2023

TIBER-IS

IMPLEMENTATION GUIDE

SEÐLABANKI ÍSLANDS

TIBER-IS

IMPLEMENTATION GUIDE

Version 1.0

June 2023

Table of contents

1 Introduction 4

Background and purpose of TIBER-IS 4
What is TIBER-EU? 4
About TIBER-IS 5
Purpose of this Guide 5
TIBER-IS Cyber Team 6
Generic threat landscape report 6

2 The Central bank´s role and responsibilities in TIBER-IS 6

Ownership of information 7
Cross-jurisdictional cooperation 7
Legal review 7

3 Stakeholders in the TIBER-IS process 8

Entities critical to the Icelandic financial system 8
Third party providers 9

4 Overview of the TIBER-IS test process 11

Generic Threat Landscape Report 11
Preparation phase 11
Testing Phase 12
Closure phase 14

5 Interactions during a TIBER-IS test 15

Closing remarks 15
Abbreviations 16

1

Introduction

Background and purpose of TIBER-IS

The Central Bank of Iceland is an independent institution owned by the State and operating under the auspices of the Prime Minister. Its objective is to promote price stability, financial stability, and sound and secure financial activities. Financial supervision is also a part of the Central bank. The Bank shall therefore monitor supervised entities to ensure their activities comply with law and with Governmental directives and that they are consistent with sound and appropriate business practices.

One of the Central Bank of Iceland's main tasks is to promote a safe, stable, and effective financial system. Financial stability means, among other things, that the financial system is equipped to withstand operational incidents to ensure the availability of capital, credit and payments system. In recent years, cyber risk has risen to become one of the major risks for financial stability. As a result, cyber risk has become part of the Central bank´s focus regarding financial stability.

What is TIBER-EU?

The European Central Bank (ECB) published the Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[1] in May 2018. The framework was jointly developed by the ECB and the EU national central banks and was inspired by the CBEST program in the UK and TIBER-NL in the Netherlands. TIBER-EU is a framework for conducting intelligence-led red team tests of entities' critical live production systems. It was produced with the financial sector in mind but can be used in other markets. The core objectives with TIBER-EU, according to the TIBER-EU framework, are to:

- Enhance the cyber resilience of entities, and of the financial sector more generally.
- Standardize and harmonize the way entities perform intelligence-led red team tests 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 and manage this form of testing at a national or European level.
- Support cross-border, cross-jurisdictional intelligence-led red team testing for multinational entities.
- Enable supervisory and/or oversight equivalence discussions where authorities seek to rely on each other's assessments carried out using TIBER-EU, thereby reducing the regulatory burden and fostering mutual recognition of tests across the EU.

1. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

- Create the protocol for cross-authority/cross-border collaboration, result sharing and analysis.

About TIBER-IS

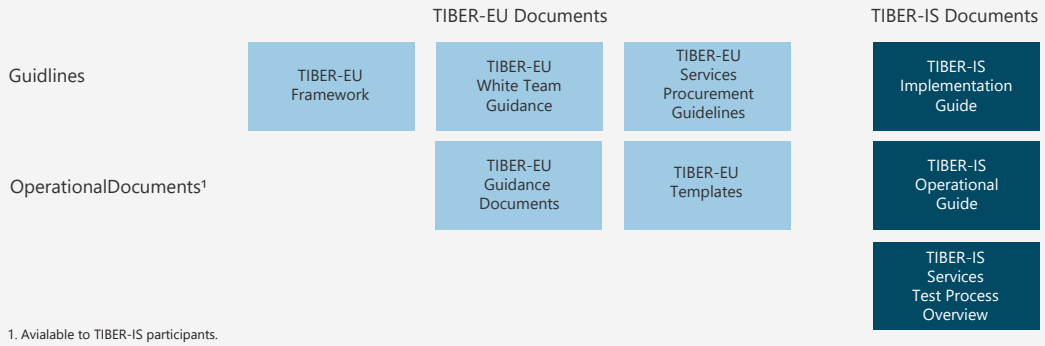
The Central bank of Iceland has decided to adopt TIBER-EU framework as the TIBER-IS program. The overall aim of TIBER-IS is to enhance cyber resilience in the Icelandic financial sector and thus promote financial stability. In TIBER-EU, it is stated that "if a jurisdiction decides to adopt the TIBER-EU framework, its national implementation must be formally adopted by the board of an authority, ideally the central bank of the European System of Central Banks (ESCB)." The Governor of the Central Bank of Iceland on behalf of the bank has adopted TIBER-EU and, with it, the national implementation of TIBER-IS. Following the implementation, the Central bank is the lead authority of the TIBER-IS program.

In this implementation guide, the Central bank describes the TIBER-IS program, with the aim to enhance the cyber resilience of entities critical to the Icelandic financial system. As cyber risk has the potential to become a systemic risk, a further important purpose of TIBER-IS is to increase resilience toward cyber risk in the Icelandic financial system. TIBER-IS is not meant to be a tool in financial supervision although the result of testing can be used as an input to supervision of operational risk.

Purpose of this Guide

This document, the TIBER-IS Implementation Guide, describes the Icelandic national implementation of the TIBER-EU framework. The TIBER-IS Implementation Guide is supplemented by other guiding documents, and collectively they represent the TIBER-IS program, see figure 1.

Figure 1
TIBER-IS documentation



1. Avialable to TIBER-IS participants.

The TIBER-IS documentation is based on documents from the TIBER-EU framework which form the foundation of TIBER like in other jurisdictions that have adopted TIBER-EU. Additionally, TIBER-IS specific documents explain the TIBER-IS implementation of the framework. The TIBER-IS Operational Guide provides a step-by-step description of each of the elements in the TIBER-IS test process, and the TIBER-IS Test Process Overview gives a graphical overview of the elements in a TIBER-IS test. An overview of the complete set of TIBER-EU and TIBER-IS documents can be found in the TIBER-IS Test Process Overview.

Enquiries about TIBER-IS should be directed to TIBER-IS@sedlabanki.is.

2

The Central bank´s role and responsibilities in TIBER-IS

The Central bank implements the TIBER-IS program for entities critical to the Icelandic financial system. The Central bank supports the entities by providing guidance, a financial sector generic threat landscape report, and Test Manager support services. Participation in the program is voluntary.

The Central bank is the lead authority of TIBER-IS and the governor of the Central bank has formal ownership of the program.

TIBER-IS Cyber Team

The Central bank is responsible for the establishment and operation of the TIBER-IS Cyber Team, TCT, which has been set up within the Central bank. The role of the TCT is twofold:

- Manage the TIBER-IS program, maintain the national implementation guide, and act as a contact for other TCTs and the TIBER-EU Knowledge Centre (TKC).
- Ensure uniform, high-quality tests by the entities that fulfill the requirements of TIBER-IS. A key part of the TCT is the Team Test Manager (TTM), who manages the tests from the TCT's side.

During a TIBER-IS test, the TCT holds the right to invalidate a test for TIBER recognition if the TCT suspects that the entity is not conducting the test in the right spirit, in accordance with the TIBER-IS principles or the requirements of the TIBER-EU framework.

The Central bank is responsible for ensuring that the TCT has adequate resources and skills to carry out its assignment.

Generic threat landscape report

A generic threat landscape report (GTL) for the financial sector is a requirement in TIBER-IS. The Nordic Financial CERT[2] authors the report and is responsible for inviting the TCT and the test participants to be involved in the drafting process and to collect feedback and validation from CERT-IS[3] for further enrichment of the report. The report will be updated yearly to ensure that the content is up to date.

The TCT is responsible for ensuring the report is available to test participants.

2. https://www.nfcert.org/
3. https://www.cert.is/

Ownership of information

The tested entity is the legal owner of all the material that is produced during the test and is responsible for sharing the material with competent authorities, if required. The Central Bank will not share any sensitive information about a TIBER-IS test with any other authority without having the specific consent of the tested entity, subject to requirements in national law. Furthermore, if results are shared, as a rule, it will only be done at an aggregate level.

Cross-jurisdictional cooperation

A core objective of TIBER-EU is to standardize and harmonize intelligence-led red team tests thus enabling cross-border testing. The TCT is responsible for liaising with relevant authorities in other jurisdictions prior to such a test. The aim for such liaison is to establish a basis for a cross-border test or to promote cross jurisdictional recognition of the test by explaining the procedures of the TIBER-IS test.

Legal review

A key part of TIBER-IS is ensuring that the requirements, methodologies, and processes contained in the TIBER-IS program do not contravene any Icelandic or EAA laws or regulations. The Central bank has conducted such a review in 2023, and the implementation of TIBER-IS is deemed compliant with legislation and regulations. In the review, legal and regulatory requirements affecting the participants in TIBER-IS have been examined using a risk-based approach, and both entity-specific and general legal and regulatory requirements have been assessed. The Central bank will monitor the question of legal and regulatory compliance of TIBER-IS continuously and is responsible for ensuring legal compliance during the program's lifetime.

Each entity that participates in a TIBER-IS test is solely and exclusively responsible and liable for the execution of the tasks attributed to it by this guidance, including compliance with the applicable laws and regulations. Financial entities always remain fully responsible for the risk associated with the test and for any negative impact on their services and on third parties. Entities that participate in TIBER-IS are thus responsible for making their own legal review before testing as they are responsible for the test.

This document contains parts from the publication „TIBER EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming"[4] to which ECB owns the copyright. Inspiration for the text and setup of the TIBER-IS implementation guide has been sought from the TIBER implementation guides of other Nordic countries with their permission.

4. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

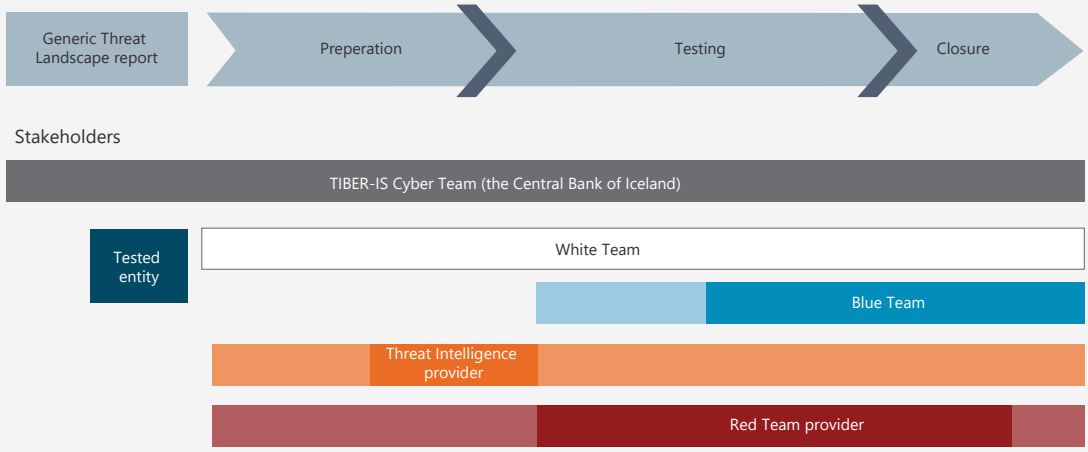
3

Stakeholders in the TIBER-IS process

The stakeholders that are directly involved in a TIBER-IS test are (see fig. 2):

- The Central bank of Iceland
  - TIBER Cyber Team (TCT) and TIBER Test Manager (TTM)
- Entities critical to the Icelandic financial system.
  - White Team (WT) and White Team Lead (WTL)
  - Blue Team (BT)
- Third party providers for threat intelligence and red team tests.
  - Threat Intelligence (TI) provider
  - Red Team (RT) provider

Figure 2
Stakeholders in a TIBER-IS test process



The roles and responsibilities of the Central bank have already been described. The roles and responsibilities of other stakeholders are described in the following chapters.

Entities critical to the Icelandic financial system

Eligible participants in the TIBER-IS program are entities that are critical to the Icelandic financial system. Each participant is responsible for its own test in its entirety. This means managing and organizing the test and ensuring that the test lives up to the TIBER-IS program, as well as hiring third-party Threat Intelligence and Red Team providers, and taking responsibility for proper risk management regarding the test.

Each financial entity participating in TIBER-IS must appoint a team to coordinate testing activities. This team is referred to as the White Team (WT), led by a White Team lead (WTL). Guidance regarding roles, responsibilities and composition of the white team can be found in the document „TIBER-EU White Team Guidance ".[5] Prior to conducting the test, the White Team conducts a risk assessment and then puts in place all the necessary risk management controls, processes and procedures to facilitate a controlled test.

All remaining staff and service providers at the tested entity that are not part of the White Team are considered part of the Blue Team (BT). A key part of TIBER-IS is that the Blue Team is completely excluded from all preparation and conduct of the TIBER-IS test, including scope, methods, and timing of the Red Team test. In the closure phase, as part of the replay workshop, selected members of the Blue Team should participate to ensure maximum learning of the Blue Team from the test.

Before executing a test, the board or executive management of the tested entity must agree and attest to the test's scope. In addition, when the test is completed, the board or executive management of the tested entity must sign an attestation in which it confirms that the test was conducted in accordance with the TIBER-IS program. Both these attestations must be shared with the TCT.

Third party providers

It is mandatory to use external third-party providers for targeted threat intelligence and Red Team testing under the TIBER-EU framework. This also applies to TIBER-IS.

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

- The Threat Intelligence provider should provide threat intelligence and develop threat scenarios for the tested entity in the form of a targeted threat intelligence report, according to the standards described in the TIBER-EU TI guide. 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 provider, using the Targeted Threat Intelligence, plans and executes a TIBER-IS test of the target systems and services agreed in the test's scope. This is followed by a review of the test and the issues arising, culminating in a red team test report drafted by the provider.

An agreement must be reached with these providers on the scope of the test, boundaries, timing, availability of necessary staff, contracts, actions to be taken and liability issues. The contracts should include at minimum:

- Security and confidentiality requirements for the third-party providers should be at least as strict as those followed by the tested entity.
- Protection of those involved, such as indemnifications.
- Data destruction requirements and breach notification provisions.
- Activities not allowed during the test. Examples are destruction of equipment; uncontrolled modification of data/programs; jeopardizing continuity of critical services; blackmail; threatening or bribing employees.
- Disclosure of results.

A key means of managing the risks associated with the TIBER-IS test is to use competent, qualified, and skilled Threat Intelligence and Red Team providers with the requisite experience to conduct such tests. Consequently, prior to engagement, the tested entity must ensure that

5. https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

the providers meet the minimum requirements, which are set out in the „TIBER-EU Services Procurement Guidelines ".[6] The guidelines also include items to consider regarding contracts with third-party providers.

It is allowed, under TIBER-IS, to use the same provider as a Threat Intelligence provider and a Red Team provider. If this is done, a separation between the Threat Intelligence team and/or Red Team within the providers organization is required.

6. https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf

4

Overview of the TIBER-IS test process

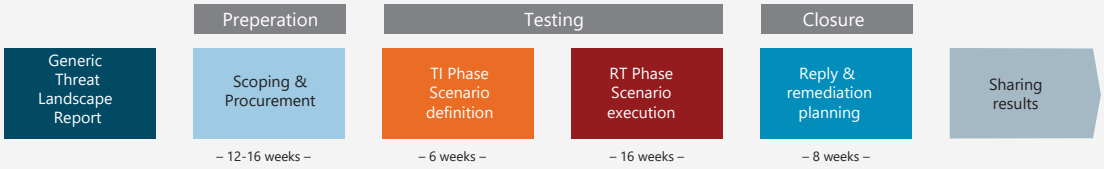
The process begins with the production of the Generic Threat Landscape report. This is followed by three phases, see figure 3:

- Preparation
- Testing
- Closure

These phases are described in the following sections.

Figure 3

TIBER-IS test process



Generic Threat Landscape Report

The TCT is responsible for the production of a Generic Threat Landscape Report (GTL) and for sharing the report with the participants in TIBER-IS. The GTL will contain information regarding threats to the Icelandic financial system. This includes a description of the threat actors and their motives and modus operandi, together with the tactics, techniques, and procedures they use to attack. The report will also contain information regarding the types of financial entities different threat actors are targeting. The purpose of the report is to provide a solid basis for the individual entities' targeted threat intelligence that is produced later in the test process. NF-CERT produces the report for the Icelandic financial market.

Preparation phase

The financial entity must decide when to initiate the process and ensure sufficient resources for the test. The entity must select a code name for the test, which cannot be connected to the entity, to ensure confidentiality of the test both within and outside the entity. The code name should be used in all communication regarding the test and must not be used in connection with the name of the entity. A key decision is setting up the White Team and appointing a White Team Lead. In this phase, the TCT will provide the White Team with the TIBER-IS documentation for the test process. The TCT and the tested entity will schedule a launch date for the test process and

the tested entity will begin its pre-planning of the test. This includes performing a stakeholder analysis.

Once the White Team has been established, the pre-launch meeting between the TCT (including Test Manager) and the White Team is held. During the meeting, discussions will be started regarding the requirements of TIBER-IS, the scoping process, procurement of third-party providers and overall project planning. Only the White Team and the TCT will be informed about the details and timings of the test.

The preparation phase will progress with scoping, risk assessment and procurement of third-party providers. The services may be procured from the same provider. The scope of the test includes the entity's critical functions including its people, processes, and technology.

The White Team is responsible for scoping, but there should be a mutual agreement between the White Team and the TCT regarding the scope to ensure that the scope meets the TIBER-IS requirements and that the test is executed according to plan. The TCT can assist the White Team with the scoping process. Systems underpinning a critical function are in scope even if they are run by third party service providers, unless an exception is made by the TCT.

During the preparation phase, i.e., prior to testing, the White Team is responsible for conducting a risk assessment and implementing the necessary controls, processes, and procedures to ensure that the test does not pose unnecessary risk to the entity's operations.

Providers of targeted threat intelligence and red teaming will be procured during this phase. These third-party providers must meet the requirements in the "TIBER-EU Services Procurement Guidelines". It is the responsibility of the White Team to ensure this, but the Test Manager will provide consultation as required for procuring these services.

To conclude the preparation phase, the TCT should schedule two meetings between the TCT and the White Team. If deemed relevant, the Threat Intelligence and/or Red Team test providers can also participate in the meetings. The meetings are:

- Launch meeting: To discuss and agree on the overall project plan.
- Scoping meeting: To discuss and finalize the proposed scope of the test, including determination of the targets and objectives of the test (flags).

The main outputs of this phase are:

- A formal decision by the entity to start a TIBER-IS test.
- Establishment of a White Team.
- Stakeholder analysis.
- Launch date for the test process.
- Scope specifications of the test, attested by the entities board.
- Procurement of the TI and RT services according to TIBER-IS requirements.
- Project plan for the test.
- Risk management documentation for the test process.

Testing Phase

The Testing Phase is the most extensive phase of the TIBER-IS program and it is split into two sub-phases: Targeted Threat Intelligence and Red Team Testing. The sub-phases are further explained below.

Testing: Targeted Threat Intelligence phase

A core ingredient of threat intelligence-led red team testing is to design attack scenarios based on current and emerging real-world threats with the scope specifications of the test in mind.

During this phase, the Threat Intelligence provider collects, analyzes, and disseminates intelligence relating to two principal areas of interest:

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

As Threat Intelligence provider in a TIBER-IS test has much more distinct time constraints than a real-world threat actor would, the tested entity must provide information in advance to the Threat Intelligence provider to compensate for this difference. This includes information on the tested entity's current threat assessment and examples of recent attacks. It will also include a business and technical overview of each system that supports a critical function that is in scope for the test.

The GTL is shared with the Threat Intelligence provider to form a basis for the Targeted Threat Intelligence report and development of attack scenarios. In the case that infrastructure of the tested entity has been outsourced and a third party is included in the scope of the test, the Targeted Threat Intelligence report should include information about that third party. The Threat Intelligence provider collects and analyzes information from other sources (e.g., open source (OSINT) and human intelligence (HUMINT)) and, together with the information received from the tested entity, it develops scenarios in close collaboration with the White Team, and if possible, also the Red Team. The final scenarios which are to be included in the Targeted Threat Intelligence report, are reviewed, commented on, and agreed upon by the White Team and the TCT.

The main output of this sub-phase is:

- Targeted Threat Intelligence (TTI) Report

Testing: Red Team test phase

The test phase begins with the Threat Intelligence provider handing over the TTI report to the Red Team provider, which includes proposed threat intelligence led scenarios for testing. This should be done in a meeting where the Threat Intelligence provider gives detailed explanations and motivations for the proposed scenarios, and the Red Team provider has the possibility of asking clarifying questions and to ensure that scenarios are viable and in scope for the test.

When the White Team and the Red Team have come to an agreement on attack scenarios, the Red Team test provider will initiate the test. Attack scenarios should be documented in the Red Team test plan. The test will be an intelligence-led red team test, aimed at the tested entity's critical live production systems, people and processes underpinning the entity's critical functions. The test must be conducted in a controlled manner, in close contact with the White Team, in such a way that risks to the tested entity and its critical functions, and any interconnected entities are minimized. The Red Team 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 methodology. Where needed, a "leg-up" will be provided by the entity. The Red Team consults with the White Team and TCT at all critical points to ensure a controlled test. Optionally, the Threat Intelligence provider can be consulted during the test to provide additional information as needed.

During the testing phase, the Red Team provider may be unable to progress to the next stage, due to time constraints or because the Blue Team has successfully protected the entity. In such cases, the White Team and the TTM may agree to give the Red Team provider a 'leg-up' or steer, by giving access to systems, internal networks and so on to continue with the test and

focus on the next flag. All leg-ups and steers must be duly documented and reported in the Red Team Test Report.

The Red Team provider can deviate from the attack scenarios within the Red Team Test Plan, as creativity is needed (as in real life cyber-attacks) if obstacles occur, to develop alternative and sophisticated ways to achieve the test objectives or flags.

The proposed time allocated for Red Team testing will naturally be proportionate to the scope. However, from experience, a period of 12 weeks would be considered appropriate.

The main outputs of this sub-phase are:

- Red Team Test Plan
- Red Team Report (draft)

Closure phase

The last phase in TIBER-IS is the closure phase, during which the tested entity receives the Red Team test report from the Red Team test provider. The Blue Team is finally informed about the test and will write the Blue Team test report, based on the Red Team test report. The Blue Team test report maps the reactions taken by the Blue Team to the steps taken by the Red Team. Following this, a replay workshop between the Red Team, the White Team and the Blue Team will be held. Optionally, a Purple Teaming workshop can be held in connection with the replay workshop to maximize the learning experience of the Blue Team. Experience has shown that this can be a good learning experience for the Blue Team, but the decision to do this is at the discretion of the entity.

The tested entity will then draft a remediation plan, which is to be agreed with the TCT. At the end of the closure phase, a test summary report, which describes the overall process and high-level results, and includes the remediation plan, will be shared with the TCT. The entity's board and the TI/RT providers sign an attestation to validate the true and fair conduct of the TIBER-EU test (to enable recognition by other relevant authorities). If mutually agreed, the lead authority and/or the entity share the Test Summary Report and attestation with other relevant authorities (where applicable).The test ends with a 360-degree feedback meeting. The TCT analyses the overall results of all the TIBER-IS tests and the lessons learned from the 360-degree feedback meetings to produce high-level, aggregated findings.

The TCT analyses the results of all TIBER-IS tests and the lessons learned from the 360-degree feedback meetings to produce high-level, aggregated findings. This information is used to enhance sector resilience and improve the TIBER-IS program.

The main outputs of this phase are:

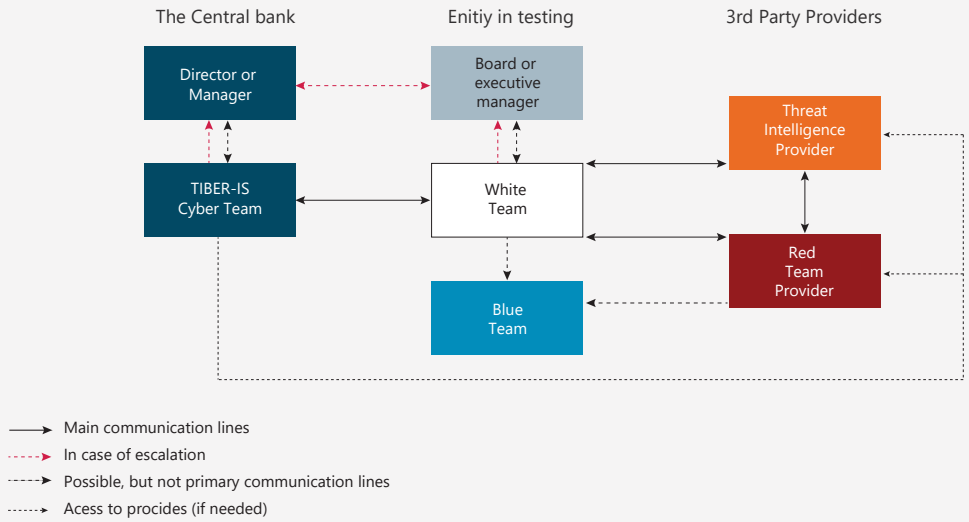
- Blue Team Report.
- Red Team Report (final).
- Test Summary Report (containing remediation plan).
- TIBER-IS attestation.

5

Interactions during a TIBER-IS test

All stakeholders should take a collaborative, transparent and flexible approach to TIBER-IS testing. The interactions between the different stakeholders are described in Figure 4.

Figure 4
TIBER-IS interactions



As shown in the chart, the White Team is the main point of contact during a test. The solid lines represent the standard communication channels, while the dashed lines represent possible, but not primary, channels of communication. Any significant deviations from the original plan should be discussed with the TCT. When differences of opinions arise and cannot be resolved between the White Team and the TCT, the issue should be escalated to their respective superiors. The red lines indicate lines of escalation.

Closing remarks

The publication of this TIBER-IS Implementation Guide marks the implementation of TIBER-EU as the basis for TIBER-IS and thus the start of the TIBER-IS test program for the Icelandic financial sector. These tests are expected to start at the end of 2023.

Abbreviations

BT	Blue Team
CBEST	Bank of England's intelligence-led red team testing program
GTL	Generic Threat Landscape Report
HUMINT	Human intelligence
OSINT	Open-source intelligence
RT	Red Team provider
TCT	TIBER-IS Cyber Team
TTM	TIBER Test Manager
TI	Threat Intelligence provider
TIBER	Threat Intelligence-Based Ethical Red-teaming
TIBER-EU	Common European framework for threat intelligence-based ethical red teaming
TIBER-NL	TIBER program in the Netherlands
TIBER-IS	TIBER program in Iceland
WT	White Team
WTL	White Team Lead