TIBER-LU Implementation Guide

Version	
1.0	Initial publication

BANQUE CENTRALE DU LUXEMBOURG
EUROSYSTEM

cssf

I) Background

The Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) enables European and national authorities to work with entities of the financial sector[1] to put in place a programme to test and improve their resilience against sophisticated cyberattacks. The TIBER-EU framework is designed to be adopted *on a voluntary basis* by relevant authorities in any EU jurisdiction as a supervisory or oversight tool, for financial stability purposes, or from a catalyst angle, applying it in a manner which suits its specificities. Besides approving the TIBER-EU Framework as such, the Governing Council of the European Central Bank specifically adopted it as an Oversight tool for Systemically Important Payment Systems (SIPS) and the TARGET2 Securities platform (T2S).

The BCL and the CSSF jointly implement the TIBER-LU framework in Luxembourg and will jointly provide resources for the TCT (TIBER Cyber Team).

A) What is TIBER-EU?

TIBER-EU is a common framework that delivers controlled, bespoke, intelligence-led red team tests of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat. An intelligence-led red team test involves the use of a variety of techniques to simulate a cyberattack on an entity's critical functions (CFs) and underlying systems (i.e. its people, processes and technologies). It helps them to assess their protection, detection and response capabilities.

The ECB published the TIBER-EU Framework in May 2018, and the TIBER-EU Services Procurement Guidelines and TIBER-EU White Team Guidance, in August 2018 and December 2018 respectively. In August 2020, the following documents have further been published: the TIBER-EU Attestation template, the TIBER-EU Guidance for Targeted Threat Intelligence, the TIBER-EU Guidance for the Red Team Test Plan and the TIBER-EU Scoping Specification Template. In September 2020, the ECB further published the TIBER-EU Guidance for Red Team Test Report and the TIBER-EU Guidance for Test Summary Report.

The table below provides a mapping of the documentation and the different phases where they are to be used.

[1] For the purposes of the TIBER-EU Framework, "entities" means "payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector

Table 1- TIBER-EU documentation

Document	Phase	Sub-phase
TIBER-EU Framework	Preparation	Pre-Launch
TIBER-EU White Team Guidance	Preparation	Pre-Launch
TIBER-EU Services Procurement Guidelines	Preparation	Procurement
TIBER-EU Scoping Specification Template	Preparation	Scoping
TIBER-EU Guidance for Targeted Threat Intelligence	Testing	Targeted Threat Intelligence
TIBER-EU Guidance for the Red Team Test Plan	Testing	Red Team test plan and scenario
TIBER-EU Guidance for the Red Team Test Report	Closure	Test reporting
TIBER-EU Guidance for the Test Summary Report	Closure	Closure
TIBER-EU Attestation Template	Closure	Closure

B) What is the purpose of the TIBER-LU Implementation Guide?

The Guide has been developed by the TCT of the BCL and the CSSF. The Guide is meant to serve the TIBER-LU participating entities and their Threat Intelligence (TI) and Red Team (RT) service providers.

The present TIBER-LU Implementation Guide ("Guide") describes in general terms how the TIBER-EU framework will be applied in Luxembourg for the entities participating in a TIBER test, and which optional elements of the TIBER-EU Framework have been adopted, as set out in Annex 1.

This document is a guide rather than a detailed prescriptive method. It should therefore be consulted alongside other relevant TIBER-LU and TIBER-EU materials, which will be provided by the TCT to TIBER-LU participants. This guide only details the TIBER-LU test process. How to implement a TIBER program is not detailed. The TCT is available to answer any questions that participating entities or cybersecurity service providers might have on the TIBER-LU test.

C) Legal disclaimer and copyright notice

This document, the "TIBER-LU Implementation Guide", is compliant with TIBER-EU framework and is based on the TIBER-NL Guide of De Nederlandsche Bank (DNB), the Bank of England's CBEST intelligence-Led Testing document and the TIBER-DK Implementation Guide. The first two works being together licensed under the Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0). The BCL and CSSF have made changes to these materials, to which the BCL and CSSF own the copyrights.

D) Responsibilities and liability

Each Participating entity in a TIBER-LU test is exclusively responsible and liable for the execution of the tasks attributed to it by this framework[2], including compliance with applicable laws and regulations. It is the responsibility of each Participating entity 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.

E) Costs related to execution of TIBER-LU test

Unless explicitly agreed otherwise, each Participating entity bears its own costs and expenses for participating in a TIBER-LU test.

II) TIBER-LU Overview

The following section describes the roles and responsibilities of the TIBER-LU stakeholders and high-level process steps of a TIBER-LU test.

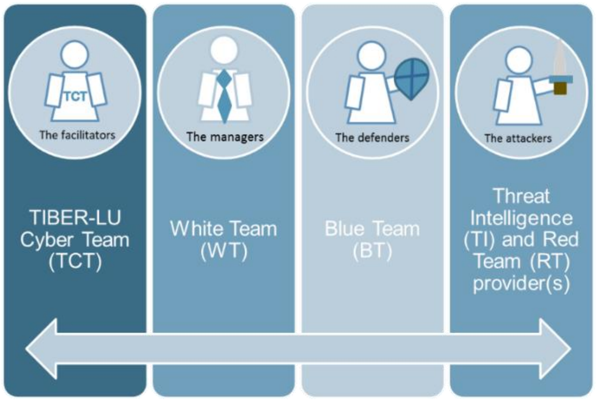
A) Stakeholders overview

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

- The Participating entities,
  - in which only the White Team (WT), led by the White Team Lead (WTL), knows about the test;
  - the Blue Team (BT) which comprises all staff at the Participating entity who are not part of the WT. The BT is unaware of the test;
- The TIBER-LU Cyber Team (TCT) of the BCL and CSSF;
- The third-party providers, e.g. Red Team provider and the Threat Intelligence provider;

[2] As stated in the TIBER-EU framework, « Overall, it is the respective entity – and not the authorities – that bears the first and final responsibility for conducting the test. »

Figure 1 – Overview of TIBER-LU stakeholders



B) Process overview

The TIBER-LU test consists of four phases:

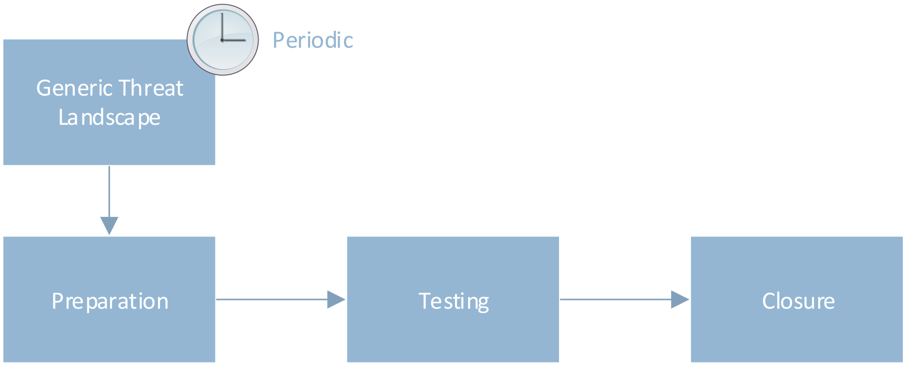
- The **Generic Threat Landscape** aims at producing a report that shows the role of the Participating entity in the ecosystem, the threat actors (including their TTP[3]s and MO[4]s) and the expected threat actor motivations. This document will, where possible, be enriched and reviewed with the input from Governmental Intelligence (GI) agency. It is an optional step in the TIBER-LU[5].
- During the **Preparation Phase**, the TIBER-LU test is formally launched, the WT is established, the scope of the test is determined and the RT and TI provider(s) is(are) procured.
- During the **Testing Phase**, the RT provider and/or TI provider enrich the generic intelligence with target intelligence, develop attack scenarios and the RT provider prepares a test plan and executes it with the objective of capturing the flags.
- During the **Closure Phase**, a replay of the executed scenarios will take place between the BT and the RT. The Participating entity remediation plan is finalized. The process is reviewed and detection and response capabilities are assessed. Participating entities may decide to share findings with peers. The Participating entities inform their respective supervisor and/or overseer about the TIBER-LU test in their regular meetings.

[3] Techniques, tactics and procedures

[4] Modus operandi

[5] Depending on the interest of TIBER-LU Participating entities the GTL may be available

Figure 2 – Overview of TIBER-LU process



C) Test management

a) Introduction

A TIBER-EU test requires the involvement of a number of different stakeholders with clearly defined roles and responsibilities. All main stakeholders involved in a TIBER-LU test should be well informed about their respective roles and responsibilities to ensure that:

- the test is conducted in a controlled manner;
- there is a clear protocol for the flow of information across all relevant stakeholders throughout the test; and
- the information flow protocol is clear on how information will be stored and shared between stakeholders.

For more clarity on the roles and responsibilities of the different stakeholders involved in the overall process of the TIBER-LU, a Responsibility Assignment (RACI) Matrix is included in Annex 3.

b) TIBER-LU Cyber Team (TCT)

The role of the TCT is to manage, operationalise and monitor the TIBER-LU framework implementation and each of the TIBER-LU tests carried out in this context. Most importantly, the TCT will act as an operational control to ensure uniform, high quality tests containing all the mandatory elements defined in the TIBER-LU Framework. In addition, the TCT is responsible for continuously updating the TIBER-LU Implementation Guide in light of lessons learnt from its implementation and the tests carried out. This will be done on a continuous basis in collaboration with the institutions participating in TIBER-LU, but also with authorities in other jurisdictions that have adopted TIBER-EU, incl. the ECB. The TCT will also review and update TIBER-LU, where appropriate, in light of relevant regulatory developments.

At the BCL, the TCT is organizationally placed in the *Oversight* section of the *Market infrastructures and Oversight* department *(IMO).* Arrangements will be made to separate the TIBER related information from regular Oversight activities.

At the CSSF, the TCT is organizationally placed in the Supervision of Information systems section (SU.S.I.) of the Supervision of Information systems and Support PFS department (PSF-SU). Arrangements will be made to separate the TIBER related information from regular Supervision activities.

The formal ownership of TIBER-LU rests with the BCL and CSSF Boards of Directors.

c) Responsibilities of White Team and White Team lead

For a TIBER-LU test, a White Team with one dedicated White Team Lead will be responsible for managing the test. The White Team Lead should coordinate all test activity including engagement with the TI/RT providers and meetings with the TCT. More details on the roles, responsibilities and composition of the White Team can be found in the TIBER-EU White Team Guidance.

The responsibility for the overall planning lies with the Participating entity. The WTL within the Participating entity coordinates all activity including engagement with the service provider(s).

Service provider(s) produce a planning for their services and inform the Participating entity so they can be factored into the overall TIBER-LU test project planning. Significant deviations in the original planning will be discussed with the TCT. The TCT has direct access to the service providers when needed.

The TCT will indicate its non-objection on the scope and the scenarios and ensures that the test is executed according to plan and is up to the standards of a TIBER-LU test. There has to be close cooperation between the TCT and the WTL and individual roles and responsibilities should be respected. When crucial decisions need to be made (e.g. deviations, during the test, from the scope agreed on) or unclarities or diverging opinions emerge, the TCT will be informed.

TIBER-LU tests should be a learning experience and should thus be underpinned by a collaborative, transparent and flexible working approach by all parties involved.

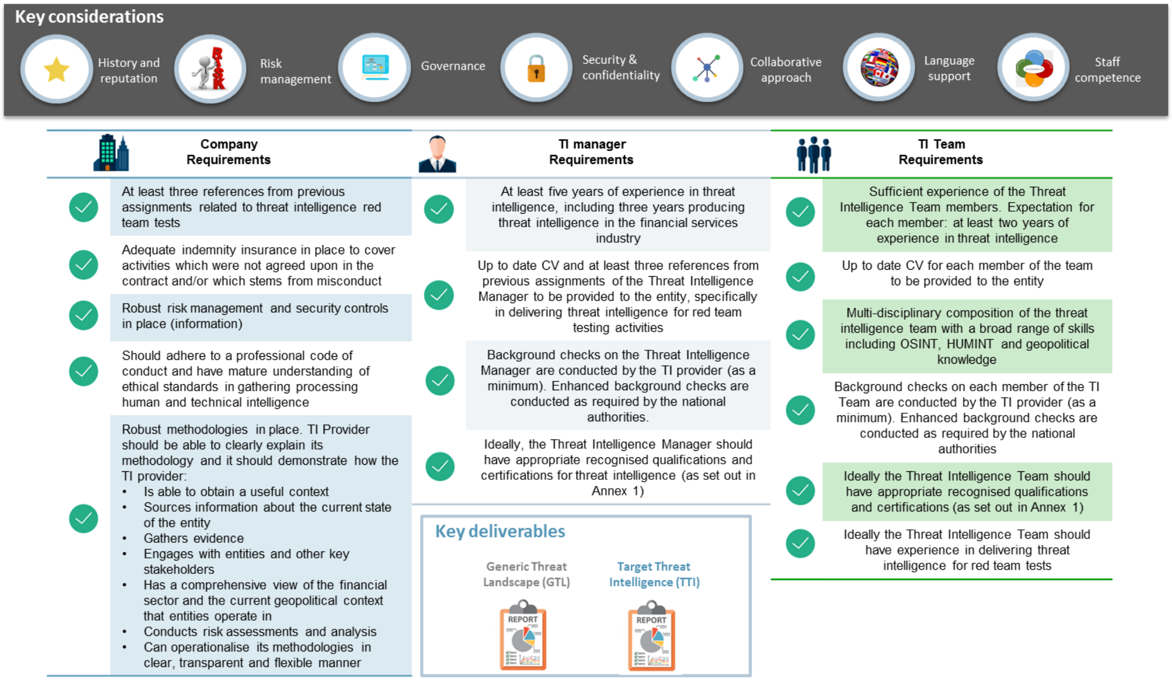
d) Third-party providers

To be recognized as a TIBER-LU test, a test will have to be conducted by independent third-party providers. For each TIBER-LU test, two types of providers will be involved:

- The threat intelligence (TI) provider should provide threat intelligence to the Participating 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 up to date as possible.
- The red team (RT) test provider plans and executes a TIBER-LU test of the target systems and services, which are agreed in the scope of the test. This is followed by a review of the test and the issues arising, culminating in a red team test report drafted by the provider.

Prior to the engagement, the Participating entity must ensure that the providers meet the minimum requirements as stipulated in the TIBER-EU Services Procurement Guidelines.

Figure 3 – TI Provider requirements overview



Key considerations

Company Requirements

- ✓ At least three references from previous assignments related to threat intelligence red team tests
- ✓ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stems from misconduct
- ✓ Robust risk management and security controls in place (information)
- ✓ Should adhere to a professional code of conduct and have mature understanding of ethical standards in gathering processing human and technical intelligence
- ✓ Robust methodologies in place. TI Provider should be able to clearly explain its methodology and it should demonstrate how the TI provider:
  - Is able to obtain a useful context
  - Sources information about the current state of the entity
  - Gathers evidence
  - Engages with entities and other key stakeholders
  - Has a comprehensive view of the financial sector and the current geopolitical context that entities operate in
  - Conducts risk assessments and analysis
  - Can operationalise its methodologies in clear, transparent and flexible manner

TI manager Requirements

- ✓ At least five years of experience in threat intelligence, including three years producing threat intelligence in the financial services industry
- ✓ Up to date CV and at least three references from previous assignments of the Threat Intelligence Manager to be provided to the entity, specifically in delivering threat intelligence for red team testing activities
- ✓ Background checks on the Threat Intelligence Manager are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities.
- ✓ Ideally, the Threat Intelligence Manager should have appropriate recognised qualifications and certifications for threat intelligence (as set out in Annex 1)

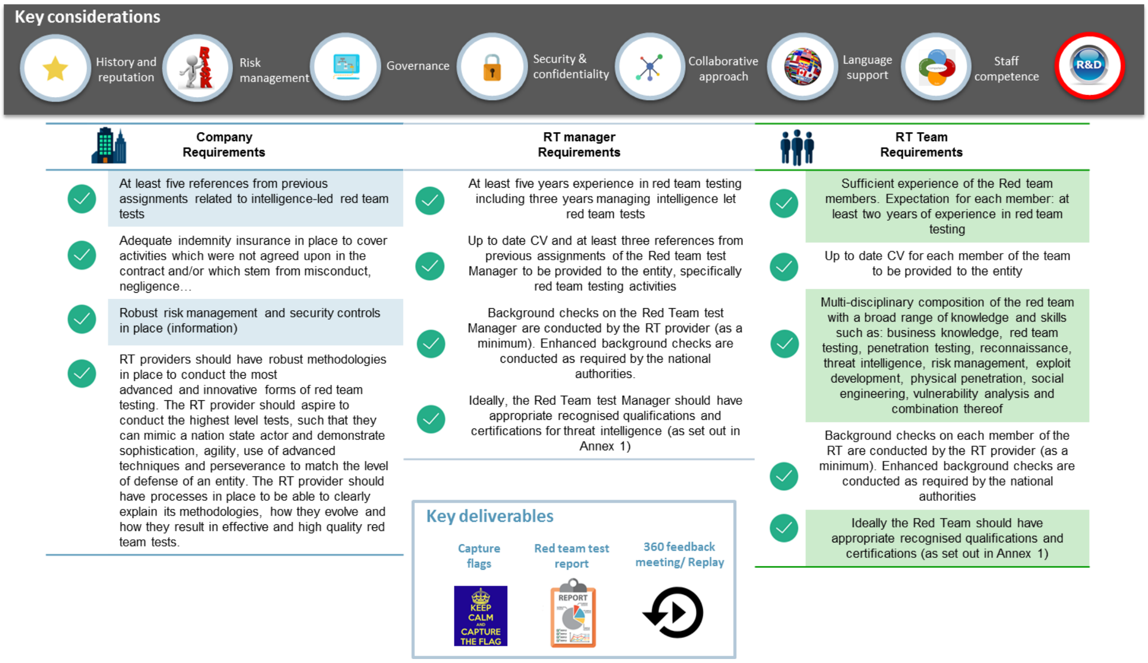
Key deliverables

Generic Threat Landscape (GTL)
Target Threat Intelligence (TTI)
REPORT
REPORT

TI Team Requirements

- ✓ Sufficient experience of the Threat Intelligence Team members. Expectation for each member: at least two years of experience in threat intelligence
- ✓ Up to date CV for each member of the team to be provided to the entity
- ✓ Multi-disciplinary composition of the threat intelligence team with a broad range of skills including OSINT, HUMINT and geopolitical knowledge
- ✓ Background checks on each member of the TI Team are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities
- ✓ Ideally the Threat Intelligence Team should have appropriate recognised qualifications and certifications (as set out in Annex 1)
- ✓ Ideally the Threat Intelligence Team should have experience in delivering threat intelligence for red team tests

Figure 4 – RT Provider requirements overview



Key considerations

Company Requirements

- ✓ At least five references from previous assignments related to intelligence-led red team tests
- ✓ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence…
- ✓ Robust risk management and security controls in place (information)
- ✓ RT providers should have robust methodologies in place to conduct the most advanced and innovative forms of red team testing. The RT provider should aspire to conduct the highest level tests, such that they can mimic a nation state actor and demonstrate sophistication, agility, use of advanced techniques and perseverance to match the level of defense of an entity. The RT provider should have processes in place to be able to clearly explain its methodologies, how they evolve and how they result in effective and high quality red team tests.

RT manager Requirements

- ✓ At least five years experience in red team testing including three years managing intelligence let red team tests
- ✓ Up to date CV and at least three references from previous assignments of the Red team test Manager to be provided to the entity, specifically red team testing activities
- ✓ Background checks on the Red Team test Manager are conducted by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities.
- ✓ Ideally, the Red Team test Manager should have appropriate recognised qualifications and certifications for threat intelligence (as set out in Annex 1)

Key deliverables

RT Team Requirements

- ✓ Sufficient experience of the Red team members. Expectation for each member: at least two years of experience in red team testing
- ✓ Up to date CV for each member of the team to be provided to the entity
- ✓ Multi-disciplinary composition of the red team with a broad range of knowledge and skills such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combination thereof
- ✓ Background checks on each member of the RT are conducted by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities
- ✓ Ideally the Red Team should have appropriate recognised qualifications and certifications (as set out in Annex 1)

e) Risk management

It is of the utmost importance that the WT 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, assessed and mitigated according to the Participating entity's own Enterprise Risk Management framework. At any time, the WT can order a temporary halt if concerns are raised over damage or potential damage to a system.

For limiting risks, the TIBER-EU framework provides for a number of practices to be followed such as:

- Conduct a risk assessment prior to the TIBER-LU test and continuously monitor risks during the test;
- Execute the test in a planned and controlled manner;
- Conduct due diligence on "in-scope systems" to ensure back-up and restoration is in place ahead of the start of the TIBER-LU test;
- Procure providers that fulfil minimum requirements as set-out in the TIBER-EU Services Procurement Guidelines and make sure there is a mutual agreement on at least the following aspects: scope of the test, boundaries, timing and availability of the providers, contracts, actions to be taken and liability (including insurance where applicable);
- Use accredited providers when there is such a mechanism in place at European level;
- Limit the awareness of the TIBER-LU test to the smallest group possible, use Non-Disclosure Agreement (NDAs) where relevant and appropriate;
- WT members should be positioned at the top of the security incident escalation chain to prevent miscommunication and avoid knowledge about the TIBER-LU test being leaked;
- Use of code-naming to secure the information flow regarding the TIBER-LU test.

It is ultimately the responsibility of the WT to ensure that all precautions are taken during the entirety of the TIBER-LU test.

The testing should be flexible enough to mimic the (seen, current and potential future) actions of a real attacker and should be performed in a planned and controlled manner in order to (amongst other things) ensure uniform testing, protect those involved (e.g. indemnifications) and prevent damage. Both elements are essential in order to make sure the Participating entity and its peers can learn and evolve, not only using their own but all relevant results and findings.

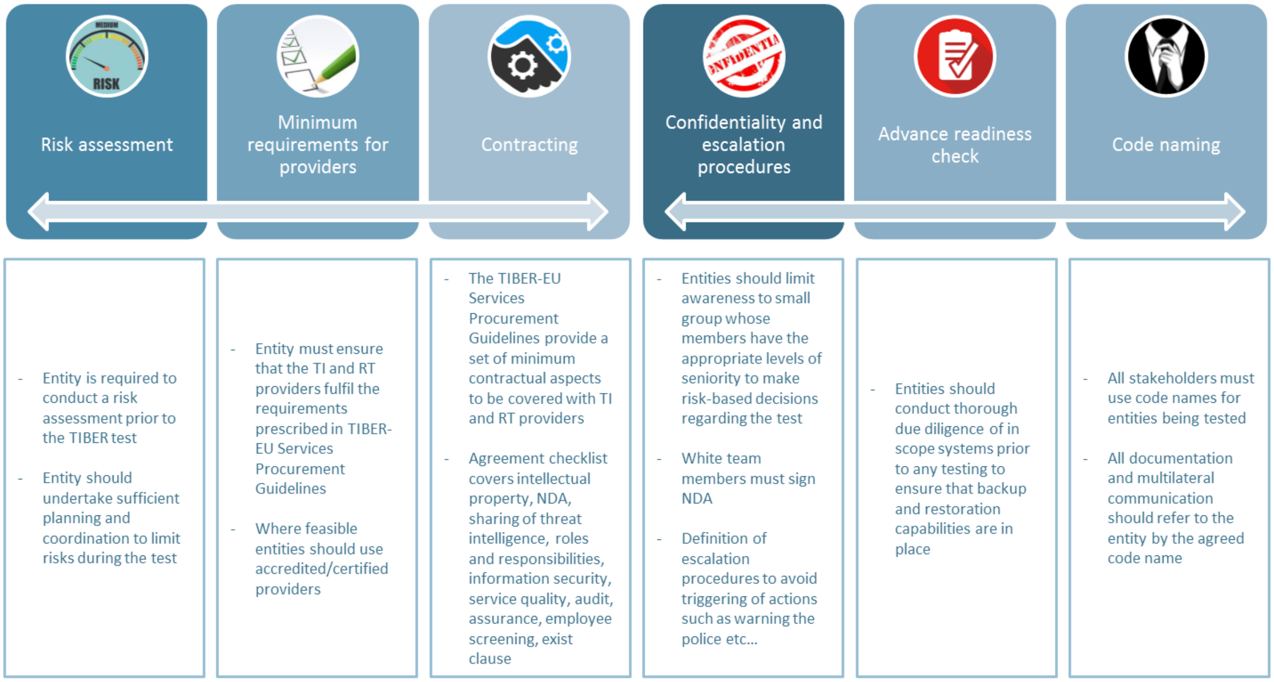
The following actions are examples of activities that are not allowed during the test:

- destruction of equipment;
- uncontrolled modification of data / programs;
- jeopardising continuity of critical services;
- blackmail;

- threatening or bribing employees;
- disclosure of results.

Intentional interception or recording of communication in which the RT provider does not participate, should only take place in accordance with applicable legislation. Personal data should only be collected and processed when absolutely necessary, and in accordance with applicable legislation.

Figure 5 - Risk management during a TIBER-LU test



Risk assessment	Minimum requirements for providers	Contracting	Confidentiality and escalation procedures	Advance readiness check	Code naming
- Entity is required to conduct a risk assessment prior to the TIBER test - Entity should undertake sufficient planning and coordination to limit risks during the test	- Entity must ensure that the TI and RT providers fulfil the requirements prescribed in TIBER-EU Services Procurement Guidelines - Where feasible entities should use accredited/certified providers	- The TIBER-EU Services Procurement Guidelines provide a set of minimum contractual aspects to be covered with TI and RT providers - Agreement checklist covers intellectual property, NDA, sharing of threat intelligence, roles and responsibilities, information security, service quality, audit, assurance, employee screening, exist clause	- Entities should limit awareness to small group whose members have the appropriate levels of seniority to make risk-based decisions regarding the test - White team members must sign NDA - Definition of escalation procedures to avoid triggering of actions such as warning the police etc…	- Entities should conduct thorough due diligence of in scope systems prior to any testing to ensure that backup and restoration capabilities are in place	- All stakeholders must use code names for entities being tested - All documentation and multilateral communication should refer to the entity by the agreed code name

f) Cross-border collaboration

The TIBER-LU framework relies on the principles exposed in TIBER-EU Framework in section 3.10 for the cross-border collaboration.

III) Generic Threat Intelligence

The following sections provide insights on the input and outputs of each phase and sub-phase. Note that the "Who" column reflects the involvement of the parties in the process. The respective responsibilities are detailed in the text and also reflected in the RACI available in Annex 1.

A) Overview

Generic Threat Intelligence will be provided by the Service Provider selected by the Participating entity(ies) (if any). The Generic Threat Landscape (GTL) report is an input to the Testing phase as context for the work of TI provider in designing the Targeted Threat Intelligence report and for the RT provider to design the attack scenarios.

The Generic Threat Intelligence consists of:

- Threat actor intelligence on the most advanced actors relevant for the Luxembourg's financial institutions in the ecosystem;
- Additional information regarding the position of the Participating entity in the ecosystem and its critical functions that may be of interest to advanced attackers (threat actor aims)

Who	**Input**	**Output**
Service Provider	OSINT, TI service provider, GIA…	Generic Threat Landscape report

B) Government Intelligence Agencies (GIA)

Government Intelligence Agencies may validate and enrich the threat intelligence provided and the high-level scenarios.

IV) Preparation phase

A) Overview

The TIBER-LU preparation phase is composed of the following main sub-phases:

- Pre-launch
- Procurement
- Launch
- Scoping

During the TIBER-LU preparation phase, the project is formally launched and the TCT starts engaging with the Participating entity. The scope is established and the Participating entity procures the service provider(s). The duration of this phase is approximately four to six weeks, not including the procurement process itself that may be longer.

B) Pre-launch

The pre-launch meeting marks the start of the planned and agreed TIBER-LU process for each Participating entity. The TCT will request the establishment of a White Team and White Team Lead once notified by the Participating entity of its intent to conduct a TIBER-LU test. The Participating entity should refer to the TIBER-EU White Team Guidance and can contact the TCT for guidance.

A pre-launch meeting[6] will be held so that the TCT briefs the Participating entity on the:

- TIBER-LU requirements and implementation guide, other templates
- Roles and responsibilities
- Security protocols (document transfer means and code word)
- Contractual considerations
- Project planning and risk management

The White Team should, as early as possible, elaborate its TIBER-LU Test Project Plan taking into consideration timelines, procurement, etc. to ensure that there are no bottlenecks or delays in the overall testing process.

The pre-test risk assessment to be performed by the WT may have started ahead of the pre-launch meeting or after it, but in any case, should be performed at least before discussing the scope.

Finally, during the pre-launch, the WTL will share with the TCT the list of intended providers (i.e. TI and RT) and submit it for information before going further with the **Procurement** sub-phase.

The inputs and outputs of the **Pre-launch** sub-phase in terms of documents and main deliverables are the following:

[6] Organisational aspects to be clarified bilaterally with the entity regarding location etc.

Who	Input	Output
TCT	TIBER-LU Implementation Guide	
TCT	TIBER-EU White Team Guidance	
TCT	TIBER-EU Services Procurement Guidelines	
TCT	TIBER-EU Scoping document Template	
TCT	TIBER-EU Attestation Template	
TCT	TIBER-EU Scope Specification Template	
TCT	TIBER-EU Targeted Threat Intelligence Guidance	
TCT	TIBER-EU Red Team Test Plan Guidance	
TCT	TIBER-EU Guidance for Red Team Test Report	
TCT	TIBER-EU Guidance for Test Summary Report	
WT;WTL	List of potential TI/RT providers	
WT;WTL	Code word	Code word shared in the pre-launched meeting
WT;WTL		Security protocols for communication

C) Procurement

After the pre-launch meeting, the WT should start its procurement process. Responsibility for ensuring that the appropriate TI/RT providers are selected lies solely with the Participating entity White Team. In particular, as stated earlier, the TI and RT providers should fulfill the criteria specified in the TIBER-EU Services Procurement Guidelines.

Once the TI and RT providers have signed NDAs, the WTL can issue the tender or procurement procedure to procure TI and RT providers. The WTL should provide the TIBER-LU Implementation Guide and the other relevant templates.

The WT should make sure to control the confidentiality by also requiring NDAs with the involved internal support functions (i.e. procurement) to avoid leaking of information.

Upon receipt from the TI and RT provider responses, the WTL provides the materials to the TCT, which provides a non-objection. The WTL will then interview and select appropriate providers. The contracts should fulfil the requirements stated in the TIBER-EU Services Procurement Guidelines and establish conditions governing the sharing, confidentiality and retention of intellectual property rights.

Following the procurement, the White Team should complete its TIBER-LU Test Project Plan, including the schedule of meetings to be held between the WT, TI/RT providers and TCT, and share this with the relevant stakeholders.

The inputs and outputs of the **Procurement** sub-phase in terms of documents and main deliverables are the following:

Who	**Input**	**Output**
WT;WTL	NDA	
TI;RT		Signed NDAs
WT;WTL	Tender	
TI;RT		Tender responses
WT;WTL		TI and RT procured, contracts signed
WT;WTL		TIBER-LU Project Plan

Note: The White Team may apply a degree of flexibility on the timing of the procurement. Hence, the White Team may start the procurement process in **parallel with the pre-launch**, or do so only once the **pre-launch** and **scoping** have been completed.

D) Launch

Since cooperation is key for a successful TIBER-LU test, the **launch meeting** is a meeting that should involve all the relevant stakeholders (including the TCT, WT, WTL and TI/RT providers). During this meeting, all stakeholders discuss the test process and their expectations, as well as the draft TIBER-LU Project Plan, which should be prepared by the WT and WTL. The earlier made agreements about security and communication protocols and the chosen code name should be shared with the TI and RT providers.

Initial discussions regarding the scoping will also take place which will allow the WT and WTL to draft the TIBER-EU Scope specification document after the meeting.

The inputs and outputs of the **Launch** sub-phase in terms of documents and main deliverables are the following:

Who	**Input**	**Output**
WT;WTL;TI;RT	TIBER-LU Project Plan	
WT;WTL	Code word	
WT;WTL	Security and communication protocols	
Service Provider	Generic Threat Landscape report (if available)	
WT;WTL;TI;RT;TCT	Scope discussion	TIBER-EU Scope Specification Document DRAFT

E) Scoping

The scoping sub-phase is composed of two main components, i) the Scoping meeting where the TCT and WT-WTL discuss the draft TIBER-EU Scope Specification document and ii) the Scoping presentation meeting where the final TIBER-EU Scope Specification document, as approved by the Board of the Participating entity, is presented to the TI and RT providers.

a) Scoping meeting

The purpose of the Scoping meeting is for the TCT and WT, on the basis of the Scope specification document, to agree on the scope of the test and the identification of the critical functions. Both the TCT and the WT should have extensive knowledge of Participating entity's business model, functions and services.

After the Launch meeting, the WT must draft a TIBER-EU Scope Specification document. The TIBER-EU Scope Specification sets out the scope of the TIBER-EU test, and lists the key systems and services that underpin each critical function. This information will help the WT set the "flags" to be captured, which are essentially the targets and objectives that the RT providers must strive to achieve during the test, using a variety of techniques. A specific guidance was issued for this document.

The WT should discuss the TIBER-EU Scope Specification document and the flags with the TCT, who should not object to them during the **Scoping meeting**. Flags are placed on the critical systems in the TIBER-EU Scope Specification document. These flags form the goal for the later test scenarios which are based on relevant threat intelligence. The Participating entity is allowed to involve the RT Provider and TI Providers in the scoping process.

Note: Although the flags are set during the scoping process, they can be changed by the WT on an iterative basis following the threat intelligence gathering and as the red team test evolves. The TCT shall be notified of such changes.

b) Scoping presentation meeting

For a successful test it is important that the TI and RT service providers understand the business of the Participating entity. Therefore, after the 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 critical functions and systems underpinning them (compromising these is the test objective) are explained. If the Participating entity feels that further interaction on the functioning of its business is necessary to arrive at realistic scenarios this is very much encouraged.

The inputs and outputs of the **Scoping** sub-phase in terms of documents and main deliverables are the following:

Who	**Input**	**Output**
WT;WTL	Draft TIBER-EU Scope Specification	Final TIBER-EU Scope Specification
Board	Final TIBER-EU Scope Specification	Approval
WT;WTL		TIBER-LU Project Plan

V) Testing phase

A) Overview

The Testing phase is composed of two main sub-phases, the i) Targeted Threat Intelligence phase and the ii) Red Team phase. The Testing phase aims at producing attack scenarios using the Targeted Threat Intelligence so that the red team captures the flags as defined in the Scoping phase.

Threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the success of testing activities. The duration of the threat intelligence process in this phase is approximately six to eight weeks but may be extended.

B) Targeted threat intelligence

The Targeted Threat Intelligence sub-phase is a gathering and analytical exercise. The TI provider will gather information from i) the GTL if available, ii) the Scope specification document, iii) the Participating entity (on a voluntary basis), and iv) its own researches (OSINT, HUMINT, TECHINT, passive reconnaissance, digital footprint …) in order to produce a draft Targeted Threat Intelligence (TTI) report using the appropriate guidance, in particular the eight steps of the TIBER Threat Intelligence Model[7].

[7] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

The draft report will be reviewed during the TTI Report review meeting with WT, WTL, TI and RT Provider and TCT. After the meeting, the TTI report and the attacks scenarios will be finalized.

In case the participating entities have elected for a GTL to be available, it will serve as basis for the Targeted Threat Intelligence and scenarios.

Who	Input	Output
WT	Generic Threat Landscape report (if available) and Scope Specification document	
TI		Targeted Threat Intelligence report and Threat scenarios

C) Red team test plan and scenarios

This sub-phase represents the key transition point between the TI and RT providers. Using the scenarios contained in the TTI Report, and in line with the TIBER-EU Test Scope Specification, the RT provider should develop and integrate the attack scenarios into a draft Red Team Test Plan using the appropriate guidance. A RT test plan review meeting will be held with WT, WTL, TI and RT Provider and TCT. After the meeting the final RT test plan will be finalized. In case of significant deviation of RT Attack Scenarios from the Threat Scenarios outlined in the TI report this must be approved by WT and the TCT should be informed.

Who	Input	Output
TI	Targeted Threat Intelligence report and Threat scenarios	
WT	Scope specification document	
WT	Generic Threat Landscape	
RT		RT Test plan

D) Red teaming

A kick-off meeting will be held with WT, WTL, TI and RT Provider and TCT ahead of the start in order to signify the start of the RT test, agree on communication and escalation protocols.

The RT provider will move into execution of the RT Test, during which the RT provider performs a stealthy intelligence-led red teaming exercise against the Participating entity's target systems. The RT Test takes approximately twelve weeks, or longer if felt necessary. The scenarios are not a prescriptive runbook which must be followed precisely during the test. If obstacles occur, the RT provider should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective. This is of course always done in close contact with the WT and the TCT. All actions of the RT provider are logged for replay with the BT, evidenced for the Red Team Report and future reference.

The test objectives (compromise actions) are the 'flags' that the RT provider must attempt to capture during the test as it progresses through the scenarios. Of course, all captures are performed in close cooperation with the WT and the overall aim is to improve the BT capabilities. The scenario is to be played out from beginning to end. The RT provider may need some help to overcome barriers, it may be discovered, etc. but the scenario must continue to make full use of the TIBER-LU exercise within the given timeframe and test all phases of the test.

RT providers are constrained by the time and resources available as well as by moral, ethical and legal boundaries. Therefore, the RT providers may require occasional steers from the WT to help them progress. Should this happen, these steers are duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

At all times the RT provider liaises closely with the WT and with the TCT. The TCT is updated at least once a week by the RT provider and WT on the progress. Meetings between the WT, TCT and RT provider during this phase are strongly encouraged since the discussions add significantly to the quality of the test.

Who	**Input**	**Output**
RT	RT Test plan	
WT;WTL	Leg-up	
RT		RT Actions log

VI) Closure phase

A) Overview

The duration of the closure phase is approximately six weeks.

During the closure phase, the RT provider will produce a RT Test report. The BT will in its turn create a BT Test report. The Replay Workshop will be the opportunity for the RT to explain their approaches and see where BT reacted and where it didn't. Potentially, Purple Teaming will also be performed, i.e. RT and BT will run through new scenarios/techniques to see how it would have affected the entity's defences. A 360 Workshop will also be held in order to review the TIBER process itself and feed the TIBER-Knowledge Center with proposals for improvements. The entity will also create a remediation plan to overcome weaknesses discovered during the RT test. Overseers and supervisors in their regular activities will follow up on the remediations. A summary test report will be produced and shared with authorities on a pre-agreed basis. Finally, the Board of the entity will approve and sign an attestation to confirm the test was executed in accordance with TIBER-EU framework. The TI and RT providers will also sign this attestation.

B) RT and BT Reports

The RT Provider will deliver within two weeks from the end of the test a RT Test report which will describe all actions taken by the RT providers during the test, the different proofs of flags' capture, potential areas of improvements of the BT in the areas of technical controls, policies and procedures and education and awareness.

The BT will use the RT report to build its BT report, i.e. put alongside RT's actions its different responses.

Who	**Input**	**Output**
RT		RT Test report
BT	RT Test report	BT Test report

C) Replay workshop(s)

The Replay Workshop aims at replaying the steps performed by both the RT and BT, and to maximize the learning on both sides. Additionally, a purple teaming element should be added in which the BT and the RT work together to see which other steps could have been taken by the RT and how the BT could have responded to those steps.

The RT provider should also offer an opinion as to what else could have been achieved with more time and resources, as genuine threat actors are not constrained by the time and resources limitations of TIBER-LU.

An Overseer/Supervisor specific replay workshop will be organized as well to share sanitized results with the authorities of the entity.

Who	**Input**	**Output**
RT;BT	RT Test report; BT Test report	
WTL		Draft TIBER-LU Test summary

D) 360° Feedback Workshop

During the 360° feedback meeting, the WT, WTL, BT, TCT, TI and RT provider(s) come together to review the TIBER-LU exercise. The TCT arranges and facilitates the workshop. In the 360° feedback report, all parties deliver feedback to each other. Goal is to further facilitate the learning experience of all those involved in the process for future exercises.

An anonymized version of the 360° Report with key findings relevant for TIBER-EU will be shared with the TIBER-Knowledge Center.

Who	Input	Output
WT;WTL;RT;TI;TCT	360° Feedback Workshop	360° Feedback Report
TCT	360° Feedback Report	360° Feedback Report – Findings for TIBER-Knowledge Center

E) Remediation plan

Once the Replay Workshop has occurred, the WT, WTL should draft a Remediation Plan for implementing improvements to mitigate the vulnerabilities identified during the TIBER-LU test. It includes findings from both RT Reports and TI Reports.

Who	Input	Output
WTL;WT;TCT	RT Test report; BT Test report	Remediation plan draft

F) TIBER-LU Test summary, attestation

A TIBER-LU Test summary report describing the overall test process and results (including the Remediation Plan) will be shared with the TCT. Upon finalization of the Test summary report, the Board of the entity will approve it and sign an attestation that the test was executed in accordance with TIBER-EU framework. The TI and RT providers will also sign this attestation. The attestation validates the true and fair conduct of the test according to the TIBER-EU Framework and enable mutual recognition with other relevant authorities, where relevant.

Who	Input	Output
WTL;TCT	Draft TIBER-LU Test summary	Final TIBER-LU Test summary
Board	Final TIBER-LU Test summary	Approval and Signed certification

G) Information sharing

As one of the main goals of TIBER-LU is enhancing the sector's resilience against advanced cyber attackers and financial stability, the Participating entities are invited to share specific information regarding weaknesses with relevant peers promptly to enhance the cyber resilience of the sector and financial stability.

The Participating entities may share more general lessons learned via the TIBER-LU Test Summary report. The TCT and the WT will discuss the forum for sharing the information and the level of detail.

VII) Oversight and Supervision

The TCT does not proactively share TIBER-LU-related information or documentation regarding a specific institution with the BCL’s Oversight team or with the CSSF’s Supervisory team.

After the TIBER-LU Test has been completed, the TCT will notify both Oversight and Supervisor that the test has ended.

On its own initiative or upon request from the Overseers and/or Supervisors, the Participating Entity will share the Remediation Plan with them. The Remediation Plan will be followed-up by the Overseers and Supervisors in accordance with their respective mandates. The TIBER-LU Test Summary report will also be shared with them.

Annex 1: TIBER-EU requirements

Preparation phase	Mandatory and adopted	Not Adopted	Optional
For each test, there is a White team (WT), independent TCT (and Test Manager) and external TI/RT provider(s).	✓		
For each test, the national intelligence agency/national cyber security centre/hi-tech crime unit is involved.			✓
Once the procurement phase has been completed, there are appropriate contracts in place between the different stakeholders, with relevant controls embedded into the contracts, to facilitate a controlled test (in a discreet manner).	✓		
Prior to conducting the test, the WT conducts a risk assessment and thereafter puts in place all the risk management controls, processes and procedures to facilitate a controlled test.	✓		
Throughout the end-to-end test process, all documentation and communication between stakeholders, uses a code name to replace the identity of the financial institution being tested.	✓		
At the outset of the test process, there is a launch meeting which includes the WT and TCT.	✓		
The launch meeting also includes other relevant authorities and the TI/RT providers.	✓		
The scope of the test includes Critical Functions (CFs), including the people, processes and technology and databases that support the delivery of CFs. This is documented in the TIBER- EU Scope Specification document and signed off in the attestation by the Board.	✓		
The financial institution expands the scope of the test beyond the CFs and includes other functions and processes.			✓
During the scoping phase, the WT (with agreement from the TCT), sets "flags" which are targets or objectives, that the RT provider aims to meet during the test.	✓		
The test is conducted on live production systems.	✓		
Only the WT and TCT are informed about the test, its details and timings – all other staff members (i.e. Blue Team) remain unaware of the test.	✓		
Only TI/RT providers that meet the minimum requirements set out in the TIBER-EU Services Procurement Guidelines can undertake the TIBER-LU test. Once there is capability within the EU, the TI/RT providers are TIBER-LU certified and accredited.	✓		

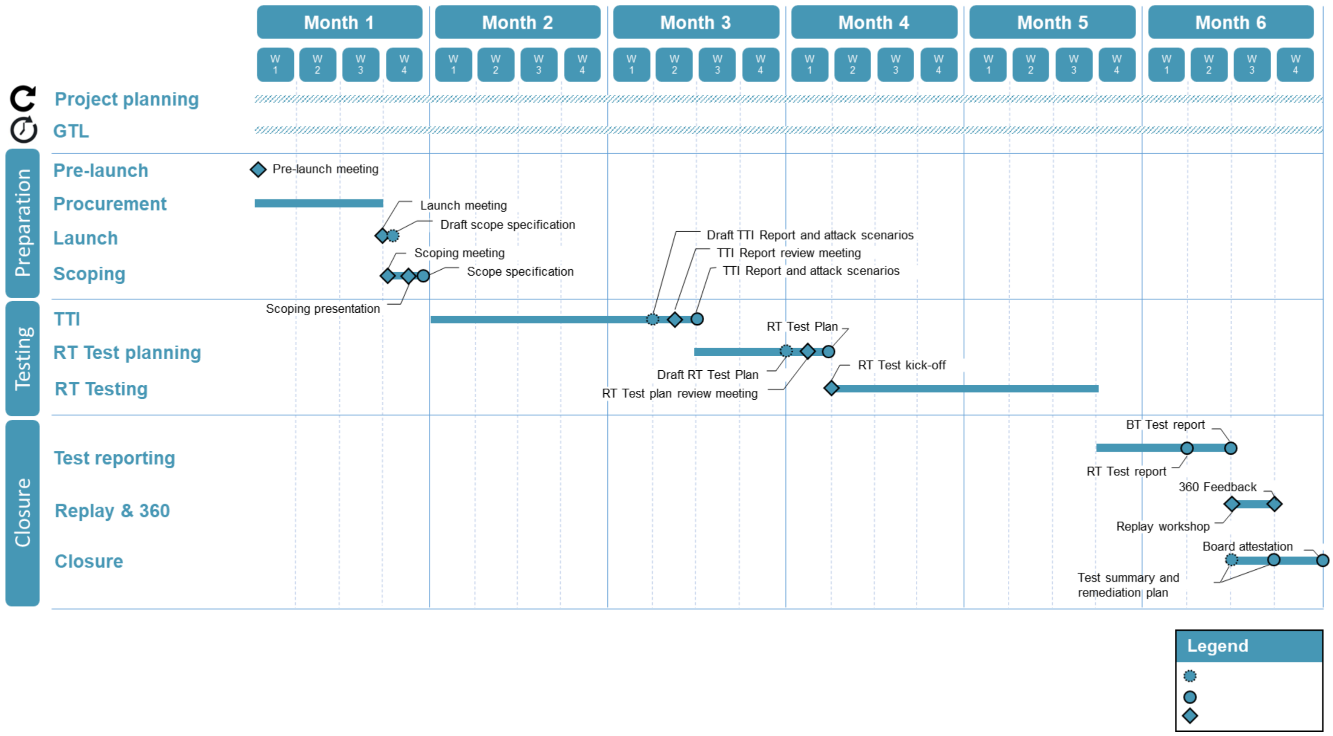
Threat Intelligence and Red Team Testing phase	Mandatory and Adopted	Not adopted	Optional
For each test, an external TI provider produces a dedicated Targeted Threat Intelligence (TTI) report on the financial institution being tested. Where infrastructure has been outsourced and a third party is included in scope, the TTI report also includes information about that third party.	✓		
For each national implementation, a Generic Threat Landscape (GTL) report for its financial sector is produced and maintained, and is used to help inform the TTI report.			✓
For each threat intelligence report (TTI & GTL), the national intelligence agency/national cyber security centre/hi-tech crime unit is involved to provide feedback.			✓
For each TTI report on the institution, the TI provider sets out multiple threat scenarios which can be used by the RT provider.	✓		
The TI provider holds a handover session with the RT provider, providing the basis of the threat scenarios.	✓		
During the testing phase, following the handover, the TI provider continues to be engaged and provides more current and credible TI to the RT provider, if and when needed.	✓		
The RT provider develops multiple attack scenarios, based on the TT*I report. This is documented in the Red Team Test Plan and shared with the WT and TCT.*	✓		
The jurisdiction, in its implementation of the TIBER framework, allows Physical Red-Teaming in scope of the methodology for the TIBER test (e.g. planting a device at the financial institution), as long as all necessary precautions are taken.			✓
The RT provider executes the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and goes through each of the phases of the kill chain[8] methodology. When needed, a leg-up will be provided by the financial institution.	✓		
During the test, the RT provider keeps the WT and TCT informed about progress, capture the flag moments, possible need for leg-ups, etc. The RT provider takes a staged approach, and consults the WT and TCT at all critical points, to ensure a controlled test.	✓		

[8] https://attack.mitre.org/resources/enterprise-introduction/

The duration of the Red Team test is proportionate to the scope, size of the financial institution, complexity of threat scenarios, etc. Sufficient and adequate time is allocated to testing, to guarantee a comprehensive test has been conducted across the enterprise. Experience suggests at least 12 weeks are required.	✓

Closure phase	Mandatory and Adopted	Not adopted	Optional
At the end of the test, the RT provider produces a Red Team Test Report, outlining the findings from the test.	✓		
The financial institution's Blue Team (BT) is informed of the test and uses the Red Team Test Report to deliver its own Blue Team report. In the Blue Team report, the Blue Team maps its actions alongside the RT provider's Team actions.	✓		
At the end of the test, the RT provider, BT and WT conduct an interactive replay of the test, where possible with live production systems to replay the impact of the actions of the RT provider.	✓		
The TCT, overseers/supervisor and TI provider are also present during these replay workshops.	✓		
A purple teaming element is added in which the BT and the RT provider can work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps.	✓		
At the end of the test, there is a 360 feedback meeting which includes the financial institution, TI/RT providers and TCT. This meeting reviews the TIBER-LU test process and allows all parties to deliver feedback.	✓		
After the BT and RT provider replay and 360 feedback workshop, the financial institution produces a Remediation Plan to address the findings. The Remediation Plan is agreed with the supervisor and/or overseer as part of their planning and control cycle.	✓		
The financial institution produces a Test Summary Report, which it shares with the lead authority.	✓		
The financial institution's Board and the TI/RT providers sign an attestation to validate the true and fair conduct of the TIBER-EU test (to enable mutual recognition amongst other relevant authorities, if applicable).	✓		
If mutually agreed, the lead authority and/or the financial institution share the Test Summary report and Attestation with other relevant authorities (when applicable).	✓		
The TCT in each jurisdiction analyses the results of all the TIBER tests and the lessons learned from the 360 feedback meetings, from that jurisdiction, to produce high level, aggregated findings. This information is used to enhance sector resilience and improve the TIBER-XX framework.	✓		

Annex 2: High level planning



Annex 3: RACI matrix

Requirement	Responsible	Accountable	Consulted	Informed	Documents
Adoption and implementation					
The TIBER-LU framework is adopted and implemented	BCL and CSSF	Executive Board	Executive Board	Executive Board	TIBER-LU Implementation Guide
Preparation phase					
Pre-launch meeting	TCT	TCT	WT	n/a	TIBER-LU Implementation Guide, TIBER-EU Services Procurement Guidelines, TIBER-EU White Team Guidance *Other templates*
Launch meeting	WT	Board of the Participating entity	TCT	n/a	n/a
Procurement process and formal contracts between the different stakeholders	WT	Board of the Participating entity	TCT	TI/RT providers	TIBER-EU Services Procurement Guidelines, Contracts, NDAs
Pre-test risk assessment	WT	Board of the Participating entity	TCT	TI/RT providers	Risk assessment
Scoping meeting	WT	Board of the Participating entity	TCT	TI/RT providers, if available	TIBER-EU Scope Specification document
Testing phase: threat intelligence					
Produce GTL Report for financial sector	Authorities and/or sector and/or TI providers	Authorities and/or sector and/or TI providers	Possibly national intelligence agency/ national cyber security centre/ high-tech crime unit	Authorities and/or sector	GTL Report
Produce a dedicated TTI Report on the Participating entity, setting out threat scenarios which can be used by the RT provider	TI provider	WT	TCT, RT provider, possibly national intelligence agency/ national cyber security centre/ high-tech crime unit	n/a	TTI Report
Testing phase: red team test					

Handover session between TI and RT providers, providing the basis for the threat scenarios	TI provider	WT	RT provider, TCT	n/a	TTI Report
Scenario development for TIBER-LU red team test	RT provider	WT	WT, TCT, TI provider	n/a	Red Team Test Plan
Weekly test meetings or updates	WT	Board of the Participating entity	RT provider, TCT	n/a	n/a
Discussion as flags are captured or when leg-ups are required	RT provider	WT	TCT	n/a	n/a
Closure phase					
Red Team Test Report, outlining the findings from the test	RT provider	WT	Senior executive at the Participating entity	TCT	Red Team Test Report
Blue Team Report, which maps the BT's actions alongside the RT provider's team actions	BT	WT	RT provider	TCT	Blue Team Report
Conduct an interactive replay of the test	WT	Board of the Participating entity	RT provider, TI provider, BT, OS, SUP[9]	TCT	n/a
360-degree feedback meeting	TCT	TCT	WT, BT, TI/RT providers	n/a	360-degree Feedback Report
Remediation Plan to address the findings	WT	Board of the Participating entity	TI/RT providers, TCT	Supervisor and/or overseer, if not involved during the test	Remediation Plan
Produce Test Summary Report	WT	Board of the Participating entity	TI/RT providers, TCT	Supervisor and/or overseer, if not involved during the test, and other relevant authorities	Test Summary Report
Signed attestation to validate the true and fair conduct of the TIBER-LU test	Board of the Participating entity	Board of the Participating entity	WT, TI/RT providers, TCT	TCT and supervisor and/or overseer, if not involved during the test, and other relevant authorities	Attestation

[9] OS and SUP in specific replay workshop during the closure phase

Annex 4: Abbreviations

ECB	European Central Bank
HUMINT	Human intelligence
OSINT	Open-Source intelligence
TCT	TIBER-LU Cyber Team
TECHINT	Technical intelligence
TIBER	Threat Intelligence-Based Ethical Red-Teaming
TIBER-EU	Common European framework for threat intelligence-based ethical red teaming
TIBER-LU	TIBER in Luxembourg
TIBER-DK	TIBER in Denmark
TIBER-BE	TIBER in Belgium
TIBER-NL	TIBER in Netherlands
TIBER-IE	TIBER in Ireland
TIBER-FI	TIBER in Finland
TIBER-SE	TIBER in Sweden
TIBER-DE	TIBER in Germany
CBEST	Bank of England’s intelligence-led red team testing programme
Leg-up	Help provided to the RT Provider during the execution of the test
RT provider	Red Team provider
TI provider	Threat Intelligence provider
WT	White Team
WTL	White Team Lead
BT	Blue Team
TTP	Techniques, Tactics and Procedures
CF	Critical Functions
GTL	Generic Threat Landscape
TTI	Targeted Threat Intelligence
OS	Oversight
SUP	Supervisor
TIBER-KC	TIBER-EU Knowledge Center is the group of TIBER Authorities that maintain the TIBER-EU Framework and related templates. It is coordinated by the ECB.