Protokollsbilaga I1
Direktionens protokoll 2019-12-12 §10

SVERIGES RIKSBANK

TIBER-SE
Implementation Guide

TIBER-SE Implementation Guide

Introduction

Background and purpose of TIBER-SE

The Riksbank is Sweden's central bank and a public authority under the Riksdag, the Swedish parliament. The Riksdag has delegated responsibility for monetary policy to the Riksbank and has stipulated in legislation that the objective of the Riksbank's activities is to maintain price stability. According to the Sveriges Riksbank Act, the Riksbank shall also promote a safe and efficient payments system.[1] This has been interpreted as having a responsibility to promote stability in the financial system.[2] 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 Riksbank's stability analysis.

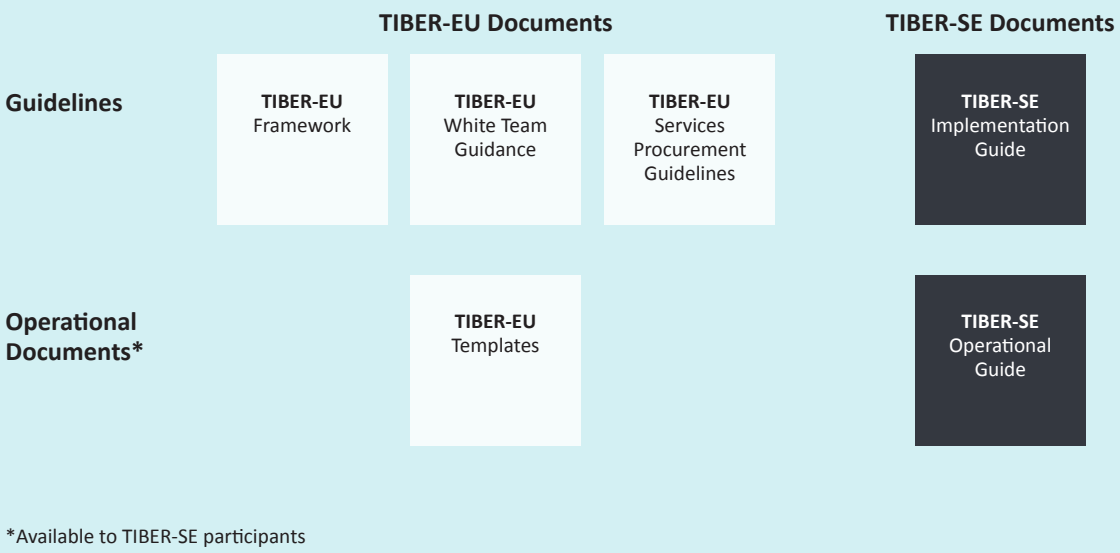
The European Central Bank (ECB) published the Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[3] in May 2018. The framework was jointly developed by the ECB and the EU national central banks and was inspired by the CBEST programme in the UK and TIBER-NL in the Netherlands. TIBER-EU 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. 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;
- standardise and harmonise 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, implement 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 on entities and fostering mutual recognition of tests across the EU;
- create the protocol for cross-authority/cross-border collaboration, result sharing and analysis.

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 Riksbank's Executive Board has adopted TIBER-EU and, with it, the national implementation of TIBER-SE. Following the implementation, the Riksbank is the lead authority of the TIBER-SE framework.

1 Chapter 1, Article 2, Sveriges Riksbank Act.
2 The Riksbank and Financial Stability, 2013.
3 TIBER-EU FRAMEWORK, How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, ECB, May 2018

Figure 1. The TIBER-SE Framework



With this implementation guide, the Riksbank describes the TIBER-SE framework, with the additional purpose of enhancing the cyber resilience of critical entities in the Swedish financial sector. As cyber risk has the potential to become a systemic risk, a further important purpose of TIBER-SE is to increase resilience toward cyber risk in the Swedish financial system as a whole.

Purpose of this guide

This document, the TIBER-SE Implementation Guide, describes the Swedish national implementation of the TIBER-EU framework. It is not a stand-alone document for TIBER-SE; instead, it builds on the TIBER-EU framework (see Figure 1).

Sveriges Riksbank's role and responsibilities in TIBER-SE

The Riksbank implements the TIBER-SE programme for critical financial entities in the Swedish financial sector. The aim of TIBER-SE is to enhance cyber resilience in the Swedish financial sector and thus promote financial stability. Participation in the programme is voluntary but binding once agreed.

The Riksbank is the lead authority of TIBER-SE and the Executive Board of the Riksbank has formal ownership of the programme.

TIBER-SE Cyber Team

The Riksbank is responsible for establishment of the TIBER-SE Cyber Team, TCT, which will be set up within the Riksbank. The role of the TCT is to manage the TIBER-SE programme, maintain the national implementation guide, and act as a point of contact for other TCTs as well as the TIBER-EU Knowledge Centre (TKC). The TCT is also involved in each of the TIBER-SE tests that are carried out in the

programme, where it performs its core function, namely ensuring uniform, high quality tests fulfilling the requirements of TIBER-SE. A key part of the TCT is the Team Test Manager (TTM), which manages the tests from the TCT's side.

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

Generic threat landscape report

An optional part of the TIBER-EU framework is the production of a generic threat landscape report (GTL) for the national financial sector. This is a requirement in TIBER-SE. The Riksbank is responsible for the production of the report and for ensuring that its content is up to date. The Riksbank should ensure that the GTL is updated at least annually. The GTL will be described below in the overview of the TIBER-SE test process.

Ownership of information

The TCT will not share information about a TIBER test with any other authority without having the specific consent of the tested entity, subject to requirements in national law. Furthermore, 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 the competent authorities, if required.

Cross-jurisdictional cooperation

One of the core objectives of TIBER-EU is to standardise and harmonise intelligence-led red team tests in such a way as to enable cross-border testing. To achieve this, the TCT is responsible for liaising with relevant authorities in other jurisdictions prior to such a test. The aim for such discussions should be either to establish a basis for a cross-border test or to promote cross-jurisdictional recognition of the test by explaining and documenting the procedures of the TIBER-SE test.

Legal review

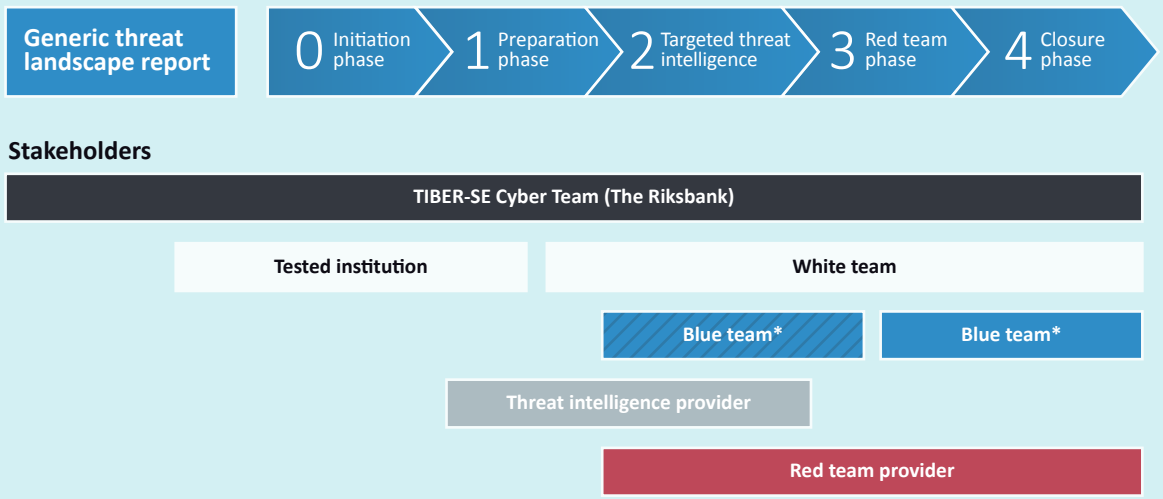
A crucial part of the TIBER-SE framework is ensuring that the requirements, methodologies and processes contained in the TIBER-SE framework do not contravene any national or European Union laws or regulations. The Riksbank has conducted such a review in 2019, with support from a third party, and the implementation of TIBER-SE is deemed compliant with legislation and regulations. In the review, legal and regulatory requirements affecting the participants in TIBER-SE have been examined using a risk-based approach, and both entity-specific and general legal and regulatory requirements have been assessed. The Riksbank will monitor the question of legal and regulatory compliance of TIBER-SE on a continuous basis and is responsible for ensuring legal compliance during the lifetime of TIBER-SE.

Regarding the targeted threat intelligence and red team tests that will be conducted as part of the TIBER-SE programme and procured by the individual tested entities, it is important to note that responsibility for ensuring legal and regulatory compliance lies with the tested entity.

Stakeholders in the TIBER-SE test process

There are three types of direct stakeholders in the TIBER-SE test process: the TCT at the Riksbank, which has been described above; critical financial entities in the Swedish financial sector; and third-party providers of threat intelligence and red team tests.

Figure 2. Overview of the TIBER-SE test process



Critical financial entities

The participants in the TIBER-SE programme are critical financial entities in the Swedish financial sector. Each entity is responsible for its own test in its entirety. This means managing and organising the test and ensuring that the test lives up to the TIBER-SE framework, as well as hiring third-party threat intelligence and red teaming providers and taking responsibility for proper risk management with regard to the test.

The tested entity is responsible for the formation of a white team, led by a white team lead, who is responsible for the coordination of all test activity. Guidance regarding roles, responsibilities and composition of the white team can be found in the document *TIBER-EU White Team Guidance*.[4] All remaining staff at the tested entity that are not part of the white team are considered part of the blue team. A key part of red team testing is that the blue team is completely excluded from all preparation and conduct of the TIBER-SE test, including the 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 from the test.

4 TIBER-EU White Team Guidance: The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test, ECB, December 2018.

Prior to a test, the board or executive management of the tested entity must agree and attest to the scope of the test. 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-SE framework. Both these attestations must be shared with the TCT.

Third-party providers

Using external third-party providers for targeted threat intelligence and red team testing is mandatory under the TIBER-EU framework, and thus also under TIBER-SE. In the process of hiring these third-party providers, the tested entity should ensure that there is mutual agreement on the scope of the test, boundaries and limitations of the test, timing and availability of the third-party provider, actions to be taken and liability. Below follows a non-exhaustive list of what the contracts with the third-party providers should include:

- 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/programmes; jeopardising continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results.[5]

Guidance regarding requirements for the third-party providers can be found in the *TIBER-EU Services Procurement Guidelines*[6], which also specifies the minimum requirements that the third-party providers need to meet. The Procurement Guidelines also set out more details to consider when formalising contractual terms with third party providers.

Overview of the TIBER-SE test process

The TIBER-SE test process begins with the production of the generic threat landscape report. Following this, each test will go through the five test phases: initiation phase, preparation phase, targeted threat intelligence phase, red team test phase and closure phase. The phases are described in the following sections and an overview of the test process is depicted in Figure 2.

Generic threat landscape report

As a first step for the TIBER-SE programme, a generic threat landscape report (GTL) should be produced. The TCT is responsible for the production of the GTL and for sharing the report with the participants in TIBER-SE. If agreed among the TIBER-SE participants, the GTL can be shared with a wider circle.

The GTL will contain information regarding threats to the Swedish financial sector and critical financial entities in the sector. 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 reports.

5 See the TIBER-EU Framework for more examples.
6 TIBER-EU Services Procurement Guidelines, ECB, August 2018.

Initiation phase

During the initiation phase, the TCT will provide the tested entities with the relevant documents 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 as well as the establishment of a white team. An optional element for the initiation phase is the possibility for the tested entity to get an early start regarding risk analysis and/or searching the market for third-party providers.

Preparation phase

The preparation phase begins with the pre-launch meeting between the TCT (including Test Manager) and the white team. During the meeting, discussions will be started regarding the requirements of TIBER-SE, 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 scope of the test includes the tested entity's critical functions and its people, processes and technology. While the white team is responsible for scoping, there should be a mutual agreement between the white team and the TCT regarding the scope. Together, they should also ensure that the scope meets the TIBER-SE requirements and that the test is executed according to plan. If the entity has critical service providers, the norm is that they should be in scope for the test.

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 sound risk management.

Providers of targeted threat intelligence and red teaming will be procured during the preparation phase. These third-party providers must meet the requirements in the *TIBER-EU Services Procurement Guidelines*[7]. It is the responsibility of the white team to see to that this is the case.

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. The meetings are

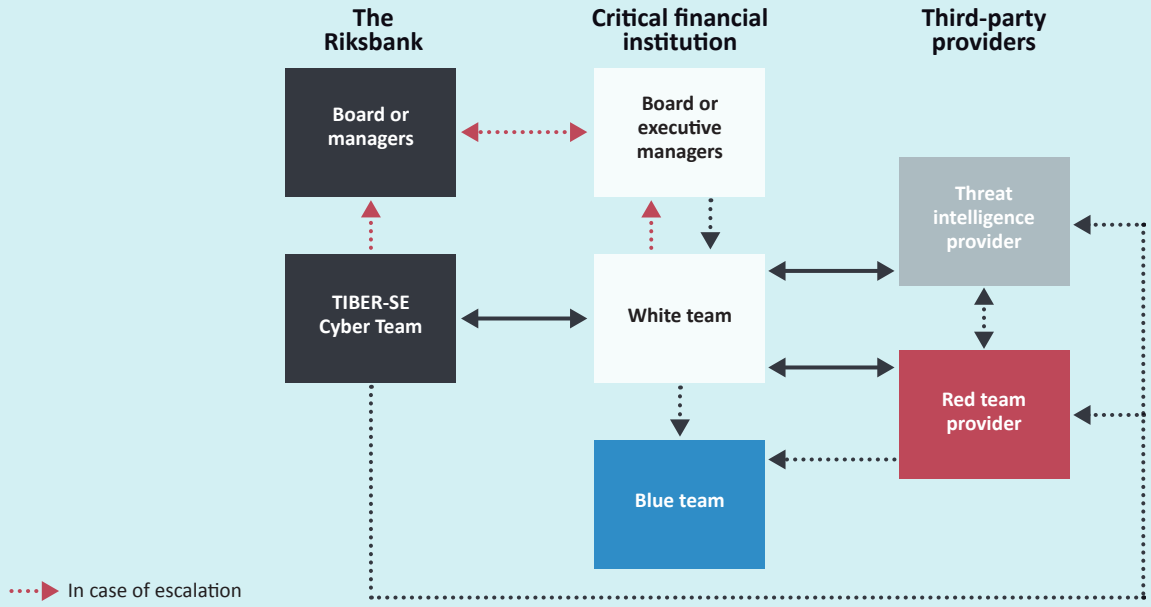
- Launch meeting: discussion and agreement on overall project plan
- Scoping meeting: discussion and finalisation of the proposed scope of the test, including determination of the targets and objectives of the test (flags)

Targeted threat intelligence phase

A core ingredient of threat intelligence-led red team testing is to design attack scenarios based on real-world threats. However, a threat intelligence provider in a TIBER-SE test has much more distinct time constraints than a real-world threat actor would. Consequently, the tested entity will provide information in advance to the targeted threat intelligence provider. This will include 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.

7 TIBER-EU Services Procurement Guidelines, ECB, August 2018.

Figure 3. Interactions during a TIBER-SE 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 analyses 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 and agreed upon by the TCT.

Red team test phase

The red team test phase begins with the threat intelligence provider handing over the targeted threat intelligence report, which includes proposed threat-intelligence led scenarios for testing. The handover should be made during 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 questions.

When the white team and the red team have come to an agreement regarding attack scenarios, the red team test provider will initiate the test. Note that the 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, with close contact with the white team, in such a way that risks to the tested entity and its critical functions and any interconnected entity are minimised. The red team consults with the white team and TCT at all critical points to ensure a controlled test.

The proposed time allocated for red team testing will naturally be proportionate to the scope. However, from experience a period of 10–12 weeks would be considered appropriate.

Closure phase

The last phase is the closure phase, during which the tested entity receives the red team test report from the red team test provider. The blue team will be informed of 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.

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 test will end with a 360-degree feedback meeting. The TCT analyses the overall results of all the TIBER-SE tests and the lessons learned from the 360-degree feedback meetings to produce high-level, aggregated findings.

Interactions during a TIBER-SE test

All stakeholders should take a collaborative, transparent and flexible approach to TIBER-SE testing. The interactions between the different stakeholders are described in Figure 3. As shown in the figure, 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 the TIBER-SE Implementation Guide marks the implementation of TIBER-EU as the basis for TIBER-SE and thus the start of the TIBER-SE test programme for the Swedish financial sector. These tests are expected to take place between 2020 and 2022.

Annex 1: Abbreviations

CBEST	Bank of England's intelligence-led red team testing programme
HUMINT	Human intelligence
OSINT	Open-source intelligence
TCT	TIBER-SE Cyber Team
TTM	Team Test Manager
TIBER	Threat Intelligence-Based Ethical Red-teaming
TIBER-EU	Common European framework for threat intelligence-based ethical red teaming
TIBER-NL	TIBER programme in the Netherlands
TIBER-SE	TIBER programme in Sweden

SVERIGES RIKSBANK
103 37 Stockholm
(Brunkebergstorg 11)

Tel 08 787 00 00
Fax 08 21 05 31
registratorn@riksbank.se
www.riksbank.se