informed about progress being made at each stage, as soon as a flag or target is in sight, or at least when the Red Team service provider has achieved the "capture the flag" moment. These updates provide the White Team with the opportunity to discuss with the Red Team service provider and TCT what actions can and cannot be taken next. It also provides a chance for escalation procedures to be invoked where necessary. The White Team can halt the test at any time if it considers it necessary to do so. All of the Red Team's actions should be logged for replay with the Blue Team, as evidence for the Red Team Test Report, and for future reference.

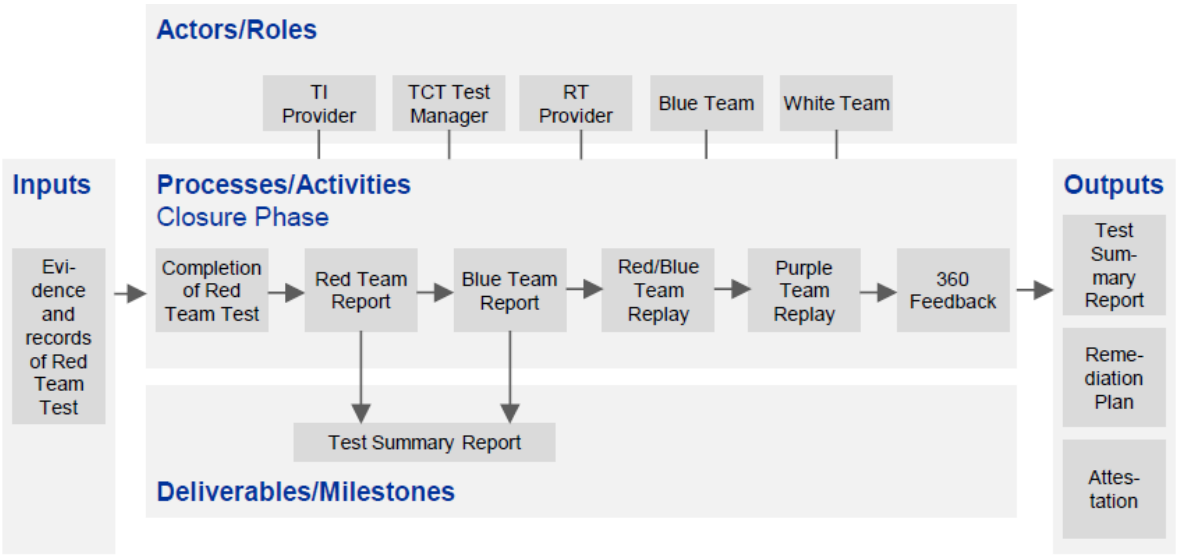
Draft Red Team Test Report

The output of this activity is a draft version of the Red Team Test Report produced by the Red Team service provider for delivery to the entity. The draft report must be issued within two weeks of test completion.

Blue Team

The key members of the entity's Blue Team are informed of the test and will use the Red Team Test Report to deliver their own Blue Team Report. In the Blue Team Report, the Blue Team maps its actions alongside the Red Team service provider's actions. The Blue Team Report should be completed ahead of the replay workshop to maximise the learnings from the replay.

The Closure Phase – TIBER-IE



Overview

The duration of the close-down activities in this final phase of work is approximately four weeks.

Red Team report & Red Team and Blue Team Replay

Objective	Deliverable	Responsible
replay for lessons learned	Replay Workshop	RT/BT
propose improvements	Purple Teaming	RT/BT

Replay Workshop

After the Red Team service provider and Blue Team deliver their reports, the entity must arrange a replay workshop. The goal of this workshop is to learn from the testing experience in collaboration with the Red Team service provider. During the workshop, a replay is organised in which the Blue Team and the Red Team service provider review the steps taken by both parties during the test.

When conducting the replay, the Red Team service provider should state how far the testing team managed to progress through the targeted attack life cycle stages of each scenario. The Red Team service provider should also offer an opinion as to what else could have been achieved with more time and resources given that genuine threat actors are not constrained by the time and resource limitations of a TIBER test.

Purple teaming

Additionally, a purple teaming element is added, in which the Blue Team and the Red Team service provider work together to see which other steps could have been taken by the Red Team service provider and how the Blue Team could have responded to those steps.

The TCT and Threat Intelligence service provider may also be present during these replay workshops.

360° Feedback Report, Test Summary Report & Remediation Planning

Objective	Deliverable	Responsible
all stakeholders provide feedback	360 Feedback Report	All
implement improvements	Remediation Plan	Entity
Entity summarises test, copies to TCT	TIBER-IE Test Summary Report	Entity
all stakeholders attest the assessment	Attestation signoff	All

360° Feedback

During the 360° feedback meeting, the entity, TCT, Threat Intelligence and Red Team service provider (s) physically meet to review the TIBER-IE exercise. The TCT arranges and facilitates the workshop. In the 360° Feedback report all parties provide feedback on each other. The goal is to further facilitate the learning experience of all those involved in the process for future exercises.

Whilst reviewing the results of the test during the 360° feedback meeting, the Red Team service provider should express this in terms of how far the testing team, as threat actor mimics, managed to progress through the targeted attack life cycle stages of each threat scenario. The RT should also offer an opinion as to what else could have been achieved with more time and resources given that genuine threat actors are not constrained by the time and resources limitations of TIBER-IE.

The key topics to be covered, from all parties' perspectives, are:

- activities/deliverables that progressed well;
- activities/deliverables for improvement;
- aspects of the TIBER-IE process that worked well;
- aspects of the TIBER-IE process that could be improved; and
- any other feedback.

In this way, the Threat Intelligence and Red Team service provider will obtain feedback on their performance, and the relevant authorities will have opportunities to identify and improve the TIBER-EU and the TIBER-IE process.

The TCT may share the output from the 360° feedback on an anonymous basis with the TIBER Knowledge Centre so that all lessons learned can be reflected on and improvements can be made to the TIBER-EU framework. This is a key part of the "learning and evolving" principle that underlies the TIBER-EU framework.

The Remediation Plan

After the Blue Team and Red Team service provider replay and the 360° feedback workshop, the entity should draft its Remediation Plan and TIBER-IE Test Summary Report.

The Remediation Plan is based on the test results, which should be used in turn to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-IE test. The Remediation Plan is for the entity's own use.

The TIBER-IE Test Summary Report

The TIBER-IE Test Summary Report summarises the overall test process and results (including the Remediation Plan). It should not however, 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. The entity must share the TIBER-IE Test Summary Report with the TCT.

Attestation signoff

At the end of the test, the entity, Threat Intelligence/Red Team service providers and the TCT should provide an attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-EU Framework. The attestation should be signed by the board/high-level executive management of the entity and Threat Intelligence/Red Team service providers to serve as a means of qualifying the test for a mutual recognition amongst other relevant authorities.

Interaction with Supervision

TIBER-EU is designed to act as a catalyst to entities that provide critical services to the financial system to enhance their cyber resilience to real potential threat actors. The framework was not designed as a supervisory tool but the role of supervisors in the process is set out in the framework.

The TCT will consult with supervisors as the scope of a specific test is developed to ensure that the business services and functions that the Central Bank's supervision team consider critical functions are considered in the scoping discussions. Then the supervision team steps away and the test is conducted by the TI and RT providers and monitored by the TCT. The TCT will not

share TIBER-IE related information or documentation regarding a specific entity with the supervision team during the test.

After the TIBER-IE process has been completed (i.e., the TIBER-IE Test Summary Report has been delivered), the TCT will notify the supervisor that the test has ended. The entity is requested to then share the Test Summary Report with the supervision team. The supervision team can request the entity to provide a copy of the remediation plan. The entity should address the TIBER-IE test and resulting remediation activities in its regular meetings with its supervision team.

Annexes

7.1 List of TIBER documents and templates used in a TIBER-IE assessment

List of TIBER documents	Responsible
TIBER-EU Framework: How to implement the TIBER-EU framework	European Central Bank
TIBER-IE National Implementation Guide	Central Bank of Ireland
TIBER-EU Services Procurement Guidelines	European Central Bank
TIBER-EU White Team Guidance	European Central Bank
TIBER-EU Test Project Plan	Entity
TIBER-EU Scope Specification Document*	Entity
TIBER-IE White Team Attestation*	Central Bank of Ireland
Generic Threat Landscape Report	Optional
Targeted Threat intelligence Report*	Threat Intelligence Provider
Input for Targeted Threat Intelligence*	Entity
Red Team Test Plan	Red Team Provider
Red Team Test Report	Red Team Provider
Blue Team Report	Entity
360° Feedback Report*	Entity
Test Summary Report*	Entity
Remediation Plan	Entity
TIBER-EU Attestation*	Entity

* Templates are available for use

Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem