



FRAKTAL

FRAKTAL

# The ultimate TIBER-FI guide

JUNE 2025

# Introduction

As a Red Teamer, my role is to emulate the tactics of cyber adversaries, uncover vulnerabilities, and help organizations strengthen their defenses in a controlled, safe fashion. The TIBER-FI framework provides a unique opportunity to test the resilience of Finland's financial institutions against real-world cyber threats. Over the years, I've seen how a mature approach to cybersecurity testing can transform an organization's cybersecurity posture and bring invaluable insights to its leaders. The purpose of this guide is to prepare you for that transformation.

This guide will walk you through the background, requirements, and process of TIBER-FI, helping you navigate the framework with confidence. Your leadership is essential in interpreting the test results and driving lasting improvements. With realistic attack simulations, TIBER-FI isn't about pointing fingers; it's about building a more resilient organization, and your role in this journey is foundational.

Cyber threats are constantly evolving, and TIBER-FI allows your organization to stay ahead of the curve. By understanding the framework, and embracing the lessons learned, you'll equip your institution to become stronger and more secure. Let this guide be your roadmap to success in navigating the critical but rewarding challenges of TIBER testing.

**Tuomo Makkonen**  
Red Team Leader, Fraktal







# Get to know TIBER-FI



# Get to know TIBER-FI

TIBER (Threat Intelligence-Based Ethical Red Teaming) is a framework that helps financial institutions strengthen their cyber resilience by simulating realistic, intelligence-led cyberattacks. It enables organizations to identify vulnerabilities and improve defenses in a controlled, collaborative, and constructive manner.

The European Central Bank (ECB) set the standard with TIBER-EU (2018), creating a unified framework for intelligence-led red teaming across critical European financial infrastructure. Finland adopted this, tailoring it to the local landscape with TIBER-FI (2020), ensuring specific national regulatory and security needs are met.

TIBER testing aligns directly with the advanced security testing requirements mandated by the EU's Digital Operational Resilience Act (DORA), specifically its Threat-Led Penetration Testing (TLPT) articles. Conducting a test project according to the TIBER-FI method will fulfil the requirements of DORA and DORA RTS for TLPT.

Engaging in TIBER is not just best practice; it's a proactive step towards demonstrating robust operational resilience demanded by regulators.

# TIBER-FI process

The TIBER-FI process starts out with **pre-planning**, which is done by the financial entity.

It is succeeded by the four formal phases of the TIBER-FI process:

1. Preparation phase – scoping with Fraktal, procurement process
2. Testing phase: Threat intelligence
3. Testing phase: Red Team
4. Closure phase

Each formal step is divided into process steps and activities.

A maximum of 18 months can be used within the given 3-year window if the entity conducts the testing as required by their local Financial Supervisory Authority (e.g. FIN-FSA in Finland).

**Reserving at least 12 months for the full process is recommended.**

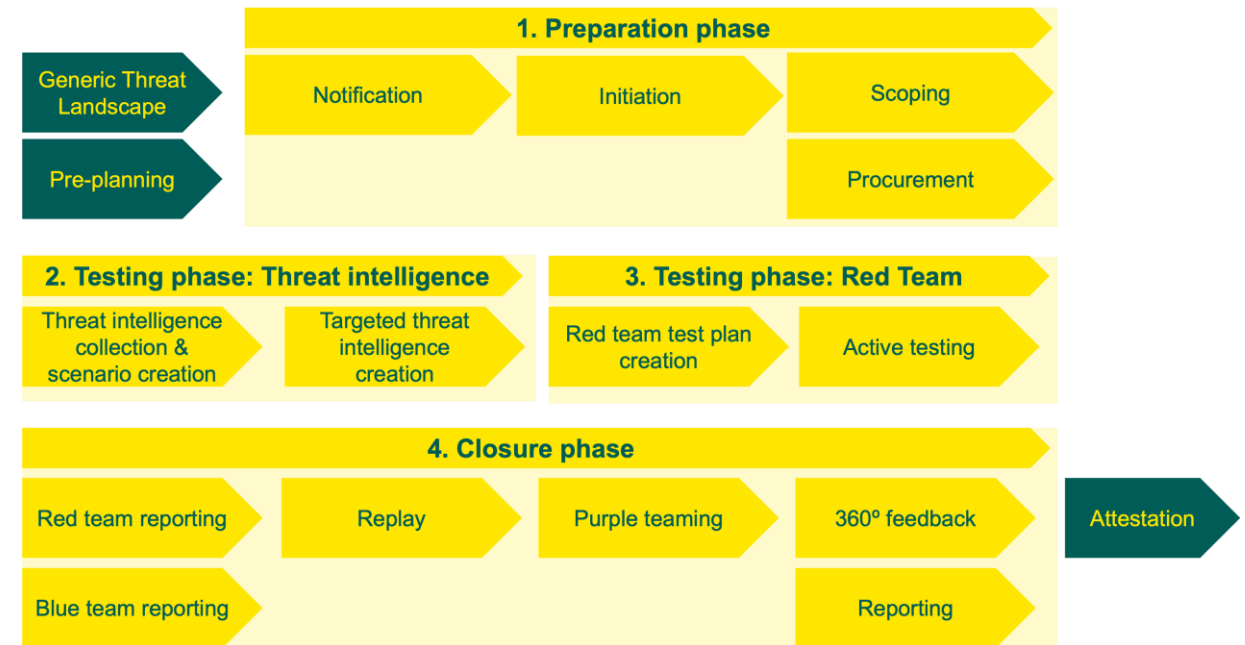


Illustration based on: TIBER-FI Procedures and Guidelines, Bank of Finland




# The strategic importance of TIBER testing

## TIBER MANDATES REALISTIC, INTELLIGENCE-LED CYBERATTACK SIMULATIONS

TIBER isn't a theoretical exercise; it's about understanding how sophisticated attackers could target specific critical functions of an organization. With TIBER a financial institution can solve many issues in one go:

- **Uncover weaknesses** in practices, processes and technology that standard testing might miss.
- Gain actionable insights derived from realistic adversary simulations to measurably **improve detection and response capabilities**.
- **Meet regulatory expectations**, through TIBER's alignment with DORA TLPT mandates.
- **Foster continuous improvement** by using test results to drive targeted investments and **uplift overall security posture** against advanced threats.



# Keys to effective TIBER testing

## START WITH HIGH-QUALITY THREAT INTELLIGENCE

Ensure you have the right intelligence foundation. Ensure the Targeted Threat Intelligence Report (TTIR) is specific, actionable, and provides a robust basis for realistic Red Team scenario development, as mandated by TIBER.



## REPLICATE THE TTPS OF RELEVANT THREAT ACTORS

Use scenario-driven testing. Execute multiple, distinct attack scenarios based directly on the TTIR, focusing on compromising Critical Functions (CIFs). Create realistic simulation of TTPs that mimic adversary behaviour, employ evasion techniques and adapt tactics to rigorously test your detection and response capabilities – not just find vulnerabilities.



## PROGRESS THROUGH PLANNED REMEDIATION

A TIBER test's true value comes from the follow-up actions that are taken. Transform the test findings into actionable steps with a documented Remediation Plan (RP). The RP ensures vulnerabilities are resolved systematically, while providing clear oversight of progress. This approach strengthens defenses and embeds lessons learned, turning the test into an investment in cyber resilience.

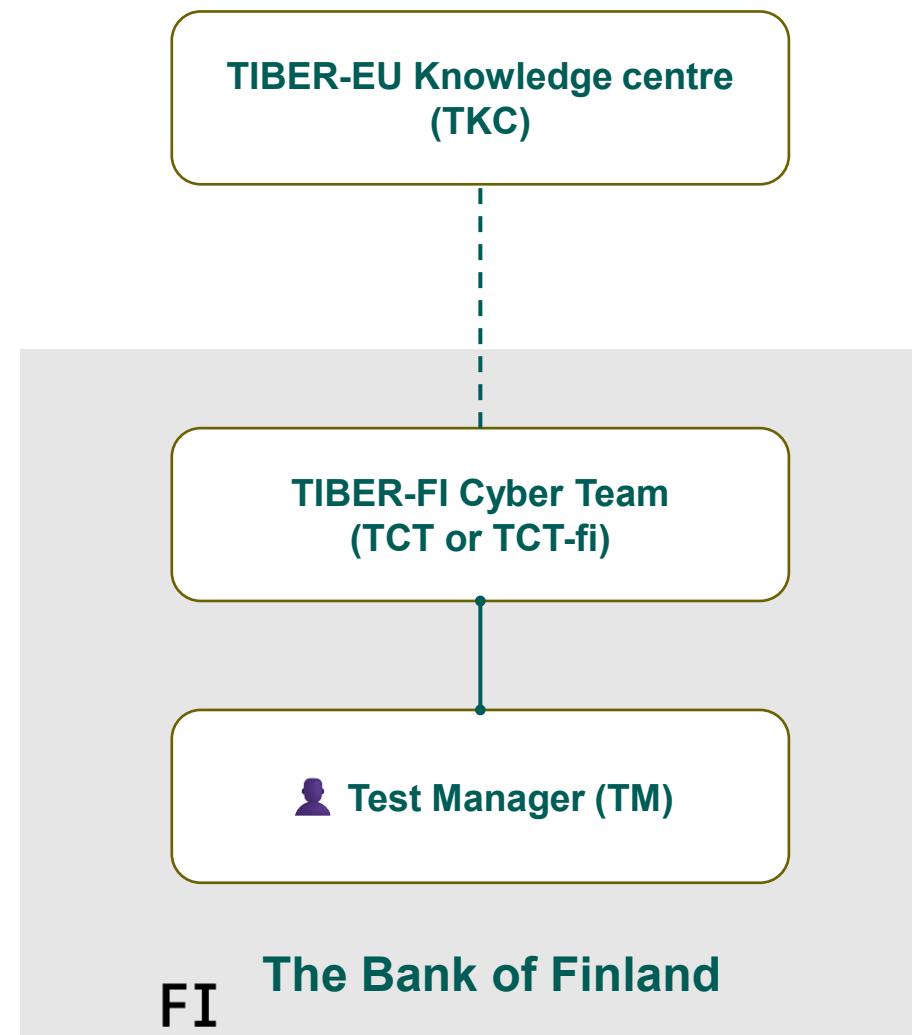
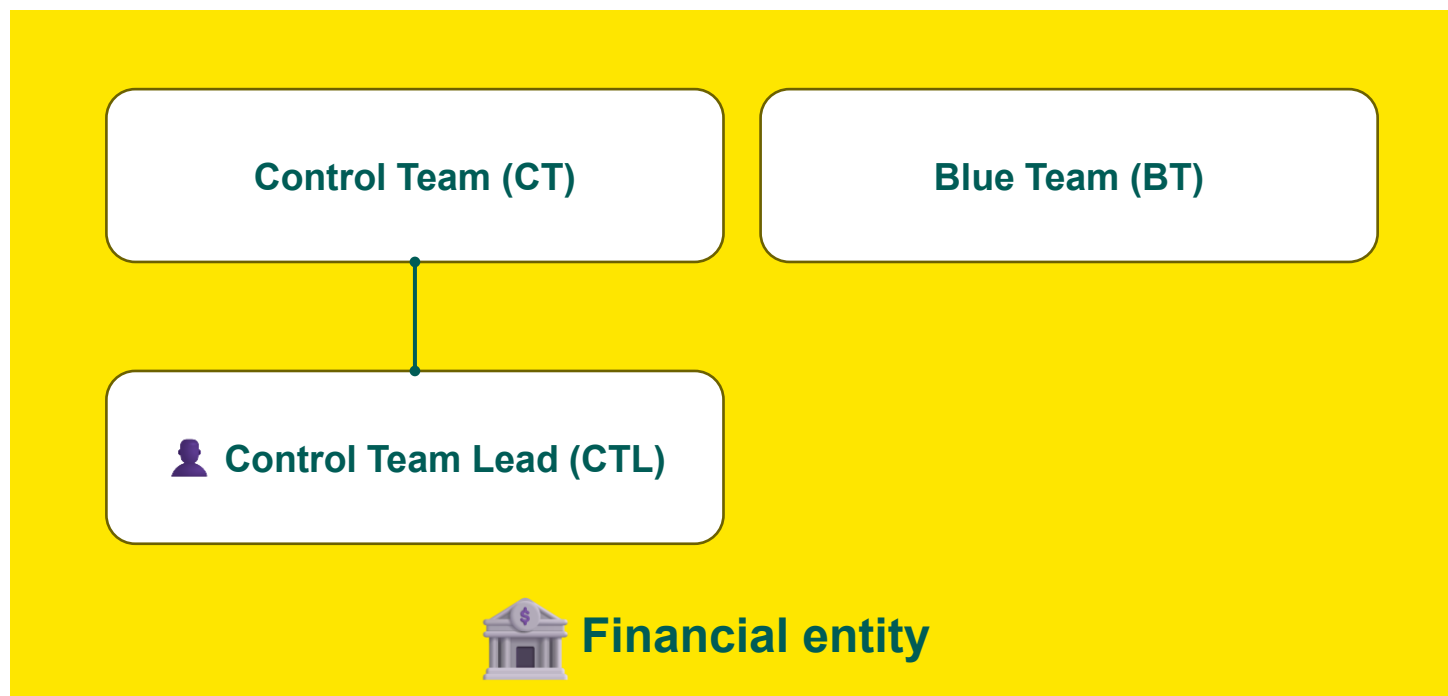




# The TIBER process







# TIBER stakeholders



See Appendix B for more detailed description of the roles.

TIBER-FI process  
phases and steps

1 Preparation phase	2 Threat intelligence	3 Red Team	4 Closure
			
Max. duration: 6 months	Indicative: 4-6 weeks	Indicative: 12-13 weeks	Indicative: 18 weeks
Notification			
Initiation			
Scoping			
Procurement			
	Threat intel collection		
	Scenario creation		
	TTI report creation		
	Approval		
		RT test plan creation	
		Active testing	
			Red team test report
			Blue team test report
			Replay exercise
			Purple teaming
			Approval
			360° feedback
			Remediation plan
			Test summary report
			Attestation

# 01 Preparation phase

## PHASE GOAL

To formally launch the test engagement and establish a definitive, approved scope that will govern all subsequent activities.

This involves securing management buy-in, understanding the test requirements, and selecting expert, independent providers who will execute the threat intelligence and red teaming components of the test.

## PHASE OUTCOME

The primary and most critical outcome of this phase is the **Approved Scoping Document**.

- This is the foundational document, formally agreed upon by the entity and the test teams, that provides the definitive mandate and boundaries for the test.
- All subsequent planning and execution, including the development of the Targeted Threat Intelligence Report (TTIR) and Red Team Test Plan (RTTP), are based directly on this approved scope.

Furthermore, the selection and contracting of an independent Threat Intelligence (TI) Provider and Red Team Testing (RTT) provider is done in this phase.



# 02 Testing phase: Threat Intelligence

## PHASE GOAL

To gather, analyze, and process threat intelligence specific to your organization's profile and the agreed-upon scope.

The objective is to transform a general threat landscape into a specific and actionable set of attack scenarios that realistically mimic the most likely and capable adversaries your organization faces.



## PHASE OUTCOME

The single, critical outcome of this phase is the **Targeted Threat Intelligence Report (TTIR)**.

- This report is delivered by the specialized TI Provider. It details the specific threat actors, their motivations, and the Tactics, Techniques, and Procedures (TTPs) that will be simulated.
- Crucially, it contains the detailed scenarios that will be used as the blueprint for the live Red Team attack. This report is reviewed and approved before the next phase can begin.

# Testing phase: Red Team

## PHASE GOAL

To simulate real-world intrusions by emulating adversary TTPs and attempting to compromise in-scope Critical or Important Functions (CIFs). This involves developing an operational Red Team Test Plan (RTTP) based on the TTIR and executing it safely on the live production environment.



## PHASE OUTCOME

The primary outcome is the **Red Team Test Report (RTTR)**. This comprehensive report, written by the Red Team, provides a detailed narrative of the entire attack.

The RTTR documents all activities, timelines, successful attack paths, and failed attempts. It also serves as the core evidence base for the findings and provides the "attacker's perspective" that will be analyzed in the final phase of the engagement.

# Closure

## PHASE GOAL

To synthesize the findings from both the attack and defense perspectives to create a holistic understanding of your security posture.

The objective is to move beyond a simple list of findings to identify the root causes of vulnerabilities, prioritize remediation, and, most importantly, maximize the learning and development for your defensive teams.

## PHASE OUTCOME

The final phase consolidates the insights and activities from the testing process, delivering a comprehensive analysis and a clear path for improvement. It culminates in a **Test Summary Report (TSR)**, which combines findings from both the Red Team and the Blue Team to provide a complete view of the test and its results. Based on these findings, an actionable **Remediation Plan** is developed, prioritizing steps to address vulnerabilities across people, processes, and technology. Additionally, the phase enhances organizational resilience through collaborative **Purple Teaming**, where the Red and Blue Teams replay attack scenarios to fine-tune and validate detection and response capabilities. This final phase not only summarizes the test but also sets the foundation for lasting improvements and strengthened defensive capabilities.





# Why Choose Fraktal?

# Beyond standard tooling: our research-driven advantage

## ADVANCED TOOLING

Standard tools often trigger standard defenses. As real-world attackers develop their own bespoke tools and capabilities, so do we.

Our proprietary implants and other offensive tooling are developed in-house, ensuring our methods are not easily identified by standard commercial detection solutions. This allows us to simulate the novel and evasive techniques used by sophisticated adversaries, providing a true test of your monitoring and response capabilities.

## BENEFITS

Fraktal's commitment to research and custom tooling means Fraktal delivers a more realistic, challenging, and ultimately more valuable TIBER test, pushing your defenses further and uncovering weaknesses that off-the-shelf approaches might miss.



FRAKTAL'S APPROACH

# Risk management and reporting

## WE APPLY STRICT RISK MANAGEMENT

All testing is conducted under strict risk management protocols agreed upon during the preparation phase. (Ref: TIBER-EU Framework - Risk Management)

## COMPREHENSIVE REPORTING

We deliver detailed RTTRs compliant with TIBER standards, outlining attack narratives, findings, and crucial observations for remediation.



# Fraktal as your TIBER partner



## Unbiased and objective

Fraktal operates solely as an independent Threat Intelligence (TI) facilitator and Red Team Testing (RTT) provider. We have no conflicting Blue Team engagements nor technology portfolio, guaranteeing the unbiased, objective assessments required by TIBER frameworks.



## Methodology excellence

Our testing methodologies are built on years of high-stakes offensive security and adversary simulation experience with most demanding clients and verticals in the Nordics.



## Focus on increasing resilience

We partner with you not just for compliance, but to achieve tangible, long-term improvements in your cyber resilience.



## Proven expertise

Fraktal's specialists have completed 50+ red teaming and 100+ purple teaming assignments. We excel in complex engagements: our experience gives us superior insight into offensive testing within demanding environments. This allows us to effectively replicate sophisticated threats with realism.



# TIBER-FI FAQ

# Q What is TIBER-FI?

TIBER-FI is Finland's national implementation of the European framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU). It is a systematic and controlled framework for conducting cybersecurity tests that are based on real-world threat intelligence. The primary objective is to test and improve the cyber resilience of financial entities and the financial sector as a whole against sophisticated, targeted cyber-attacks.

TIBER-EU Documentation can be found at: <https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu>

TIBER-FI Documentation can be found at: <https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-framework/>



# How does TIBER-FI relate to the DORA regulation?

Conducting a test according to the TIBER-FI procedures and guidelines fulfils the requirements for Threat-Led Penetration Testing (TLPT) as mandated by the Digital Operational Resilience Act (DORA). The TIBER-EU framework is designed to be used as detailed operational guidance on how to complete DORA TLPT requirements.





# Is a TIBER-FI test a "pass or fail" exercise?

No. A TIBER-FI test does not result in a 'pass or fail' grade. Instead, the test provides valuable insights into an organization's strengths and weaknesses, enabling the entity to learn, evolve, and achieve a higher level of cyber maturity.

However, the test must be conducted according to the TIBER guidelines. After the entity has completed the four phases, and submitted the required documents, the Bank of Finland provides a signed attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-FI framework.

# Q How long does a typical TIBER-FI test take from start to finish?

The entire process is comprehensive and spans several months:

- **Preparation Phase:** This phase has a maximum duration of six months.
- **Testing Phase (Threat Intelligence):** This part typically takes 4-6 weeks.
- **Testing Phase (Red Team Testing):** The active testing portion has a mandatory minimum duration of 12 weeks to ensure a realistic and thorough test.
- **Closure Phase:** This final phase can take 18 weeks or more, as it includes report writing, replay exercises, feedback, and developing the final remediation plan.

Reserving at least 12 months for the full process is recommended.



# Can we use our internal red team for the test?

Using an external, independent Red Team provider is strongly encouraged to ensure a fresh and unbiased perspective. The use of internal testers is possible only in exceptional circumstances and requires prior approval from the Test Manager. Furthermore, an entity must use external testers for at least one in every three tests.

TIPs are always procured externally.

# Q What is the role of Purple Teaming in a TIBER test?

Purple Teaming in TIBER is a collaborative exercise between the Red Team (attackers) and the Blue Team (defenders) to maximize learning. It occurs at two specific points:

- **Limited Purple Teaming (LPT):** This approach can be used as a last resort during the active testing phase to continue a test that might otherwise have to be stopped.
- **Purple Teaming Exercise:** This is a mandatory and fixed element of the Closure Phase. It is used to enhance learning by re-exploring scenarios, discussing alternative attack vectors, or investigating specific vulnerabilities in a collaborative setting.



# What are CIFs and the flags to be captured?

CIFs are the financial entities' Critical or important functions. TIBER testing is focused on the CIFs as well as the underlying systems supporting these CIFs, i.e. people, processes and technologies.

In TIBER testing, “flags” refer to predefined objectives or pieces of evidence that the Red Team strives to capture during the simulation. These flags are closely tied to the Critical or Important Functions (CIFs). They simulate the data, access, or actions an adversary would target in a real-world attack to compromise the organization’s critical operations.

The full definition of a CIF in DORA:

“a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law”.



## TIBER-FI FREQUENTLY ASKED QUESTIONS



**What are the key deliverables of TIBER-FI project?**



**What are the key roles in a TIBER-FI project?**

See Appendix A for a list of the key deliverables and Appendix B for a list of the key roles.



# Appendices

# Appendix A: Key deliverables of a TIBER-FI project

Deliverable	Abbrev.	Description	Phase	Responsible	Delivered to
Notification letter		Marks the start of the test and the requirements to be followed during testing	Preparation	TIBER authority	Entity
Initiation documents		Several documents, incl. the project charter	Preparation	Entity (CT / CTL)	TIBER authority
TIBER Scope Specification Document	SSD	Lists the CIFs, the systems and services underpinning each CIF, and the flags to be captured for each system	Preparation	Entity (CTL)	TIBER authority, TM
Targeted Threat Intelligence Report	TTIR	Details the specific threat actors and realistic attack scenarios that will be simulated.	Testing phase: Threat Intelligence	TIP	CT delivers to TM for approval
Red Team Test Plan	RTTP	The plan translates the TTIR scenarios into a detailed, operational plan for the live attack simulation.	Testing phase: Red Team Testing	RTT	CT delivers to TM for approval
Red Team Test Report	RTTR	Details the full narrative of the attack, including all actions taken, vulnerabilities found, and flags captured.	Closure	RTT	CT delivers the report to the BT, and TM.
Blue Team Test Report	BTTR	The entity's defensive team (Blue Team) creates this report, mapping their detections and responses to the actions described in the RTTR.	Closure	BT	CT delivers the report to the RT, and TM.
Written 360° feedback		Written feedback from test participants (CT, TIP, RTT, BT)	Closure	TM facilitates	TM
Remediation plan		A concrete plan to address the identified vulnerabilities and improve its security posture.	Closure	CT	TM
Test Summary Report	TSR	Synthesizes the findings from all previous reports and exercises to provide a holistic overview of the test and its results.	Closure	CT	TM
Remediation plan		A concrete plan to address the identified vulnerabilities and improve its security posture.	Closure	CT	TM
Attestation		A signed attestation confirming that the test was conducted in accordance with the TIBER-FI framework.	(After closure)	TIBER authority	Entity



# Appendix B: Key roles in a TIBER-FI project

Role	Abbrev.	Description	Your notes
Blue Team	BT	The internal security/IT team tasked with detecting and responding to potential cyberattacks. Unaware of the specific timing or details of the TIBER test.	
Control Team	CT	A group of internal stakeholders who oversee the test execution to ensure everything runs within the defined scope while maintaining operational safety.	
Control Team Lead	CTL	The leader of the Control Team, responsible for coordinating all aspects of the exercise, ensuring alignment with the Scope Document and Rules of Engagement (RoE), and maintaining effective communication during the test.	
Red Team	RT	A group of ethical hackers tasked with simulating the actions of malicious actors to test an organization's detection and defense capabilities.	
Red Team Testers	RTT	The ethical hackers or "attackers" tasked with executing the simulated cyberattacks based on the Threat Intelligence Provider's input. Their ultimate goal is to test the institution's ability to detect and respond to adversaries under realistic conditions.	
Threat Intelligence Provider	TIP	An external service provider responsible for gathering and analyzing tailored threat intelligence relevant to the financial institution. Their insights form the foundation for the design of realistic attack scenarios.	
TIBER-FI Cyber Team	TCT-FI or TCT	Team at Bank of Finland that promotes the adoption of the TIBER-FI procedures and provides support and guidance for financial entities in the application of the TIBER-FI procedures.	
Test Manager	TM	A designated test manager who is working on the Bank of Finland's mandate. The test manager ensures entities conduct TIBER-FI tests in a uniform and controlled manner, and in accordance with the TIBER-FI framework and applicable requirements.	



**FRAKTAL**

**FRAKTAL.FI/TIBER**