

## **TIBER-EU Attestation Template**

In accordance with the TIBER-EU Framework, at the end of each test, the board of the entity, the threat intelligence (TI) provider and the red team (RT) provider should sign an attestation confirming that the test was conducted in accordance with the mandatory requirements of the TIBER-EU framework.

This will provide the legitimacy for mutual recognition. Furthermore, the lead authority(ies) should confirm to other relevant authorities that it oversaw the test conducted. If the lead authority(ies) considers that the conduct of the test was not in line with the requirements and spirit of the TIBER-EU framework and the national or European Implementation Guide, it has the right to invalidate the test for TIBER-EU recognition and mutual recognition.

The TIBER-EU Attestation Template below should be used by entities undergoing a TIBER-EU test. The entity should replicate the letter below, setting out the requested details, and it should be signed off at board level. The entity should request the TI/RT providers to also sign off the annexes, to validate their role during the test and to confirm that they complied with the requirements of the TIBER-EU Framework. The annexes contained herein set out the mandatory requirements for the entity and TI/RT providers, and signing off of the templates (including the annexes) will imply that the aforementioned stakeholders confirm to have fulfilled all the listed requirements.

In case the test was cross-jurisdictional, the lead authority(ies) should confirm that the test was in line with the TIBER-EU or TIBER-XX implementation, and was sufficient for recognition by the other authorities and in line with their respective TIBER-YY standards. The lead authority(ies) can either provide this assurance via signing off the attestation or by providing verbal confirmation to the other authorities.

The Attestation, in conjunction with the TIBER-EU Test Summary Report, will form the basis for mutual recognition and other authorities with a legitimate interest in the outcome of the test on the entity, will rely on these outputs.

# Letterhead of entity

Attestor: Mr/Ms/Mrs Initial(s) Surname>

<Position in entity>

<Name of entity>

xx Month 20xx

<Address>

**TIBER-EU Attestation for test performed on [name of tested entity]**

Dear <Mr/Ms/Mrs Surname>,

We hereby confirm that [Insert Name of Attestor's organisation]'s participation in the TIBER-XX test has been based on the standards and principles of TIBER-XX, and that the conduct of the test process has complied with the core requirements in the TIBER-EU Framework. The main objective of the test has been to maximise learnings with the aim of, in the best way possible, improving [Insert Name entity]'s capabilities to protect, discover and react to sophisticated cyberattacks, which could potentially threaten the financial system as a whole.

This implies that:

- The scope has included such services and systems which, if disrupted, to the best of our knowledge, could potentially have detrimental impact on the stability of the financial system, the tested entity's safety and soundness, the entity's customer base or market conduct.
- The scenarios have to the best of our knowledge, been based on commercially obtained up-to-date high-quality threat intelligence that reproduces the tactics, techniques and procedures currently used by real high-level adversaries.
- The test has been executed by a team of experienced and independent threat intelligence providers and red team testers, against live critical production infrastructure, and without, to the best of our knowledge, the foreknowledge of the Blue Team. The providers have attested to fulfilling their responsibilities in Annexes 3 and 4.
- The test phase was followed by full disclosure and a replay between the Red Team and the Blue Team to identify gaps, address findings, improve the response capability, and maximise the learning output.

# Letterhead of entity

- [Insert Name of Attestor's organisation] has fulfilled the responsibilities listed in the overview of table in Annex 2, and which are further elaborated and documented in the respective TIBER-XX and TIBER-EU framework documents and templates.

---

Date

---

Signature

# Letterhead of entity

## Annex 1: [Name of authority(ies) of TIBER-XX] has been responsible for:

Adopting and implementing the TIBER-EU Framework.	✓
Acting as lead authority(ies) of the TIBER-xx programme.	✓
Publishing and maintaining the TIBER-xx Implementation Guide.	✓
Conducting a review of existing laws and regulations with the conclusion that the requirements, methodologies and processes contained in the TIBER-xx Guide do not contravene with any national or European laws or regulations.	✓
[Producing a Generic Threat Landscape report for the critical financial entities in TIBER-XX, and providing a copy to all relevant stakeholders in the test process].	(✓)
Identifying [insert name of entity] as a critical financial entity in [name of jurisdiction] eligible for participating in TIBER-xx, and inviting [insert name of entity] to participate in the programme.	✓
<p>Setting up an appropriate governance structure of TIBER-xx with adequate resources. Including establishing a centralised and independent TIBER-xx Cyber Team, TCT, with the following responsibilities:</p> <ul style="list-style-type: none"> <li>○ Managing, operationalising and overseeing the TIBER-XX test. ✓</li> <li>○ Controlling that the test contained all mandatory elements defined in the TIBER-XX Guidelines, and all requirements defined in the TIBER-EU Framework, incl.: <ul style="list-style-type: none"> <li>▪ Securing progress, e.g. by arranging periodic status meetings ✓</li> <li>▪ Agreeing to the scope of the test ✓</li> <li>▪ Controlling that the external independent third party providers meet the requirements in the TIBER-EU Services Procurement Guidelines. ✓</li> <li>▪ Agreeing to the project plan of the entity ✓</li> <li>▪ Agreeing to threat scenarios and test scenarios ✓</li> <li>▪ Monitoring the conduct of the test, including the quality and risk management ✓</li> <li>▪ Confirming to the best of our knowledge that the Blue Team was not informed about the test. ✓</li> </ul> </li> <li>○ Liaising with authorities in other jurisdictions that are relevant for the TIBER-XX test of [insert name of entity]. ✓</li> <li>○ Arranging a 360- feedback meeting, and completing the 360- feedback template. ✓</li> <li>○ Agreeing with the Remediation Plan proposed by [insert name of entity]. ✓</li> <li>○ Keeping the confidentiality of the test, e.g. by using code names and refraining from sharing any information about the TIBER-XX test without specific consent from [insert name of entity]. ✓</li> </ul>	

# Letterhead of entity

## Annex 2: [Name of entity] has been responsible for:

Establishing a White Team (WT) responsible for [Insert name of entity]'s own management and organisation of the TIBER-xx test process, including for producing and maintaining a project plan.	✓
Procuring independent external providers responsible for the targeted threat intelligence (TI provider) and the red team test (RT provider).	✓
Ensuring that the TI/RT providers meet the minimum requirements set out in the TIBER-EU Services Procurement Guidelines, and otherwise undertaking due diligence in the procurement process with the TI/RT providers.	✓
Developing the scope of the test which includes [Insert name of entity]'s critical functions (CFs), including the people, processes and technology and databases that support the delivery of the CFs.	✓
Arranging the scoping meeting, where the proposed scope of the test are discussed and finalised, and the targets and objectives of the test are agreed upon.	✓
Documenting the scope in the TIBER-xx Scope Specification Template which was signed off by a member of [Insert name of entity]'s Executive Board.	✓
Arranging the launch meeting with all relevant stakeholders, i.e. WT, TCT, TI/RT providers, where the overall project plan was discussed and agreed upon.	✓
Conducting a risk assessment and put in place the necessary risk management controls, processes and procedures to facilitate a controlled test.	✓
Providing information in advance to the TI provider by using the TIBER-xx Guidance for Targeted Threat Intelligence Template.	✓
Providing feedback to the TI provider during the process of developing the Targeted Threat Intelligence report and the threat scenarios.	✓
Facilitating the Threat Scenario review process.	✓
Facilitating the handover session between the TI and RT providers.	✓
Providing feedback to the RT provider during the process of developing attack scenarios and Red Team Test Plan.	✓
Securing the legal soundness of the test, i.e. that the test will not contravene any national or European laws or regulations.	✓
Allowing test to be executed on live production systems.	✓
Continuously being in contact with the RT provider during the execution of the test, including approving progress, and providing "legs-up" if needed.	✓

## Letterhead of entity

Securing that only the WT and TCT are informed about the test, its details and the timings – all other staff members (outside the White Team) remained unaware during the execution of the test.	✓
Providing feedback to the RT provider during the process of drafting the Red Team Test Report when the test was finalised.	✓
Facilitating replay workshops between the Red Team and relevant members of the Blue Team.	✓
Producing a Blue Team Report, where [Insert name of entity]'s own IT-security team mapped its actions alongside the Red Team's actions.	✓
Participating in the 360-feedback meeting.	✓
Producing a Remediation Plan in agreement with [name of authority(ies) of TIBER-XX].	✓
Producing a Test Summary Report which is shared with [name of authority(ies) of TIBER-XX].	✓
Providing an Attestation confirming that the test was conducted in accordance with the core requirements (i.e. signing-off this document).	✓

# Letterhead of entity

## Annex 3: [Name of TI provider] has been responsible for:

Meeting minimum requirements for TI providers set out in the TIBER-EU Services Procurement Guidelines.	✓
Participating in the launch meeting.	✓
[Using the Generic Threat Landscape Report as a basis for drawing the targeted threat landscape for [Insert name of entity], and adding to the threat landscape where relevant.]	(✓)
Producing a Targeted Threat Intelligence Report for [Insert name of entity] following the requirements in the contract with [Insert name of entity], such that it at a minimum meets the requirements in the TIBER-xx Guide.	✓
Securing the legal soundness of the test, i.e. that collection of threat intelligence will not contravene any national or European laws or regulations.	✓
Arranging the handover session with the RT provider.	✓
Continuing to be engaged during the testing phase and providing additional up-to-date, credible threat intelligence to the RT provider, where needed.	✓
Participating and providing input to the post-test replay, if relevant.	✓
Participating in the 360-feedback meeting.	✓
Contributing to Remediation Plan.	✓
Contributing to the Test Summary.	✓
Providing an Attestation confirming that the test was conducted in accordance with the core requirements (i.e. signing-off this document).	✓

[Insert Name of threat intelligence provider] has fulfilled the responsibilities listed in the overview of the table in Annex 3.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

# Letterhead of entity

## Annex 4: [Name of RT provider] has been responsible for:

Meeting minimum requirements for RT providers set out in the TIBER-EU Services Procurement Guidelines.	✓
Participating in the launch meeting.	✓
Participating in the handover session with the TI provider.	✓
Developing multiple attack scenarios, based on the Targeted Threat Intelligence Report.	✓
Producing the Red Team Test Plan.	✓
Securing the legal soundness of the test, i.e. that the execution of the test will not contravene any national or European laws or regulations.	✓
Executing the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and going through each of the phases of the kill chain methodology.	✓
Keeping the WT and TCT informed about progress during the test, “capture the flag” moments, the possible need for leg-ups, etc.	✓
Taking a stage-by-stage approach and consults the WT and TCT at all critical points to ensure a controlled test. The total time used for testing was xx days.	✓
Producing a Red Team Test Report for [Insert name of entity] following the requirements in the contract with [Insert name of entity], such that it at a minimum met the requirements in the TIBER-XX Guide.	✓
Participating in replay workshops between the Red Team and relevant members of the Blue Team.	✓
Participating in the 360-feedback meeting.	✓
Contributing to the Remediation Plan.	✓
Contributing to the Test Summary.	✓
Providing an Attestation confirming that the test was conducted in accordance with the core requirements, i.e. signing-off this document.	✓

[Insert Name of red team provider] has fulfilled the responsibilities listed in the overview of the table in Annex 4.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature



**Letterhead of entity**