DANMARKS NATIONALBANK

January 2025 | TIBER-DK 4.1

# TIBER-DK
# Implementation Document

# Contents

# Introduction

## What is TIBER-EU?

TIBER-EU[1] is a common European framework developed by the European Central Bank (ECB), providing a uniform and high-quality standard for implementing realistic intelligence-led red team tests on live production environments.[2] It delivers a controlled, bespoke, intelligence-led red team test of entities' critical or important functions. Threat intelligence-led red team tests mimic the tactics, techniques, and procedures of real-life threat actors who, based on threat intelligence, are perceived as posing a genuine threat to entities. A threat intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions and underlying systems, i.e. people, processes, and technologies. The learnings from the test help an entity to assess its protection, detection, and response capabilities and enhance the cyber resilience of entities and thereby of the financial sector more generally.

## What is DORA TLPT?

Ensuring the cyber resilience of the European financial sector constitutes an area of central importance. To address this, the EU has established the Digital Operational Resilience Act (DORA), setting regulatory requirements relating to risk management and IT security.[3] Inter alia, DORA sets requirements regarding Threat Led Penetration Testing (TLPT), stating that TLPT should be used as a learning experience to enhance the digital operational resilience of financial entities. The DORA regulation is in accordance with TIBER-EU, and the TIBER-EU Framework has incorporated the DORA TLPT requirements. The TIBER-EU Framework and supplementary documents should thus be seen as providing additional guidance and contextualisation to the DORA TLPT requirements laid down in DORA and in the Regulatory Technical Standards TLPT (RTS TLPT).

## What is TIBER-DK?

TIBER-DK is based on harmonised requirements in the TIBER-EU Framework, uses TIBER-EU Framework documents in the test process and incorporates the requirements of DORA TLPT in DORA and the RTS TLPT. Thus, a financial entity subject to DORA TLPT, who has performed a TIBER-DK test, has in effect also performed a DORA TLPT.[4]

The focus of a TIBER-DK test is to maximise the entity's learnings and provide insights into strengths and weaknesses in the entity's cyber defence by applying a scenario-based testing approach building on threat intelligence. When working with the findings from the TIBER-DK test, the entity strengthens its cyber defence. This increases the cyber resilience in the Danish financial sector and thereby contributes to the stability of the Danish financial system, which is the overall purpose of the TIBER-DK programme.

[1] TIBER stands for Threat Intelligence-Based Ethical Red teaming.
[2] Please refer to the TIBER-EU Framework (*link*) for more information.
[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector (DORA) and related RTS TLPT. The regulation is translated into Danish law by Act No. 481 of 22 May 2024 and the Danish executive order "Bekendtgørelse om henlæggelse af beføjelser til Danmarks Nationalbank".
[4] According to DORA, financial entities subject to TLPT may refer to and apply the TIBER-EU Framework, or one of its national implementations, in as much as that framework or implementation is consistent with the requirements set out in Article 26 and 27 of the regulation and the corresponding RTS TLPT. See also paper from the ECB *(link)* regarding TIBER-EU and DORA TLPT.

Six principles of TIBER-DK support this purpose, and adhering to these principles will help entities to obtain a valuable test with maximum learning:

- *Learn and evolve*: Being resilient to advanced cyber threats requires practice. TIBER-DK trains entities' protection, detection, and response capabilities, identifies strengths and weaknesses and raises awareness at all organisational levels.
- *Be responsible*: Testing the cyber resilience of entities which are integral to the provision of some of society's most critical functions in live production systems entails a great responsibility, strong ethical behaviour and requires careful planning and risk management as well as competent and controlled execution by all parties involved.
- *Treat cyber risks as threats to the business*: When cyber risks are translated into a context of threatening core business functions, the responsibility of mitigating them shifts from the technical staff to the top management. This shift entails a strategic prioritisation.
- *Be realistic*: A test will resonate and be impactful if the scenarios played out are realistic and the results are believable. Therefore, the intelligence on real threats leads the way for a creative red team that stays true to the narrative of the scenarios.
- *Think holistically*: TIBER-DK targets the core functions that are critical to both the Danish society and to the entity itself, and the scenarios played out would have a systemic impact on financial stability if they were real. TIBER-DK tests are not only technical – roles, processes, and systems are in scope.
- *Share experiences*: By creating a trusted community where TIBER-DK entities learn from each other, each test contributes even more to increasing the cyber resilience in the financial sector.

The first version of the TIBER-DK Implementation was published in December 2018, and the TIBER-DK tests started in January 2019.[5]

This TIBER-DK Implementation Document, published by Danmarks Nationalbank (DN), describes how the requirements in TIBER-EU are adopted and implemented in TIBER-DK. The TIBER-DK Implementation Document also provides a step-by-step description of the TIBER-DK test process, and the TIBER-DK Test Process Overview gives a graphical overview of the elements in a TIBER-DK test. In addition, there are several other TIBER documents, and a document overview can be found in the TIBER-DK Test Process Overview.

This TIBER-DK Implementation Document and other TIBER-DK documents contain elements from the TIBER-EU Framework documents to which the ECB owns the copyrights. If TIBER-DK documents or sections thereof are used outside of the TIBER-DK programme, copyright notice should be included.

Enquiries about TIBER-DK should be directed to: **TIBER-DK@nationalbanken.dk**

[5] More information can be found in Annex 1.

# Stakeholders in TIBER-DK and Cooperation

The key stakeholders involved in a TIBER-DK test are:

- DN as TIBER-DK authority and TIBER-DK Cyber Team
- Entity critical to the Danish financial system, consisting of the Control Team and the Blue Team
- Threat Intelligence Provider and Red Team Testers.

A prerequisite for a valuable test is close cooperation between the key stakeholders.[6] All stakeholders involved in a TIBER-DK test should take a collaborative, transparent and flexible approach to the work together. It is critical that the relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any issues can be addressed in a timely fashion.

## Danmarks Nationalbank as TIBER-DK Authority and TIBER-DK Cyber Team

According to article 26(9), DORA allows Member States to designate a single public authority, i.e. a TLPT authority. The TLPT authority is responsible of all tasks and responsibilities related to TLPT in that Member State. According to Danish law[7], DN has been designated the TLPT authority in Denmark.[8] In the TIBER-DK Implementation, the term TIBER authority is used as a synonym for the TLPT authority.

DN is responsible for setting up an appropriate governance structure of TIBER-DK. This includes establishing a centralised TIBER-DK Cyber Team (TCT)[9] at DN. The TCT is organisationally a part of the section Infrastructure and Cyber under the department Financial Stability and is ringfenced from the remainder of DN. The formal ownership of TIBER-DK rests with a DN governor. The organisation described here is also the formal chain of command used in cases where escalation is deemed necessary.

The role of the TCT is to manage and operationalise the TIBER-DK programme and support each TIBER-DK tests carried out in the programme. Most importantly, the TCT will ensure that the test contains all the mandatory elements defined in the TIBER-DK Implementation. This requires that the TCT participates in all phases of the test, thereby being able to provide feedback to, validate and approve relevant material as well as being able to guide and advice the activities performed. The TCT will assign a designated Test Manager (TM) and an alternate TM to each test as well as dedicated project-, scope- and threat intelligence experts. The TCT also manages the overall planning of TIBER-DK tests, ensuring that the timing of each individual test fits into the overall plan for tests in the TIBER-DK programme.

The entity should provide any information pertaining to the TIBER-DK test to the TCT upon request. The TCT will not share information about the specific TIBER-DK test internally or with any other authority without having consent from the entity. During a TIBER-DK test, the TCT holds the

[6] Exceptions are made for the Blue Team, please refer to section "Entities, Control Team and Blue Team'.
[7] Act no. 481 of 22 May 2024 and the Danish executive order "Bekendtgørelse om henlæggelse af beføjelser til Danmarks Nationalbank".
[8] The competent authorities may follow up on the results of the TIBER test, including the Remediation Plan. However, it is important to note that TIBER is a learning exercise and that TIBER tests are snapshots of specific scenarios rather than comprehensive assessments. The follow-up of results should therefore be conducted in the appropriate spirit, both by the entity and by the authorities.
[9] The term TCT is exclusively used throughout the TIBER-DK Implementation, equating to both the Test Manager (TM) and to the TIBER authority/TLPT authority.

right to invalidate a test from TIBER recognition, if the TCT assesses that the entity is not conducting the test in the right spirit, in accordance with the TIBER-DK principles and requirements, which includes the mandatory requirements of the TIBER-EU Framework or the DORA TLPT regulation.

The TCT is also responsible for updating the TIBER-DK Implementation considering lessons learnt from its implementation and the tests carried out. This can be done in collaboration with the entities participating in TIBER-DK, but also with authorities in other jurisdictions that have adopted TIBER-EU, including the ECB. The TCT facilitates a Danish sector group, the TIBER-DK Group, with the purpose of sharing knowledge and experiences between entities participating in TIBER-DK.[10] The TCT also participates in the knowledge sharing forum for TIBER authorities, TIBER-EU Knowledge Centre (TKC), where countries with an active TIBER programme are represented by their TCT. The TKC is hosted by the ECB.[11]

## Entities, Control Team and Blue Team

The TIBER-DK programme is implemented for the key entities in the Danish financial system with the aim of contributing to the stability of the Danish financial system. Financial entities under DORA TLPT[12] as well as voluntary entities, who are not under DORA TLPT but important for the stability of the Danish financial system[13], are included in the TIBER-DK programme. Generally, an entity performs a TIBER test at least every three years.

For each TIBER-DK test, the entity must establish a Control Team (CT) with a dedicated Control Team Lead (CTL). The CTL coordinates all test activities and is responsible for the day-to-day management of the test and the decisions and actions of the CT. The CT should have the necessary mandate within the entity to guide all aspects of the test, without compromising the secrecy of the test. The members of the CT are the only ones within the entity that know of the TIBER-DK test. The CT should be as small as possible and access to information pertaining to any planned or ongoing TIBER-DK test should at entity level be limited to a need-to-know basis to the CT and the management to reduce the risk of compromising the test.

All staff members of the entity who are not part of the CT are referred to as the Blue Team (BT). In practice, the BT is the employees defending the entity against cyber attacks. The BT can also include external resources, for instance from an external Securities Operations Centre (SOC) or Cyber Defence Centre (CDC). The BT does not know that the test is being prepared or taking place. Since the secrecy of a TIBER-DK test is of utmost importance, all members of the BT are excluded from the information, the preparation, and the conduct of the TIBER-DK test until the Closure Phase.

Each entity is responsible for its own management and organisation of the test, including hiring the Threat Intelligence Providers and Red Team Testers, and for implementing appropriate controls, processes, and procedures to ensure that the test lives up to best practices and that risks are mitigated properly. There are inherent elements of risks associated with a TIBER-DK test as the test takes place in live production environments. Hence, a solid risk management throughout every stage is essential. It is very important that the entity is at all points aware of the particular risks that arise and that these are managed to ensure the TIBER-DK test is conducted in a controlled and safe

[10] Please refer to Annex 2 for more information on the TIBER-DK Group.
[11] More information on TKC can be found in the TIBER-EU Framework (*link*).
[12] Please refer to Annex 3 for more information on entities under DORA TLPT.
[13] For these entities, participation in the TIBER-DK programme is voluntary, but once an entity has agreed to participate, this agreement is considered binding and testing should be performed.

manner. It is important to emphasise that it is the responsibility of the entities to ensure that they conduct the TIBER-DK tests within the remit of all laws and regulations, and that appropriate risk management controls are in place to enforce this. Furthermore, the entity is the legal owner of all the material produced during the TIBER-DK test and is responsible for sharing relevant material with its competent authorities, when required.

## Threat Intelligence Providers and Red Team Testers

For each TIBER-DK test, a Threat Intelligence Provider (TIP) and Red Team Testers (RTT) will be involved. The main tasks for the TIP are to collect and provide threat intelligence and develop threat scenarios in the Targeted Threat Intelligence Report. The RTT, utilising the Targeted Threat Intelligence Report, plan and execute attack scenarios on the target systems and services, and create a Red Team Test Report. It is the responsibility of the RTT to ensure that they conduct the attack scenarios within the remit of all laws, regulations, and ethical boundaries and that appropriate risk management controls are in place to enforce this. Also, the TIP and RTT must work closely together during the test.

As the testing takes place in live production environments only experienced TIP and RTT should be selected by the entity. It is essential that the TIP and RTT have the highest level of skills and expertise, strong ethical behavior and an appropriate experience in threat intelligence and red team testing in the financial sector to be able to deliver effective and most qualified professional services and to reduce the risks.[14]

Based on the DORA regulation, it is mandatory to use an external TIP. In addition, the usage of external testers as RTT is the point of departure. The use of internal testers as RTT is however possible if stringent requirements[15] are fulfilled, and contingent upon TCT approval. The intention is that the internal testers should carry out TIBER tests as effectively and safely as external testers, without the security or the activities of the entity being endangered. When considering using internal testers as RTT, the entity should take notice of that in every three tests they contract external testers as RTT and that a RTT consisting of both internal and external testers are considered as use of internal testers.

## Cross-border Cooperation

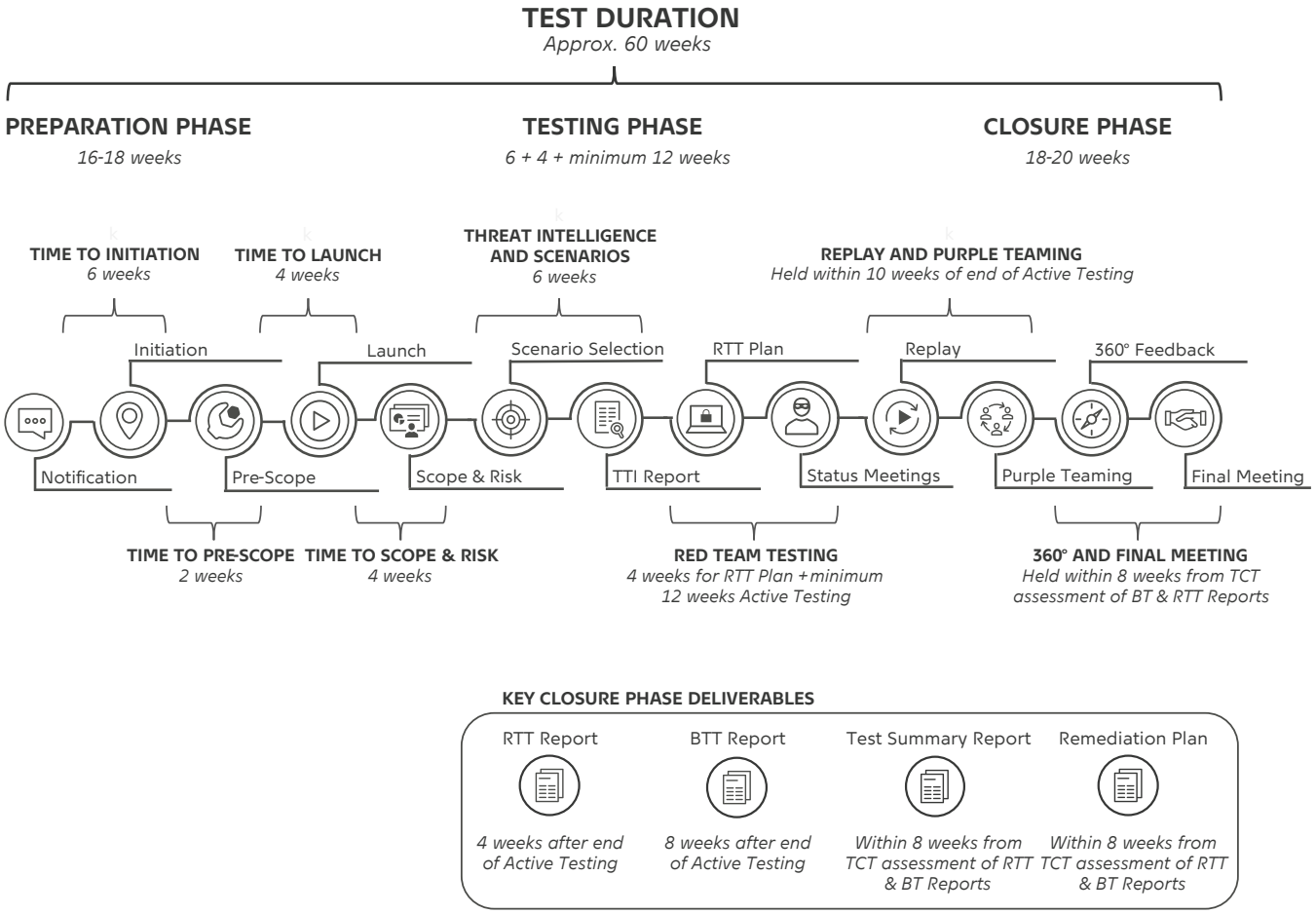
The harmonised approach in TIBER-EU enables cross-border TIBER testing for multinational entities while ensuring focus on regional differences[16]. It is the responsibility of the TCT to liaise with other authorities that potentially are relevant for the test of such a multinational entity. In the beginning of the test, the entity will provide an overview of the entity's operations in other Member States, which will be included in the assessment of whether a cross-border test should be conducted. Also, group structure and the setup of ICT[17] systems in the group will be included in the assessment. Based on the result of the assessment, TCT will reach out to the authorities in these Member States with the aim of establishing cross-border collaboration for the test, including specifying the roles of all parties, or providing documentation for cross-border recognition of the test results.

[14] More information can be found in TIBER-EU Guidance for Service Provider Procurement (*link*).
[15] The internal testers should adhere to the requirements in the TIBER-EU Framework (*link*) and TIBER-EU Guidance for Service Provider Procurement (*link*). Furthermore, the requirements in the RTS TLPT regarding internal testers should be fulfilled.
[16] Please refer to the TIBER-EU Framework and the RTS TLPT for more information on cross-border cooperation.
[17] 'ICT' stands for Information and Communication Technology.

# TIBER-DK Process

This section gives an overview of the TIBER-DK timelines and durations for phases, deliverables, and meetings. More details on the phases can be found below and in the TIBER-DK Test Process Overview.

The DORA regulation sets out requirements regarding timelines and durations for some activities and deliverables. In TIBER-DK, these requirements are incorporated into the documentation. However, based on experience, some durations from the DORA regulation are shortened in TIBER-DK. For instance, the DORA regulation states that the scope should be finalised within 6 months from the start of the test. In TIBER-DK, this period is shortened to approximately 16-18 weeks. In the concrete planning of a specific test, the durations can be extended as long as the planning adheres to the requirements in the DORA regulation.



# Pre-Planning

Before an entity receives a formal notification to carry out a TIBER-DK test, preparatory dialogue will take place between the TCT and designated points of contact at the entity. Pre-Planning will either be arranged for upon the closure of the entity's previous TIBER-DK test or through early dialogue. The TCT will be available to assist and answer any questions the entity may have during all phases, including Pre-Planning.

The entity is encouraged to begin establishing relevant arrangements in a timely manner, including by familiarising itself with TIBER-DK, ensuring appropriate budget and resource allocation, initiating procurement (*link*), ensuring that internal information regarding critical or important functions (CIFs) and critical systems (*link*) is available, and commencing the concrete preparation of leg-ups following the TIBER-DK Guidance for Leg-Ups, to ensure a smooth and well-orchestrated Preparation Phase.

In preparing for a TIBER-DK test and throughout the process, the TIBER-DK Implementation Document, the TIBER-DK Test Process Overview, and the TIBER-EU Framework should be consulted.

It is important to ensure that any information on the TIBER-DK test is limited on a need-to-know basis, including in regard to the management of the entity to preserve the confidentiality and integrity of the test.

# Preparation Phase

As a basis for the Preparation Phase, the entity should become acquainted with the requirements in TIBER-DK and consider the arrangements which need to be in place before the Testing Phase. The following documents are particularly relevant:

- TIBER-EU Control Team Guidance
- TIBER-EU Initiation Documents Guidance
- TIBER-DK Initiation Documents and Rules of Conduct
- TIBER-EU Guidance for Service Provider Procurement
- TIBER-DK Compliance Checklist for TIP
- TIBER-DK Compliance Checklist for RTT
- TIBER-DK Generic Threat Landscape Report
- TIBER-EU Scope Specification Document Guidance
- TIBER-DK Scope Specification Template
- TIBER-DK Guidance for Risk Management

In the Preparation Phase, several key activities are completed that all play an essential role in making the TIBER-DK test successful. These activities include the completion of Initiation Documents and Rules of Conduct, Detailed Project Planning, Procurement and Compliance Checklists, Scope Specification and Risk Management.

## Letter of Notification

Responsible: TCT

Deliverables:
- Letter of Notification

Documents to consult:
- N/A

Process:
- The TCT submits a Letter of Notification to the entity.
- The start date in the Letter of Notification initiates the Preparation Phase in the TIBER-DK test.

Each TIBER-DK test formally starts with a Letter of Notification from TCT. The start date in the Letter of Notification indicates the start of the Preparation Phase and the Letter of Notification includes the requirements on the entity to be followed during testing. Deliverables and deadlines to be followed are provided in the Test Process Overview, which is finalised in the Notification process.

## Notification Meeting

Responsible: TCT

Participants: Entity, TCT

Type: Physical

Duration: 2 hours

Minutes of meeting: TCT

Prerequisites:
- Entity consults the TIBER-DK Test Process Overview provided by the TCT
- Entity prepares suggestion for code name for the test

Agenda:
- Presentation of Letter of Notification, Implementation Document and Test Process Overview
- Introduction to TIBER-DK Initiation Documents and Rules of Conduct, incl. agreement on code name
- Introduction to Procurement and Risk Management

Outcomes:
- Formal notification to conduct a TIBER-DK test elaborated
- Alignment on TIBER-DK Test Process Overview
- Familiarisation with the TIBER-DK test process
- Preparation for producing the TIBER-DK Initiation Documents and Rules of Conduct
- Early start of procurement (*link*), including associated Risk Management (*link*)
- Follow-up meeting planned

Prior to the Notification Meeting, the TCT will provide a draft Test Process Overview with dates to the entity. At the Notification Meeting, the TCT will align with the entity in this regard to finalise the Test Process Overview.

The TCT will also introduce the entity to the requirements and documentation for a TIBER-DK test, with focus on the Preparation Phase, stakeholder roles and responsibilities, and key activities. The main topics are Initiation Documents and Rules of Conduct (*link*), Detailed Project Plan (*link*), Scope Specification (*link*), Risk Management (*link*), and Procurement and Compliance Checklists (*link*). Finally, a follow-up meeting will be planned to provide guidance during the early stages of the Preparation Phase.

## Initiation Documents and Rules of Conduct

Responsible: Entity

Deliverables:
- Initiation Documents and Rules of Conduct

Documents to consult:
- TIBER-DK Initiation Documents and Rules of Conduct
- TIBER-EU Initiation Documents Guidance
- TIBER-EU Control Team Guidance

Process:
- The entity prepares and delivers the Initiation Documents and Rules of Conduct to the TCT.
- The TCT validates the Initiation Documents and Rules of Conduct, including core CT.
- The TCT notifies the CT of its validation.

The Initiation Documents and Rules of Conduct comprise important information regarding the test and the entity, and the Initiation Documents and Rules of Conduct are mainly used as input for preparation and planning activities in the Preparation Phase. The Initiation Documents and Rules of Conduct also describe rules of conduct and practical matters related to the TIBER-DK test process and details in the cooperation between the CT and the TCT.

The entity (in practice, the envisaged CTL) will prepare and deliver the Initiation Documents and Rules of Conduct for the TIBER-DK test to the TCT for assessment and validation. Once the

Initiation Documents and Rules of Conduct are validated by the TCT, the CTL is formally appointed, and the CT established. When the TIP and the RTT are in place, the relevant content of the Initiation Documents and Rules of Conduct should be shared with the TIP and the RTT.

The appointment of a CTL is a key component of the Initiation Documents and Rules of Conduct. Since the CTL is responsible for all test preparations and test activities, including coordination with the TIP and RTT and meetings with the TCT, it is very important that the CTL is appointed early in the Preparation Phase. A CTL is foreseen to use a substantial amount of time during all phases of the TIBER-DK test and is expected to be a senior resource with excellent project management and communication skills. The CTL plays a key role in the safe conduct of a TIBER-DK test and should therefore have sufficient mandate within the entity to guide all aspects of the test whilst safeguarding its confidentiality. In appointing a CTL, both role, in-depth knowledge of the entity, strategic positioning, seniority and access to the management board should be considered.

The CTL is responsible for the day-to-day management of the TIBER-DK test and the decisions and actions of the CT. Due to the importance of the CTL role, it is crucial that at least one other member of the CT is kept well informed about the test details to deputise for the CTL if and when needed.

As part of the Initiation Documents and Rules of Conduct, the CTL should arrange the entity's own organisation of the management of the TIBER-DK test. For the TIBER-DK test, the CTL must follow the TIBER-EU Control Team Guidance (*link*) to establish a CT[18].

The CTL will inform the TCT of the members included in the CT by adding the relevant names and contact information to the Initiation Documents and Rules of Conduct. The TCT must validate the initial composition of the CT along with any subsequent composition changes. The CT must provide any information pertaining to the TIBER-DK test to the TCT upon request.

The CT should be kept as small as possible to reduce the risk of compromising the secrecy of the TIBER-DK test. Therefore, the CTL should ensure that the CT is comprised of a select number of individuals with critical decision-making capacity and/or subject matter expertise, including within cyber, operational risk, business and project- and test management domains. The CT should have a well-rounded overview of the organisation, including of its business areas, technical landscape and security posture. In addition, the CT should have access to the top of the security incident escalation chain to stay abreast of any developments or impact as needed. The CT must ensure that it is informed of any detection of the TIBER-DK test, both by staff members of the financial entity and/or of its third-party service providers where relevant. In such cases, the CT must contain the escalation of the resulting incident response as needed.

The CT should ensure that access to information pertaining to any planned or ongoing TIBER-DK test is limited on a need-to-know basis to the CT, the entity's management body, the TCT, TIP and RTT. This ensures the secrecy of the TIBER-DK test. To safeguard secrecy, staff members of the entity outside of the CT must only be made aware of a planned or ongoing TIBER-DK test in case of cogent reasons and prior agreement from the TCT. This ensures secrecy is upheld as widely as possible, even in case of detection. In addition, arrangements protecting the secrecy of the TIBER-

[18] In the *TIBER-DK Process*, the term 'entity' is exclusively used until the CT is formally established in the TIBER-DK Initiation Documents and Rules of Conduct (*link*), after which the term 'CT' is exclusively used. Within the described processual bounds, the specified terms equate to both 'entity' and the 'CTL' where the latter terms are used instead in the TIBER-EU Framework and/or applicable regulation.

DK test, applicable to staff of the entity, of relevant ICT third-party service providers, TIP and RTT must be put in place by the CT.

It should be noted that the CT might be supplemented as the preparations continue and that the core CT could be extended, for instance to include key contact persons from critical suppliers. As relevant, this could include representatives from for instance the Nordic Financial CERT (NFCERT) and the Centre for Cyber Security (CFCS). Relevant Subject Matter Experts (SMEs) can later be included in the CT as the TIBER-DK test develops pending TCT approval, including in connection with Scope Specification and in regard to scenarios pertaining to the SMEs respective areas of expertise.

Because of the sensitive nature of the preparation and execution of the TIBER-DK test, the entity could consider the need for CT members to sign a non-disclosure agreement (NDA) on a voluntary basis to ensure the internal/external confidentiality of the test. An example NDA is embedded in the Initiation Documents and Rules of Conduct.

To ensure that the test runs effectively, it is important to consider the relevant stakeholders of the test, including which role service providers critical to the delivery of the core services to the entity should have. In the Initiation Documents and Rules of Conduct, an overview of the entity's ICT third-party service providers and operations in other Member States should be specified to ensure identification of which entities might be included in the test. For inspiration, more related information can be found under Scope Specification and Attestation (*link*).

Furthermore, it should be anchored whether the entity will use an external provider as RTT, internal testers as RTT, or both. At this point in time, if the entity intends to use internal testers as RTT, it is expected that the entity has already submitted the formal application required to the TCT, and that the TCT has made the assessment and informed the entity thereof.

## Initiation Meeting

Responsible: TCT

Participants: Entity, TCT

Type: Physical

Duration: 2 hours

Minutes of meeting: TCT

Prerequisites:
- Entity appoints CTL and establishes CT
- Entity drafts Initiation Documents and Rules of Conduct

Agenda:
- Presentation of Initiation Documents and Rules of Conduct and Procurement status
- Alignment on Initiation Documents and Rules of Conduct
- Introduction to Detailed Project Plan and preparation for Pre-Scope Meeting

Outcomes:
- Alignment on Initiation Documents and Rules of Conduct
- Briefing on current status on Procurement (*link*)
- Status on initial risk management efforts (*link*) undertaken by the CT
- Preparation for upcoming Pre-Scope Meeting
- Planning regular CT progress meetings

At the Initiation Meeting, the CT will brief the TCT on the contents of the Initiation Documents and Rules of Conduct, including the composition of the proposed CT. In addition, the entity's current status on and considerations regarding procurement should be presented, along with the initial efforts undertaken to manage the risks of the test.

If necessary, the TCT will guide the entity towards the finalisation of the Initiation Documents and Rules of Conduct. Furthermore, the CT will be able to raise questions that have been identified during the initial project planning. In particular, discussions on scope will be a focal point as the TCT prepares the CT for the upcoming Pre-Scope Meeting (*link*).

Finally, regular CT progress meetings between the CT and the TCT will be scheduled at the Initiation Meeting to ensure that the preparations advance according to plan.

## Detailed Project Plan

Responsible: CT

Deliverables:
- Detailed Project Plan

Documents to consult:
- TIBER-DK Initiation Documents and Rules of Conduct
- Test Process Overview

Process:
- The CT shares the Detailed Project Plan with the TCT.
- The TCT provides high-level feedback to the Detailed Project Plan.

As early as possible, the CTL should begin developing a Detailed Project Plan. The entity should use its own format for the Detailed Project Plan, but the content of the plan should be based on the Test Process Overview and the dates agreed between the entity and the TCT.

The Detailed Project Plan must include a schedule of meetings to be held between the CT, the TIP, the RTT and the TCT as well as a schedule for other activities, including but not limited to input collection to deliverables, review and approval processes, delivery of the planned deliverables in draft and final draft versions, and internal communication. An example template is provided in the Initiation Documents and Rules of Conduct.

Once the TIP and RTT are in place in the Preparation Phase, the CT must finalise the Detailed Project Plan. It should be noted that the entity can continuously update the Detailed Project Plan; however, deviations from the original planning in the Test Process Overview should be discussed in advance with the TCT.

## Preliminary List of CIFs

Responsible: CT

Deliverables:
- Prepare Preliminary List of CIFs for the Pre-Scope Meeting and as input for the subsequent work on the TIBER-DK Scope Specification (*link*)

Documents to consult:
- TIBER-DK Scope Specification Template
- TIBER-EU Scope Specification Document Guidance

Process:
- The CT prepares a preliminary list of the entity's CIFs and underpinning critical systems.

In preparation for the Pre-Scope Meeting, the CT should create a preliminary list of the entity's CIFs and investigate how the societal impact of these functions and their dependencies on critical ICT

systems, roles and processes.

A CIF is defined as: *"a function, the disruption of which would materially impair the performance of an 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 an entity with the conditions and obligations of its authorisation, or with its other obligations under applicable law"*.

For this purpose, for example high-level system architecture diagrams or internal risk assessments of the system landscape should be acquired to provide an overview of the entity's critical systems underpinning the CIFs. The CT can consult the Scope Specification Template to find examples on how to fill out the scope that can help identify which information is needed. Related information can be found under Scope Specification and Attestation (*link*).

## Pre-Scope Meeting

Responsible: TCT

Participants: CT, TCT

Type: Physical

Duration: 2 hours

Minutes of meeting: TCT

Prerequisites:
- CT establishes a methodology for identifying CIFs
- CT creates a Preliminary List of CIFs
- CT acquires information on high-level system architecture
- CT acquires information on critical business processes

Agenda:
- Presentation of scope process incl. Scope Specification Template and examples
- Presentation of business areas and Preliminary List of CIFs and systems
- Discussion of Preliminary List of CIFs and flags

Outcomes:
- Preliminary identification of the entity's CIFs, their underpinning critical systems/processes, and discussion of potential flags

The TCT guides the work of the CT on scope to commence as early as possible in the Preparation Phase. To provide a strong foundation for the Scope Specification, the TCT will arrange a Pre-Scope Meeting.

At the Pre-Scope Meeting, the CT will present their business areas, the Preliminary List of CIFs and explain the high-level system landscape of the entity. The TCT will provide relevant input, examples of CIFs and flags, in addition to guiding the CT on the remainder of the process. For this purpose, it may be relevant to include Subject Matter Experts (SMEs) with extensive insights into both the business and IT side of the entity, taking into consideration the secrecy of the test. If these resources are not already present within the CT and if the entity chooses to include them, the SMEs could sign an NDA.

The outcome of the Pre-Scope Meeting is to ensure relevant progress on identifying the entity's CIFs, its underpinning critical systems/processes and potential flags in the Scope Specification (*link*).

## Procurement and Compliance Checklists

Responsible: CT

Deliverables:
- Compliance Checklist for TIP
- Compliance Checklist for RTT
- Signed TIP and RTT Contracts (should not be shared with TCT)

Documents to consult:
- TIBER-DK Compliance Checklist for TIP
- TIBER-DK Compliance Checklist for RTT
- TIBER-EU Guidance for Service Provider Procurement

Process:
- The CT documents assessment of TIP and RTT compliance with applicable requirements and criteria and provides evidence of its assessment to the TCT.
- The CT delivers Compliance Checklists for TIP and RTT to the TCT.
- The CT does not proceed with contracting the selected TIP/RTT where the TCT is of the opinion that the selected TIP/RTT do not ensure compliance.

Procurement constitutes an essential overarching precondition for the test. The time needed for procurement varies across entities, and appropriate time and resources should be allocated to ensure a timely procurement process. Therefore, it is recommended that the procurement process for external TIP and RTT be started early, often already at the time of Notification or during the late stages of Pre-Planning.

The same early start is recommended if the entity intends to use internal testers as RTT in a TIBER-DK test. The entity should as early as possibly indicate this intention to the TCT, preferably in the preparatory dialogue that takes place between the TCT and the entity during Pre-Planning (*link*). To use internal testers as RTT, the respective entity must submit to the TCT a concrete application for assessment by the TCT in connection with the applicable TIBER-DK test. The TCT can provide guidance on the requirements for such an application. This early start is important, if the internal testers cannot be used as RTT as intended in the specific test, so that procurement of external RTT can take place timely.

TIP and RTT with adequate experience are a key means of managing the risks associated with the TIBER-DK test, and the CT must make sure to use the most competent, qualified, and skilled TIP and RTT that meet the right standards of risk management and show strong ethical behaviour. Relevant questions to include in the dialogue when procuring TIP and RTT can be found in the Guidance for Service Provider Procurement.

To ensure that the TIP and RTT meet the appropriate standards for conducting a TIBER-DK test, the entity should carry out due diligence to ensure compliance with the minimum requirements and guidance set out in detail in the Guidance for Service Provider Procurement. Furthermore, it is the responsibility of the entity, the TIP and the RTT to ensure that they conduct tests within the remit of law and regulation and that appropriate risk management controls (e.g. contracts) are in place to enforce this.

To document compliance with the minimum requirements and guidance and to assure the TCT of the entity's due diligence regarding the selection of TIP and RTT, the entity should fill out the Compliance Checklists for the TIP and the RTT and share them with TCT before signing the contracts with the TIP and RTT, respectively. The TCT may request more details regarding the TIP and RTT, e.g. regarding the team composition and qualifications as well as their methodology. On the basis of the Compliance Checklists, TCT will provide its feedback either in the form of "non-

objection", whereby the procurement process can continue, or as an "objection", in which case TCT will explain the reasons for the objection. The entity must receive a non-objection in order to proceed with the procurement process, i.e. signing the contracts.

Signed contracts with the TIP and RTT must be in place before the Launch Meeting. The contracts should not be shared with the TCT.[19]

Once the procurement process has been completed, all relevant contractual arrangements should be in place.

## Launch Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Physical

Duration: 2 hours

Minutes of meeting: CT

Prerequisites:

- CT establishment of Detailed Project Plan (*link*)
- TIP and RTT presentations of teams and approaches

Agenda:

- Presentation of CT expectations incl. scheduling and current status
- Presentations from TIP and RTT on team composition, approach and cooperation
- Presentation on TCT expectations

Outcomes:

- Establish a good basis for cooperation
- Align expectations on cooperation and the coming test phases and activities
- Alignment on scheduling

Once the TIP and the RTT are in place, the Launch Meeting marks their onboarding and thereby the beginning of the cooperation between the CT, TCT, TIP and RTT. The Launch Meeting provides the opportunity for expectation alignment, including by ensuring that the TIP and RTT are briefed on key aspects of preparations thus far, and that the road ahead is mutually understood.

During the Launch Meeting, all stakeholders introduce their roles and their expectations of the test process. The TIP and RTT are expected to present their teams and to explain their approaches in regard to the TIBER-DK test. The TIP and the RTT should also outline how they will cooperate during the Testing and Closure Phases. Expectations for cooperation and deliverables with the CT and TCT should additionally be mutually aligned**.** Scheduling will also be introduced, taking point of departure in the Detailed Project Plan (*link*) delivered by the CT and the Test Process Overview. Finally, the forthcoming steps regarding Scope Specification and Attestation (*link*) and Risk Management Documentation (*link*) are discussed.

[19] In the case of a multi-party test, the same external RTT and TIP shall be used for the purpose of conducting the test. The involved entities should mutually agree on contractual arrangements with the selected TIP and RTT. The TIBER-EU Guidance for Service Provider Procurement sets out in greater detail agreement checklists for the entity and TIP/RTT to consider when formalising their contractual agreements.

## Scope Specification and Attestation

Responsible: CT

Deliverables:
- Scope Specification
- Letter of Attestation for Scope

Documents to consult:
- TIBER-DK Scope Specification Template
- TIBER-EU Scope Specification Document Guidance
- TIBER-DK Letter of Attestation for Scope

Process:
- The Scope Specification is delivered by the CT to the TCT.
- The TCT validates and approves the Scope Specification and notifies the CT thereof.
- The CT ensures that the TIBER-DK Letter of Attestation for Scope is signed by high-level management at the entity.
- The final Scope Specification should be shared by CT with TIP and RTT.

In a TIBER-DK test, the scope serves to focus efforts on relevant functions and systems by societal criticality, thereby ensuring value in generated learning. The key objective of the scope activity is for the entity and the TCT to agree on the scope of the TIBER-DK test, formalised in the Scope Specification, which must be approved by the TCT.

The scope is useful in a multitude of processes and activities throughout the TIBER-DK test, including as input for refinement in the construction and operationalisation of threat intelligence-based test scenarios by the TIP and RTT. Therefore, the entity should consider its CIFs (*link*) and the systems that support it at an early stage, thereby taking the initial steps towards the creation of a test scope.

The Scope Specification must include all the identified CIFs of the entity and list the key systems and services that underpin each CIF. This includes CIFs which have been outsourced or contracted to ICT third-party service providers. If an identified CIF is not to be included in the scope of the test, a justification should be provided in the Scope Specification for its exclusion. Pending the outcome of the final scenario selection in the Testing Phase: Threat Intelligence and Scenarios (*link*), some included CIFs may not be tested. If deemed appropriate by the CT in consultation with the TCT, additional non-CIFs (i.e. roles, processes and technologies) may be supplementarily included in the scope, provided these do not negatively affect the testing of the CIFs.

In the inclusion of CIFs, the CT should consider as criteria:

- the criticality or importance of the function and its possible impact to the financial sector and on financial stability in Denmark and the EU
- the importance of the function for the day-to-day business operations of the financial entity
- the exchangeability of the function
- the interconnectedness with other functions
- the geographical location of the function
- the sectoral dependence of other entities on the function
- where available, threat intelligence concerning the function.

In the Scope Specification, the CT must use the included CIFs and key systems to specify flags to be captured in the TIBER-DK test. Flags essentially constitute the targets and objectives that the RTT must strive to achieve during the Active Testing if the specifically related CIF is part of an attack scenario. Flags should therefore be specified for each CIF included in scope for testing. Although the flags are set during the scope process, they can evolve on an iterative basis following the

Testing Phase: Threat Intelligence and Scenarios (*link*) and during the Testing Phase: Red Team Testing (*link*). The CT should discuss the flags with the TCT.

The TCT will review and provide feedback to the Scope Specification, and the TCT must approve the Scope Specification in order for it to be final. The TCT will validate that the Scope Specification is complete and ensures the performance of an appropriate and effective test.

Importantly, when approved by TCT, the Scope Specification will also need to be approved via attestation by high-level management at the entity. In addition, the final Scope Specification must be shared with the TIP and RTT once approved.

## Scope Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Virtual

Duration: 1 hour

Minutes of meeting: CT

Prerequisites:
- CT prepares Scope Specification

Agenda:
- Presentation of core business areas, ICT setup and Scope Specification incl. methodology, CIFs and justification for inclusion
- Alignment on Scope Specification

Outcomes:
- Align on the Scope Specification

At the Scope Meeting, the CT presents the Scope Specification and the methodology for selecting the CIFs, underpinning systems and services as well as related flags. The CT presentation should include walkthroughs of:

- business model, including core business areas, ICT third-party service providers, overall ICT setup and governance,
- CIFs and justification(s) for inclusion, specifying the prioritised areas of focus,
- flags and justification(s) for inclusion of ICT system(s).

For the test to be successful, it is important that the TIP and RTT understand both the Scope Specification and the business of the entity. Therefore, the TIP and RTT shall participate at the Scope Meeting. The Scope Meeting will be held in conjunction with the Risk Meeting.

## Risk Management Documentation

Responsible: CT

Deliverables:
- Risk Management Documentation

Documents to consult:
- TIBER-DK Guidance for Risk Management

Process:
- The CT should consult the TCT on the risk assessment and risk management measures.
- The CT shall review the risk assessment and risk management measures where the TCT is of the opinion that they do not adequately address the risks of the TIBER test.
- The CT should regularly assess the risks and the related mitigation measures throughout the test.

A TIBER-DK test harbours elements of risk[20], for instance owing to the criticality of the target systems in live production environments, and the roles and the processes involved in the tests. The CT is responsible for implementing appropriate controls, processes and procedures to ensure that the test is carried out with sufficient assurances for all stakeholders that risks will be identified, analysed and handled according to the entity's practices.

The CT should conduct a risk assessment before and during the active testing, linking this to relevant risk management measures. The CT should consult the TCT on the risk assessment and risk management measures.

The CT should document to the TCT that appropriate risk management activities have been conducted prior to the Risk Meeting. For this purpose, the Risk Management Documentation embedded in the Guidance for Risk Management should be filled out by the CT. If the CT has a preferred format different to that provided in the Risk Management Documentation, the CT may instead use their alternative format. However, regardless of the format, the information contained in the documentation must comply with the requirements set out in the Guidance for Risk Management. The CT shall review the risk assessment and risk management measures where the TCT is of the opinion that they do not adequately address the risks of the TIBER-DK test. In addition, the CT should regularly assess the risks and related mitigation measures throughout the TIBER-DK test, for instance when the attack scenarios have been developed.

During Active Testing (*link*), the Risk Management Documentation should be consulted as needed and any risk not already identified related to RTT activity should be assessed by the CT and discussed at the Status Meetings (*link*).

## Risk Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Virtual

Duration: 1 hour

Minutes of meeting: CT

Prerequisites:

- CT drafts Risk Management Documentation

Agenda:

- Presentation of basis for Risk Assessment incl risks and risk strategy
- Alignment on Risk Management Documentation

Outcomes:

- Walkthrough of the Risk Management Documentation

At the Risk Meeting, the CT presents the risks identified as part of the conducted risk assessment. For each risk, the CT should describe their risk strategy by specifying acceptance, mitigation or elimination, and provide actions as needed to reduce or avoid the identified risk(s).

When the Risk Meeting takes place, most risks will have been identified, and some may remain open or partially managed, for instance those requiring RTT input. This reflects that risk assessment and management are fluid processes, and the Risk Meeting provides the opportunity

[20] For instance, 1) Introducing malware in live production environments may ultimately lead to shutting down systems as part of the playbook to isolate the infected system, causing unavailability, 2) Important service accounts may be locked out as a result of Active Testing activities causing downtime.

to take stock of current preparations. Risk Management will naturally continue throughout the Testing Phases and revisited on bi-weekly CT progress meetings.

The Risk Meeting will be held in conjunction with the Scope Meeting.

# Testing Phase: Threat Intelligence and Scenarios

After the Preparation Phase, focus is shifted to the threat intelligence components of the test. The TIBER process is designed to create realistic threat scenarios describing attacks against an entity's CIFs. The threat scenarios will be elaborated in a Targeted Threat Intelligence Report , also containing tailored and contextualised analysis of relevant target and threat intelligence on the entity.

In the TIBER-EU Framework, it is recommended that national jurisdictions should produce a national Generic Threat Landscape Report for the financial sector. In TIBER-DK, it has been chosen to follow this recommendation, since it is effective to describe the threat landscape in one consolidated report, in relation to both reducing costs and promoting knowledge sharing. The Generic Threat Landscape Report contextualises the Danish financial sector's threat landscape by mapping CIFs to relevant threat actors. The TCT has the overall responsibility for ensuring that such a report is available to the entities. The NFCERT (*link*) authors the report and is responsible for inviting the TCT and the entities to be involved in the drafting process and to collect feedback and validation from the CFCS (*link*) for further enrichment of the report. The report will be updated yearly. The Generic Threat Landscape Report contains foundational analysis for the Testing Phase: Threat Intelligence and Scenarios, and should be leveraged by the TIP via contextualisation, ensuring that its insights are tailored, augmented, and nuanced to the entity. In this process, the TIP should also ensure that analyses from the Generic Threat Landscape Report relevant to the entity are brought up to date in light of the significant pace of developments in the threat landscape.

In the Testing Phase: Threat Intelligence and Scenarios, the following documents are particularly relevant:

- TIBER-DK Generic Threat Landscape Report
- Scope Specification
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-DK MITRE ATT&CK® Template

## Scenario Longlist

Responsible: TIP

Deliverables:
- Scenario Longlist

Documents to consult:
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-DK Generic Threat Landscape Report
- Scope Specification

Process:
- The TIP prepares and proposes a longlist of 6-10 draft threat scenarios.
- Taking into account specified criteria, including input from the TCT, the CT selects and suggests adaptations for three or more scenarios.
- The TIP notes the suggestions for adaptation and details the selected scenarios in full within the Targeted Threat Intelligence Report (*link*) for TCT approval.

The TIP should prepare a Scenario Longlist of 6-10 relevant draft threat scenarios based on intelligence acquired via target identification (*link*). The draft threat scenarios should be contextualised and tailored by analytically synthesising insights on the entity's business environment and system landscape with intelligence on threat actors, their objectives, and the modus operandi and methodologies used to achieve them. In designing the draft threat scenarios, the TIP should evaluate and involve every CIF included in scope of the test. As such, the draft threat scenarios should include the threat actors the TIP assesses as being most likely to target the entity. The TIP should ensure diversity among the draft threat scenarios, including regarding threat actors, TTPs and targeted CIFs, to ensure broad generation of learning pending the final selection and/or adaptation into final threat scenarios. The draft threat scenarios may also benefit from including elements of a forward-looking nature to provide the opportunity to generate future-proof learning.

The scenario selection of the CT should be based on the following criteria:

- the recommendation of the TIP, taking into account the threat-led nature of the scenarios
- the input provided by the TCT
- the feasibility of the proposed scenarios for execution, based on the expert judgement of the RTT
- strategic criteria (e.g. regarding scenarios of past tests, the need for leg-ups)
- the size, complexity and overall risk profile of the entity and the nature, scale and complexity of its services, activities and operations.

Real-world threat actors may have months to prepare an attack. To ensure efficient intelligence gathering within time and resource constraints, the TIP should request information from the CT relevant to the scope and business of the entity and the CT should provide all the information to the TIP it deems relevant. For this purpose, the TIP's preferred format can be used. Some examples of the information that should be provided are:

- a business and technical overview of each CIF-supporting system in the scope
- the current threat assessment and/or threat register
- examples of recent attacks on the entity or its environment
- previous Targeted Threat Intelligence Reports used in TIBER tests, if relevant and deemed feasible by the entity.

Obtaining the relevant input for the TIP without alerting the organisation of an imminent test may require the CT to gather information slowly and to use convincing cover stories. Therefore, these activities may begin as early as the Preparation Phase once the contract with the TIP is signed.

Ensuring a controlled information flow towards the RTT is imperative. The information given by the CT to the TIP should serve to help focus their analysis, but the information should only be handed over to the RTT if the TIP is able to confirm the information provided by the CT. The reasoning behind such information flow control measures is to ensure that the RTT are not provided with unintended advantages in Active Testing.

If deemed necessary by the CT, and with explicit consent from the TCT, the RTT may commence non-intrusive active reconnaissance[21] at a suitable point in time during the Testing Phase: Threat

[21] Port scanning, phone calls, sending emails and linking on social media are all considered active reconnaissance. Activities like Google and dark web searches as well as browsing the entity's web pages are considered passive reconnaissance.

Intelligence and Scenarios. This potential head start of Active Testing activities has the purpose of accommodating stealthy reconnaissance without prolonging the test by providing TIP with relevant information they are not allowed to obtain themselves. If active reconnaissance is conducted by the RTT, it is imperative that the same precautions to remain undetected as would be taken during the Active Testing are observed.

## Scenario Selection Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Virtual

Duration: 2 hours

Minutes of meeting: CT

Prerequisites:
- TIP prepares Scenario Longlist

Agenda:
- Presentation of Scenario Longlist incl. background, methodology, threat actors, TTPs and CIFs
- Suggestions for adaptation
- Alignment on selection of scenarios

Outcomes:
- Draft threat scenarios presented by TIP and discussed by participants
- Alignment on a minimum of three scenarios to be selected or adapted

At the Scenario Selection Meeting, the prepared Scenario Longlist is discussed. The TIP will explain the background and methodology for each threat scenario in draft, and the participants will evaluate the Scenario Longlist and narrow it down with focus on threat actors, TTPs and targeted CIFs, to ensure broad generation of learning. The participants may offer their suggestions for adaptation at and/or in connection with the Scenario Selection Meeting. Thereby, the most relevant threat scenarios to proceed with for further adaptation and detailing are selected.

## Targeted Threat Intelligence Report

Responsible: TIP

Deliverables:
- Targeted Threat Intelligence Report
- MITRE ATT&CK Template

Documents to consult:
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-DK MITRE ATT&CK Template

Process:
- The TIP creates and delivers the Targeted Threat Intelligence Report to the CT, including a populated MITRE ATT&CK Template.
- Upon receipt from the TIP, the CT delivers the Targeted Threat Intelligence Report and filled out MITRE ATT&CK Template to the TCT and RTT.
- The RTT may provide feedback to enrich the Targeted Threat Intelligence Report.
- The TCT must approve the Targeted Threat Intelligence Report, including scenarios, for finalisation thereof.
- The TCT informs the CT of Targeted Threat Intelligence Report approval.

The main deliverable in the Testing Phase: Threat Intelligence and Scenarios is the Targeted Threat Intelligence Report on the entity, setting out the threat scenarios for the test.

During the targeted threat intelligence process, the TIP collects, analyses, and disseminates CIF-focused intelligence relating to two key areas of interest:

1. Targeted intelligence or information on potential attack surfaces and exposures across the entity
2. Threat intelligence or information on relevant threat actors and probable threat scenarios.

To identify targets (item 1 above), the TIP should carry out a broad exercise of the kind typically undertaken by real threat actors as they prepare for their attack. The objective is to form a detailed preliminary picture of the entity with focus on points of interest from the attacker's perspective, including those stemming from the use of third-party service providers (e.g. network, IT processing, software providers). The Targeted Threat Intelligence Report should specify CIFs in scope, their geographical location, the official EU language(s) in use, the relevant service providers and the period of time over which the research is gathered.

If active reconnaissance has been conducted by the RTT, this may be used to validate the passively collected intelligence, and the RTT are expected to share their findings with the TIP in order to enable the information to be reflected in a separate section of the Targeted Threat Intelligence Report.

The output of the target identification is a description, on a CIF focused, system-by-system basis, of the attack surfaces of roles, processes and technologies in relation to the entity and its digital footprint. This includes information that is intentionally published by the entity and internal information that has been unintentionally leaked. This should result in an overall assessment of the concrete, actionable intelligence that can be found on the entity, including elements such as:

- employee usernames and passwords
- look-a-like domains which can be mistaken for those of the entity
- technical reconnaissance of vulnerable and/or exploitable software
- systems and technologies
- information related to the entity posted by employees on social media which might be used for the purposes of the attack
- information for sale on the dark web
- any other relevant information available on the internet or public networks
- where relevant, physical targeting information, including ways of access to the premises of the financial entity.

If the targeted intelligence points to any threats or vulnerabilities that need immediate action and follow-up, these findings should be addressed according to the entity's practices in risk management.

With regard to threats (item 2 above), the TIP should use the Generic Threat Landscape Report as a basis for the identification of relevant threat actors. With this starting point, the TIP collects, analyses and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence specifically tailored to the entity's business environment, which should also include third-party service providers if these providers are critical to the operation of the CIFs included in the scope.

The output resulting from the threat identification is a summary of the key threats and detailed profiles of the most relevant threat actors that may target the entity. This includes the systems of the entity that malicious actors are most likely to compromise or target, the possible motivation,

intent and rationale for the potential targeting and the possible modus operandi and TTPs of the attackers.

Equipped with the output from target identification and threat identification, the TIP produces at least three fully elaborated intelligence-led threat scenarios[22] describing an end-to-end attack path. Of these, at least one scenario should include, but not be limited to, respectively (i) compromised service availability, (ii) compromised data integrity and (iii) compromised information confidentiality.

Threat scenarios are written from an attacker's point of view and emulate the attacker's capabilities. This implies a detailed description of the emulated threat actor's preferred methodology. To avoid the threat scenarios being only backward-looking, the TIP should enhance each threat scenario with forward-looking plausible TTPs emulating what the attackers may be capable of in the near future. However, there should be a clear distinction between the evidence-based backward-looking and the hypothetical forward-looking TTPs in the threat scenario description. A maximum of one of the final scenarios may be non-threat led, allowing for investigation and generation of learning regarding future or otherwise relevant attack vectors, including hybrid, novel TTPs and applying a forward-looking focus.

Within the final scenarios, a breadth of threat actors, motivations, modus operandi, TTPs, initial access vectors and targeted CIFs should be ensured with emphasis on societal criticality to ensure the generation of diverse and future-proof learning. The TIP should populate the relevant sections in the MITRE ATT&CK Template with the TTPs known and/or foreseen to be used by the selected threat actors as threat scenarios are finalised.

The result from the targeted threat intelligence process is a Targeted Threat Intelligence Report that should at least include the following three outputs:

- tailored threat scenarios which will support the formulation of a realistic and effective Red Team Test Plan
- threat actor goals and motivations which will help steer the RTT in their attempt to capture the flags agreed upon in the Scope Specification
- validated evidence which will underpin the business case for post-test remediation and improvement.

The CT, TIP and TCT should schedule regular TIP progress meetings to simultaneously ensure progress and alignment on the threat scenarios.

The RTT should also be kept informed during the production of the Targeted Threat Intelligence Report and provide feedback for the actionable intelligence and threat scenarios. In this context, the RTT can suggest the TIP to search for specific information that would help the RTT operationalise and execute each threat scenario. An example could be information that could be used directly for spear phishing campaigns.

The CT must review the Targeted Threat Intelligence Report in order for the report to live up to the requirements in the TIBER-EU Targeted Threat Intelligence Report Guidance. The actionable

[22] In case of a multi-party test involving an ICT third party provider, at least one of the selected scenarios should cover the ICT third party providers' systems, processes and technologies supporting the CIFs of the entities in scope.

data to be used by the RTT, e.g. the digital footprint of the entity, should be verified by the CT to ensure efficiency in the Testing Phase: Red Team Testing.

The CT should provide the Targeted Threat Intelligence Report to the TCT, which must approve the deliverable in order for it to be finalised. In the Targeted Threat Intelligence Report, the CT and TCT may opt to update or modify the flags based on the threat intelligence. In addition, the CT should provide the TCT with the populated MITRE ATT&CK Template delivered by the TIP.

When the final threat scenarios are in place, the CT should revisit the CT composition to ensure relevant expertise in light of the CIFs, roles, processes and technologies included in the threat scenarios.

## Targeted Threat Intelligence Report Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Virtual

Duration: 1.5 hours

Minutes of meeting: CT

Prerequisites:

- TIP develops Targeted Threat Intelligence Report

Agenda:

- Presentation of the Targeted Threat Intelligence Report incl. digital footprint, threat landscape and threat scenarios
- Alignment on Targeted Threat Intelligence Report
- Handover of MITRE ATT&CK Template

Outcomes:

- Presentation of the Targeted Threat Intelligence Report
- Alignment on contents of the Targeted Threat Intelligence Report, with focus on threat scenarios in full detail

At the Targeted Threat Intelligence Report Meeting, the TIP introduces the Targeted Threat Intelligence Report focusing on target intelligence, intelligence on the threat landscape faced by the entity and the detailed threat scenarios. All stakeholders will have been kept informed during the Testing Phase: Threat Intelligence and Scenarios and may provide feedback to the Targeted Threat Intelligence Report and detailed threat scenarios, including via identifying potential remaining aspects to be added or adapted. At this point, only minor adjustments to the detailed scenarios are expected. The Targeted Threat Intelligence Report as a whole, including the detailed scenarios, must be approved by the TCT. Following the Targeted Threat Intelligence Report Meeting, a final version of the Targeted Threat Intelligence Report including detailed threat scenarios is delivered and thereby ready for handover to the RTT, leading into the Testing Phase: Red Team Testing.

# Testing Phase: Red Team Testing

Following completion of the Testing Phase: Threat Intelligence and Scenarios, focus shifts to red team testing activities. During the Testing Phase: Red Team Testing, the RTT operationalise and schedule the deployment of the selected threat scenarios in a Red Team Test Plan. The RTT then execute the Active Testing of the target systems and services that underpin the selected CIFs in scope. The test objectives agreed during the Preparation Phase and possibly updated during the Testing Phase: Threat Intelligence and Scenarios are the flags that the RTT aim to capture during the Active Testing as they progress through the scenarios.

In the Testing Phase: Red Team Testing, the following documents are particularly relevant:

- Scope Specification
- Risk Management Documentation
- TIBER-DK Generic Threat Landscape Report
- Targeted Threat Intelligence Report
- TIBER-DK Guidance for Leg-Ups
- TIBER-EU Red Team Test Plan Guidance
- TIBER-DK MITRE ATT&CK Template
- TIBER-EU Red Team Test Report Guidance

## Red Team Test Plan

Responsible: RTT

Deliverables:
- Red Team Test Plan
- MITRE ATT&CK Template

Documents to consult:
- Scope Specification
- Risk Management Documentation
- Targeted Threat Intelligence Report
- TIBER-DK Guidance for Leg-Ups
- TIBER-EU Red Team Test Plan Guidance
- MITRE ATT&CK Template (pre-populated)

Process:
- The RTT create and deliver a Red Team Test Plan, including a populated MITRE ATT&CK Template.
- The TIP may provide feedback to the Red Team Test Plan.
- The CT and the TCT must approve the final Red Team Test Plan, including any subsequent changes.
- The TCT informs the CT of its approval of the Red Team Test Plan.

In the Red Team Test Plan, the RTT must outlay their operationalisation of and concrete planning for the deployment of the selected threat scenarios to be carried out during Active Testing. Communication channels and procedures to be followed during Active Testing should also be specified along with test status reporting procedures and frequency. The latter must incorporate Full Status (*link*) and Status Update (*link*) Meetings during Active Testing.

By assuming an attacker's point of view, the threat scenarios designed and agreed upon in the Targeted Threat Intelligence Report must be used as an evidential basis and justification for transformation into technically operational plans for achieving the concretely defined flags.

The RTT should indicate various creative options for the in, through and out stages based on various TTPs used by the advanced attackers to anticipate changing circumstances or as contingency planning in case the first option does not work. The scenario writing is a creative process. The TTPs do not simply mimic scenarios seen in the past but combine the techniques of the various relevant threat actors. Their specification in the Red Team Test Plan must also include the TTPs allowed and forbidden for use during Active Testing, including ethical boundaries for social engineering, and how the privacy of the involved parties is being safeguarded.

The RTT should align their flags with the goals of each of the actors, map these to the CIF supporting systems, roles and processes and produce credible real-life attack scenarios for the test. The attack scenarios are designed to provide background to the tradecraft employed by each threat actor to conduct a successful attack. This may also involve testing elements of a forward-looking nature to facilitate future-proof learning. The TIP may be consulted by the RTT to assess whether a specific creative approach is in line with the simulated attacker's expected behaviour to ensure a threat intelligence-led approach.

The RTT should adapt their attack methodology to replicate or leverage insights on real-life attack scenarios, and this information should be used in designing and justifying the proposed Red Team Test Plan and its operationalisation of attack scenarios. This must include descriptions for each attack scenario, specifying the simulated threat actor(s), their intent, motivation and goals, the target function(s) and supporting ICT system(s), the targeted confidentiality, integrity, availability and authenticity aspects and the flags aligned with the Targeted Threat Intelligence Report.

Simultaneously, a detailed description of each attack path, including prerequisites and possible leg-ups to be provided by the CT, including deadlines for their provision and potential usage must be specified in the Red Team Test Plan. The RTT are constrained by the time and resources available as well as by moral, ethical and legal boundaries. It is therefore expectable that the RTT may require occasional leg-ups from the CT to aid progress through a complete kill chain, spanning both in, through and out stages. Leg-ups contribute to ensuring that maximum learning is derived from a constraint and time-limited test. As the RTT describes and plans for potential leg-ups in the test plan, the leg-ups should be discussed in advance with the CT and the TCT for alignment and for the CT to commence preparations for these leg-ups as early as possible.

The Red Team Test Plan must also specify the concrete scheduling of red teaming activities, including time planning for the execution of each scenario. This should, at a minimum split according to the in, through and out stages the RTT take throughout the Active Testing, respectively entering the entity’s ICT systems, moving through the ICT systems and ultimately executing action(s) on objective(s) and extracting itself from the ICT systems. In addition, any particularities of the entity’s infrastructure to be considered during testing and, if any, additional information or other resources necessary to the RTT for executing the scenarios should be described. The order of executing the scenarios should be aligned with the risks of detection.

It is advised for the CT to arrange RTT progress meetings with the RTT, the TCT and optionally, the TIP during the Red Team Test Plan creation to ensure progress and alignment with the scope, the threat intelligence and the overall expectations of the attack scenarios and the attack plan. The CT should ensure the Red Team Test Planlives up to the requirements in the TIBER-EU Red Team Test Plan Guidance and that proposed actions are in accordance with risk appetite and scope. The CT, TCT, and optionally, the TIP, should therefore review and provide feedback to the Red Team Test Plan.

The output of this activity is the final Red Team Test Plan which must be formally approved by both the CT and TCT, including attack scenarios to be followed. In addition, the RTT should populate the relevant sections in the TIBER-DK MITRE ATT&CK Template prepared by the TIP with the TTPs planned to be used in each attack scenario. The CT should provide the TCT with the populated MITRE ATT&CK Template delivered by the RTT.

## Red Team Test Plan Meeting

Responsible: CT

Participants: CT, TCT, TIP, RTT

Type: Virtual

Duration: 1.5 hours

Minutes of meeting: CT

Prerequisites:
- RTT develop Red Team Test Plan, including populated MITRE ATT&CK Template

Agenda:
- Presentation of Red Team Test Plan, incl. overall time plan, planned attack steps, flags, leg-ups, risk management and MITRE ATT&CK Template
- Alignment on Red Team Test Plan

Outcomes:
- Presentation of the Red Team Test Plan, including key elements

At the Red Team Test Plan Meeting, the RTT should present the planned attack steps for each end-to-end scenario, including detailed flags and expected leg-ups. In addition, time planning for each scenario along with dedicated milestones and leg-ups should be described. The RTT should also describe escalation contacts and procedures and present rules of engagement and supporting agreements along with risk management measures taken by the RTT. The populated MITRE ATT&CK Template should also be presented by the RTT. All present stakeholders may provide additional feedback on and discuss the Red Team Test Plan, identifying any remaining aspects to be added or adapted.

## Active Testing

Responsible: RTT, CT

Participants: TCT, TIP

Deliverables:
- None

Documents to consult:
- Red Team Test Plan
- MITRE ATT&CK Template
- TIBER-DK Guidance for Leg-Ups
- TIBER-EU Red Team Test Plan Guidance
- TIBER-EU Red Team Test Report Guidance

Process:
- The CT ensures relevant leg-ups are prepared and ready for deployment as detailed in the Red Team Test Plan.
- The RTT perform Active Testing of target CIFs, systems and services, aiming to obtain the flags.
- The RTT regularly provide updates at Full Status (*link*) and Status Update (*link*) Meetings.
- The TIP provides relevant threat intelligence support during Active Testing, including via participation in Full Status Meetings (*link*).
- The CT maintains close communication with the RTT and TCT to ensure Active Testing is conducted in a safe and controlled manner.

Once the Red Team Test Plan is approved, Active Testing will commence, in all cases spanning a minimum duration of twelve weeks. This ensures a realistic and comprehensive test during which chosen attack stages are executed and the RTT aim to achieve all flags.

The RTT should deploy a diverse range of TTPs during the Active Testing to generate broad learning. In addition, the RTT should follow a rigorous and ethical red team testing methodology. Irrespective of the methodology used by the RTT, the test should be conducted in a controlled manner, taking a stage-by-stage approach. Risks to the entity and its CIFs, such as degradation of services, need to be kept to an absolute minimum and in accordance with the risk appetite of the entity.

During Active Testing, the RTT should perform a stealthy intelligence-led red team test of the target systems and services, seeking to obtain the flags. The attack scenarios are not a prescriptive playbook which must be followed with stringent precision during the test. If obstacles or opportunities occur, the RTT should show their creativity, as advanced attackers would, to develop alternative ways to reach the flag(s).

To facilitate this, the TIP should also be engaged at Full Status Meetings (*link*) conducted during the Active Testing. In real life, an attacker can leverage threat intelligence whilst actively attempting to compromise a target. Interaction between the TIP and the RTT during the test may add greater value for the entity and ensure any changes to the plan follow the modus operandi of the selected threat actors. The TIP can therefore provide ongoing threat intelligence to the RTT during Active Testing which may provide more useful reconnaissance and more insights into how to achieve the flags.

The CT must ensure relevant leg-ups are prepared and ready for deployment as detailed in the Red Team Test Plan. In addition to leg-ups foreseen during the creation of the Red Team Test Plan, it may occur that the RTT require ad hoc leg-ups from the CT to help them progress. In such cases, the leg-ups should be discussed, and approved via non-objection from the TCT. The RTT must log relevant actions as evidence for the Red Team Test Plan, providing a basis for learning for the BT.

For the CT, Active Testing can be intensive. The CT is expected to keep close communication with both the RTT and the TCT to ensure the TIBER-DK test is conducted in a safe and controlled manner. As input to the activities in the Closure Phase, it is beneficial for the CT to keep a log of the attack seen from their point of view, including their own actions. During Active Testing, the Risk Management Documentation (*link*) should be consulted as needed and any risk not already identified related to RTT activity should be assessed by the CT and discussed at Full Status (*link*) or Status Update (*link*) Meetings.

During Active Testing, the BT will defend the entity to the best of their ability whilst not being aware of the ongoing test. Their time and resources will likely be needed, for instance during response and escalations as a reaction to the activities of the RTT. The CT must ensure that arrangements are in place to be sufficiently informed of actions taken by the BT including escalations. The CT should consult the TCT prior to revealing test activities by involving any members of the BT at any point before to the Closure Phase. To this end, the CT should also ensure that viable cover stories are prepared in advance to preserve the confidentiality and integrity of the test in case of BT detections.

If members of staff at the entity or its ICT third-party service provider(s) detect testing activities, the CT must propose and submit measures to the TCT for validation, allowing the continuation of the TIBER-DK test whilst ensuring to uphold its secrecy.

Discovery of an actual compromise or any other exceptional circumstances triggering risks of impact on data, damage to assets, disruption to CIFs, services or operations can also occur during Active Testing. Under such exceptional circumstances, the CT may suspend the test as needed to thereby facilitate delays or employ other changes to continue the test and maximise the entity's learning. In such cases, the TCT should be consulted. In supplement, should any critical vulnerabilities be discovered during Active Testing, the CT may also in close consultation with the TCT initiate remediation actions building on technical feedback provided by the RTT whilst ensuring the least possible degree of impact upon testing activities along with confidentiality and integrity.

Though the TIBER methodology ensures thorough planning, unexpected circumstances may arise during a live test forcing the stakeholders to act pragmatically to balance the objective of maximising the learning outcome against a strict interpretation of the framework.

As a last resort and subject to prior validation by the TCT, if continuation of the test is not otherwise possible, testing activities can be continued as a limited Purple Teaming exercise during Active Testing. Insofar as possible, the limited Purple Teaming should be restricted within the relevant scenario to ensure the test is not impacted as a whole. Such exceptional circumstances may vary on a case-by-case basis. Decisions regarding limited Purple Teaming during Active Testing are preceded by a thorough consideration of several alternative ways forward. For example, one should duly estimate if postponing the remainder of the test would constitute the best option. It is then up to the TCT to evaluate each case individually in close dialogue with the CT and RTT to assess whether limited Purple Teaming is an option. The duration of the limited Purple Teaming will count towards the minimum length of Active Testing.

As detailed below, the CT and TCT should be continuously informed of progress to guide the RTT regarding which actions can and cannot be taken next. At relevant frequencies, i.e. at Full Status Meetings, the TIP should also be involved in these dialogues. In addition to this, contact between the CT, TCT and RTT should be established via secure platform(s), ensuring swift and confidential communication. If more frequent touchpoint meetings are held, for instance during critical stages of Active Testing, the TCT should be invited.

## Full Status Meeting

Responsible: RTT

Participants: CT, RTT, TCT, TIP

Type: Virtual and weekly

Duration: 1 hour

Minutes of meeting: RTT presentation

Prerequisites:
- RTT prepare status updates on actions, flags, timeline and upcoming Active Testing steps in an illustrated walkthrough, along with populated MITRE ATT&CK Spreadsheet
- CT prepares status on leg-ups

Agenda:
- Scenarios status: actions, flags, leg-ups, timeline
- Upcoming Active Testing steps
- MITRE ATT&CK Template
- Purple Teaming candidates and postponed activities

Outcomes:
- Ensure stakeholders are thoroughly informed of Active Testing status
- Alignment on upcoming Active Testing activities and associated risks

Full Status Meetings must be held on a weekly frequency throughout Active Testing. The meeting should provide a full status to ensure relevant stakeholders can be duly informed exclusively via participation at the weekly Full Status Meeting.

The first Full Status Meeting during Active Testing is dedicated to the formal kick-off of Active Testing. At the first Full Status Meeting, a key area of focus is ensuring that all relevant preparatory measures are in place for Active Testing, and particularly its initial stages, including that any leg-ups planned for usage are ready for deployment. In addition, expectations should be aligned regarding the initial steps to be taken during Active Testing, and risk management measures may also be reiterated and aligned upon.

At the remainder of Full Status Meetings, the RTT will walk through the current status for each scenario according to the agreed time plan. In addition, an illustrated walkthrough of actions conducted by the RTT since the latest Full Status Meeting and relevant updates in these regards should be presented, including status in relation to flags. In addition, alignment and advancement on planned and unplanned leg-ups should be ensured. The RTT will also present the plan for the upcoming week's activities, including if needed by facilitating the prioritisation of its targeting. This serves to ensure understanding of and alignment on associated risks.

The RTT will walk through the TTPs used since the latest Full Status Meeting, taking point of departure in the continuously populated MITRE ATT&CK Template.

Finally, candidates for purple teaming and postponed activities will be presented and aligned upon.

The TIP should participate in Full Status Meetings in order to facilitate the ongoing provision of threat intelligence to the RTT during the test, which may include updated insights, more useful reconnaissance and additional suggestions for how to achieve flags in a threat intelligence-based manner, building on the modus operandi of the selected threat actors.

## Status Update Meeting

Responsible: RTT

Participants: CT, RTT, TCT

Type: Virtual and 2-4 per week

Duration: 30 minutes

Minutes of meeting: RTT presentation

Prerequisites:
- Regular Active Testing advancements

Agenda:
- Scenarios status: actions, flags, leg-ups, timeline
- Upcoming Active Testing steps

Outcomes:
- Information on Active Testing advancements since last status

Status Update Meetings constitute a required supplement to Full Status Meetings and should be conducted on a frequency determined by the CT and TCT, varying from 2-4 Status Update Meetings per week.

At Status Update Meetings, the RTT will present a status for each ongoing scenario since the latest status. In addition, the upcoming Active Testing steps will be specified by the RTT to provide the opportunity for relevant discussions.

# Closure Phase

The Closure Phase allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity. Thereby, the Closure Phase plays a pivotal role in augmenting and consolidating the learning from the TIBER-DK test within the entity.

The key members of the entity's BT are informed of the test once Active Testing has ended, and the RTT and the BT respectively prepare Red and Blue Team Test Reports. In order to enable the BT to begin its reporting activities early, the CT and/or the RTT are encouraged to provide the BT with an initial overview of the Active Testing in the beginning of the Closure Phase. The CT is responsible for the production of a Test Summary Report and Remediation Plan. In addition, the CT is responsible for arranging both the Replay and Purple Teaming Exercises, and for generally communicating and anchoring the results and learning points within their organisation.

In the Closure Phase, the following documents are particularly relevant:

- TIBER-EU Red Team Test Report Guidance
- TIBER-EU Blue Team Test Report Guidance
- TIBER-EU Purple Teaming Guidance
- TIBER-EU Test Summary Report Guidance
- TIBER-EU Remediation Plan Guidance

## Red Team Test Report

Responsible: RTT

Deliverables:
- Red Team Test Report
- MITRE ATT&CK Template

Documents to consult:
- TIBER-EU Red Team Test Report Guidance
- MITRE ATT&CK Template (pre-populated)

Process:
- The RTT develop and deliver the Red Team Test Report, including the populated MITRE ATT&CK Template, to the CT.
- The CT delivers the Red Team Test Report, including the populated MITRE ATT&CK template, to the BT.
- The CT makes the Red Team Test Report available to the TCT for review onsite.
- The CT shares the populated MITRE ATT&CK Template with the TCT.
- The TCT assesses whether the Red Team Test Report contains the required information and notifies the CT thereof.

After the conclusion of Active Testing, the RTT will develop the Red Team Test Report, which will include details of the approach taken to the testing and the findings and observations from the test. The Red Team Test Report must at minimum include the following information on the performed attack:

- the targeted CIF(s) and identified ICT systems, processes and technologies supporting the CIF(s), as identified in the Red Team Test Plan
- a summary of each scenario
- flags reached and not reached

- attack paths followed successfully and unsuccessfully
- TTPs used successfully and unsuccessfully
- deviations from the Red Team Test Plan, if any
- leg-ups granted, if any.

In addition, the Red Team Test Report should specify all the actions the RTT are aware of that were performed by the BT. This serves to aid the BT in reconstructing the attack and mitigating its effects. Insofar as possible, the RTT should include timestamped logs regarding the concrete usage of the TTPs that constitute key elements of Active Testing along with relevant related details. This serves to facilitate the BT's learning and improve both the level of detail and degree of relevance of their response within the Blue Team Test Report.

Importantly, the Red Team Test Report should also include information on the discovered vulnerabilities and other findings, including a (a) description of the vulnerabilities and other findings, as well as their criticality, (b) a root cause analysis of successful attacks, and (c) recommendations for remediation and an indication of the remediation priority.

Along with the Red Team Test Report, the RTT should deliver the populated MITRE ATT&CK Template in a fully populated state to the CT, who will then ensure its delivery to the TCT.

The CT reviews the Red Team Test Report to ensure coverage of the requirements in the Red Team Test Report Guidance, and that the report documents the Active Testing and results sufficiently. The CT should not alter the RTT's conclusions if the CT does not agree with these, since the CT can comment on such matters in the Test Summary Report.

The TCT will review the final Red Team Test Report at the entity's premises to ensure the required contents are included. The TCT will notify the CT thereof. The TCT does not store the Red Team Test Report.

The CT should deliver the Red Team Test Report to the BT.

## Blue Team Test Report

Responsible: BT

Deliverables:
- Blue Team Test Report

Documents to consult:
- Red Team Test Report
- MITRE ATT&CK Template
- TIBER-EU Blue Team Test Report Guidance

Process:
- The BT develops and delivers the Blue Team Test Report to the CT.
- The CT delivers the Blue Team Test Report to the RTT.
- The CT makes the Blue Team Test Report available to the TCT.
- The TCT assesses whether the Blue Team Test Report contains the required information and notifies the CT thereof.

The BT will use the Red Team Test Report, including the fully populated MITRE ATT&CK Template, as input to the Blue Team Test Report. The BT can find relevant information and begin to develop the Blue Team Test Report as soon as Active Testing has concluded. In order for the BT to begin preparing the Blue Team Test Report before the Red Team Test Report has been finalised, the CT and/or the RTT are encouraged to provide the BT with an initial overview of the Active Testing in the beginning of the Closure Phase.

In the Blue Team Test Report, the BT maps their actions alongside the RTT actions. For each attack step described by the RTT in the Red Team Test Report, the Blue Team Test Report should include a list of detected attack actions, and log entries corresponding to those detections.

In addition, the Blue Team Test Report should include:

- an assessment of the findings and recommendations of the RTT
- evidence of the attack by the RTT collected by the BT
- a list of lessons learned and identified potential for improvement
- a list of topics to be addressed in the Purple Teaming exercise.

The Blue Team Test Report should be completed ahead of the Replay Exercise to maximise the learnings from the exercise.

The TCT will review the final Blue Team Test Report at the entity's premises to ensure the required contents are included. The TCT will notify the CT thereof. The TCT does not store the Blue Team Test Report.

## Replay Exercise

Responsible: CT

Participants, part I: CT, BT, TCT, TIP, RTT, executive management at entity

Participants, part II: CT, BT, RTT, TCT

Type: Physical

Duration: 1-2 days

Minutes of meeting: CT (only conclusions should be noted)

Prerequisites:

- CT plans contents of the Replay Exercise
- TIP prepares threat intelligence presentation
- RTT prepare Red Team Test Report presentation and scenario replays

Agenda:

*Part I*

- Presentation of TIBER-DK and Test Scope
- Presentations of Targeted Threat Intelligence and Red Team Test Reports incl. key findings and recommendations

*Part II*

- Scenario replays
- Alignment on Purple Teaming Exercise

Outcomes:

- Overview of the test, including key findings and recommendations (Part I)
- Step-by-step presentation of the test from the RTT and BT points of view (Part II)
- RTT recommendations for remediation
- Decision on elements to include in Purple Teaming Exercise

After the RTT and the BT have delivered their reports, a Replay Exercise is held. The objective of the Replay Exercise is for all participants to learn from the testing experience.

Prior to the Replay Exercise, the BT and RTT must agree on the timeline of events during Active Testing. This is necessary to facilitate a meaningful Replay Exercise and discussion about the actions taken by the BT and RTT during the test.

The Replay Exercise consists of Parts I and II. Part I functions as the introduction and executive summary. During Part I, the scene is set via overall introductions, including to TIBER-DK, the scope of the test, and the Targeted Threat Intelligence and Red Team Test Reports, including key findings and recommendations. Executive management, regardless of enrolment in the CT, should

participate in Part I, whereby an overarching understanding of the specific TIBER-DK test will be convened. In addition, the TIP should take active part in Part I in order to present relevant threat intelligence, including in regard to threat actors and threat scenarios. However, neither executive management nor the TIP are required to partake in Part II of the Replay Exercise, for which focus shifts to content of a more detailed and technical nature.

In Part II, focus is shifted to detailed technical explorations of test findings. During Part II of the Replay Exercise, scenario replays are organised in which the BT and the RTT review the steps taken by both parties during the test. When conducting the scenario replays, the RTT should state how they managed to progress through attack stages of each scenario along with the relevant learning generated. This may include discussions on the progression through attack stages of each scenario and the relevant learning generated, potential remediation measures, and explorational discussions and perspectives regarding what the RTT may have been able to achieve with more time and resources, given that genuine threat actors are not constrained by the time and resource limitations of a TIBER test. In addition, general questions from the BT may be discussed.

The meeting should conclude with alignment on the elements to include at the subsequent Purple Teaming Exercise.

The CT should note all conclusions drawn during the Replay Exercise, including if decisions are taken in regard to follow-up.

## Purple Teaming Exercise

Responsible: CT

Participants:
CT, BT, RTT, TCT

Type: Physical

Duration: 1-2 days

Minutes of meeting:
CT (only conclusions should be noted)

Prerequisites:
- CT consults TIBER-EU Purple Teaming Guidance
- RTT prepare Purple Teaming activities with the CT and the BT

Agenda:
- Presentation of activities to be covered
- Playthrough exploring identified vulnerabilities, missing detection capabilities, alternative scenarios, etc.
- Alignment on anticipated remediation measures and learning points

Outcomes:
- Training of BT capabilities and processes
- Input for Remediation Plan (*link*)

The Purple Teaming Exercise ensures that the BT and RTT continue to work closely together in discussing all remaining or additional topics and uncovering which other steps within systems or processes could have been taken by the RTT along with potential BT responses. Supplementarily, the Purple Teaming Exercise can cover:

- relevant issues that could not be tested during Active Testing
- particular vulnerabilities identified during the test
- alternative scenarios and their potential consequences
- proof of concepts
- discussion of anticipated remediation measures with the RTT

- business continuity exercises.

The Purple Teaming Exercise is an opportunity to explore challenges regarding protection, detection and response, evaluate the existing processes and system monitoring tools, and augment the BT's capabilities.

The CT should note all conclusions drawn during the Purple Teaming Exercise, including if decisions are taken in regard to follow-up.

## Test Summary Report

Responsible: CT

Deliverables:
- Test Summary Report

Documents to consult:
- TIBER-EU Test Summary Report Guidance
- Scope Specification
- Risk Management Documentation
- Targeted Threat Intelligence Report
- Red Team Test Report
- Blue Team Test Report
- TIBER-DK MITRE ATT&CK Template

Process:
- The CT delivers the Test Summary Report to the TCT.
- The TCT assesses and approves the Test Summary Report and notifies the CT thereof.
- The entity is obliged to submit the Test Summary Report to its competent authority in accordance with applicable regulation.

The Test Summary Report summarises the overall test process and results and should draw on the documents specified above. The Test Summary Report should not contain detailed technical information regarding findings and vulnerabilities, as information at that level of detail is highly sensitive and may cause great risk in the wrong hands.

The findings and learnings from both the Replay and Purple Teaming Exercises will also feed directly into the Test Summary Report, which must include at least:

- the parties involved
- the project plan
- the validated scope, including the rationale behind the inclusion or exclusion of CIFs and identified ICT systems, processes and technologies supporting the CIFs covered by the test
- selected scenarios and any significant deviation from the Targeted Threat Intelligence Report
- executed attack paths, and used TTPs
- captured and non-captured flags
- deviations from the Red Team Test Plan, if any
- BT detections, if any
- Purple Teaming during Active Testing, where conducted and the related conditions
- leg-ups used, if any
- risk management measures taken
- identified vulnerabilities and other findings, including their criticality
- root cause analysis of successful attacks
- high level plan for remediation, linking the vulnerabilities and other findings, their root causes and remediation priority
- lessons derived from feedback received.

The entity must share the Test Summary Report with the TCT for assessment and approval. The TCT will notify the CT of the approval.

Following the test, the entity is obliged to submit the Test Summary Report to its competent authority in accordance with applicable regulation.

## Remediation Plan

Responsible: CT

Deliverables:
- Remediation Plan

Documents to consult:
- TIBER-EU Remediation Plan Guidance
- Test Summary Report
- Targeted Threat Intelligence Report
- Red Team Test Report
- Blue Team Test Report

Process:
- The CT delivers the Remediation Plan to the TCT.
- The entity is obliged to submit the Remediation Plan to its competent authority in accordance with applicable regulation.

The entity should draft a Remediation Plan based on the test results, which should be used to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-DK test. The plan may incorporate input and recommendations from the TIP and the RTT. The findings and learnings from both the Replay and Purple Teaming Exercises will feed directly into the Test Summary Report. The elements to be included are:

- a description of the identified shortcomings
- a description of the proposed remediation measures and of their prioritisation and expected completion, including where relevant measure to improve the identification, protection, detection and response capabilities
- a root cause analysis
- the entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements
- the risks associated to not implementing the mentioned remediation measures, and, where relevant, risks associated to the implementation of these measures.

Following the test, the entity is obliged to submit the Remediation Plan to its competent authority in accordance with applicable regulation.

The TCT does not follow up on the Remediation Plan subsequent to the TIBER-DK test.

## 360˚ Feedback Report

Responsible: CT, TCT, TIP, RTT

Deliverables:
- 360˚ Feedback Report

Documents to consult:
- TIBER-DK 360˚ Feedback Report

Process:
- Feedback from all stakeholders must be delivered via the CT to the TCT.
- The TCT will provide the CT with a consolidated version before the 360˚ Feedback Meeting.
- The CT shares the consolidated 360˚ Feedback Report with the TIP and the RTT.

The specified parties should deliver feedback relating to the remainder of the listed stakeholders and the overall TIBER-DK process, including activities and deliverables. The goal is to further facilitate the learning experience of all those involved in the process for future TIBER-DK tests. For this purpose, the 360˚ Feedback Report is used to collect suggestions and feedback. The feedback from the TIP and the RTT should be delivered to the CT, who will share it with the TCT along with the CT's input. In turn, the TCT will provide the CT with a consolidated version before the 360˚ Feedback Meeting for the CT to share with the TIP and RTT.

## 360˚ Feedback Meeting

Responsible: TCT

Participants: CT, TCT, TIP, RTT

Type: Physical

Duration: 2.5 hours

Minutes of meeting: None

Prerequisites:
- CT, TIP, RTT and TCT provide input to 360˚ Feedback Report

Agenda:
- Feedback on key elements of the test to and from stakeholders: CT, TIP, RTT and TCT
- Input to the TIBER-DK Implementation and TIBER-EU Framework

Outcomes:
- Exchange of feedback from all Involved stakeholders

At the 360˚ Feedback Meeting, the CT, TIP, RTT and TCT should deliver feedback on each other and the overall TIBER-DK process, including activities and deliverables, based on the 360˚ Feedback Report.

The TCT may share the output from the 360˚ Feedback Report on an anonymous basis with the TIBER Knowledge Centre, so that all lessons learnt can be reflected on and improvements can be made to the TIBER-EU Framework.

## Signed Letter of Attestation

Responsible: CT

Deliverables:
- Signed Letter of Attestation for Test

Documents to consult:
- Letter of Attestation for Test

Process:
- The TCT provides the Letter of Attestation for Test to the CT.
- High-level management at the entity attest the receipt of the Letter of Attestation for Test.
- The entity is obliged to submit the Letter of Attestation for Test to its competent authority in accordance with applicable regulation.

At the end of the test, once all reports and the Remediation Plan have been approved, the TCT should provide a Letter of Attestation for Test to the CT confirming that the test was conducted in accordance with the requirements of TIBER and in accordance with the DORA TLPT regulation. Through the TCT's active participation in each phase of the test, the TCT can effectively assess the basis of attestation. Also, the CT progress meetings will provide information on test advancements to ensure that no issues will arise in the final attestation process.

The Letter of Attestation for Test should be signed by the TIBER authority and the receipt thereof should be attested by the high-level management at the entity. The signed receipt of the Letter of Attestation for Test should be provided to the TCT. The Letter of Attestation for Test will provide the grounds for mutual recognition of the test among authorities if mutual recognition is required.

The entity is obliged to submit Letter of Attestation for Test to its competent authority in accordance with applicable regulation.

## Final Meeting

Responsible: TCT

Participants: CT, TCT

Type: Physical

Duration: 1 hour

Minutes of meeting:
TCT

Agenda:
- Alignment on any remaining matters
- Document sharing infrastructure and archiving
- Arranging the sharing of learnings and results
- Timing of next TIBER-DK test

Outcomes:
- Closure of the TIBER-DK test process for the entity

At the end of the test process, a final meeting between the TCT and the CT is held to formally close the test and to align on timing for the entity's next TIBER test. Any remaining matters will be closed, and an agreement on when to close common document folders will be made. In addition, sharing learnings relevant on a broader scale to enhance cyber resilience amongst other members in the TIBER-DK Group will be encouraged (*link*).

The TCT will also arrange a physical experience sharing meeting at management level in conjunction with or shortly after the Final Meeting. Due to the confidentiality surrounding the TIBER tests, TCT cannot share experiences, results, learnings and value gained from the individual TIBER tests with the management of the Financial Stability department at DN. The meeting is arranged to give insight into

these subjects. At the experience sharing meeting at management level, the entity should present the test setup, the scenarios, the results and findings, learnings and the value gained from the test based on slides without sensitive details. The entity will assess what to share, and anything shared will be treated confidentially.

# Annex 1: TIBER-DK Background

In 2016, Danmarks Nationalbank (DN) established the Financial Sector forum for Operational Robustness (FSOR) to counter the fact that a large cyberattack against the financial sector could entail a systemic risk and potentially affect financial stability. Ahead of establishing FSOR, DN had first put operational risks and cyber risks on the agenda of the Systemic Risk Council in December 2015, and subsequently held a seminar with the CEOs and CISOs from the financial sector to secure the support of high-level management in the financial entities.

FSOR is a forum for collaboration between authorities, critical service providers and key financial sector entities and can be described as a public/private partnership forum. DN chairs FSOR and acts as the secretariat for the forum. FSOR meets twice a year, and between the meetings different working groups continuously work on different FSOR issues. Participation in FSOR is voluntary, but the entities in FSOR have agreed that participation is binding in the sense that members are committed to taking the necessary steps to work seriously with the issues and allocating sufficient resources to the work.

Based on DN's dialogue with the Bank of England and De Nederlandsche Bank on their experiences with the CBEST programme and TIBER-NL, DN, at an FSOR meeting in February 2017, proposed to establish a Danish threat intelligence-led test programme.

The focus of the programme should be on maximising the entity's learning from the red team testing experience. FSOR agreed in principle that a Danish threat intelligence-led red team test programme should be established, and the secretariat therefore continued its efforts to establish the programme. In early 2018, all the entities included in the programme agreed to establish a Danish threat intelligence-led red team test programme for the financial sector.

Meanwhile, the European Central Bank (ECB), started its work on establishing the TIBER-EU Framework, issued in May 2018, in which DN also participated. Consequently, it was decided that the Danish intelligence-led red team test programme should be based on TIBER-EU. The process of establishing TIBER-DK was thereby started and resulted in the publication of the TIBER-DK Implementation in December 2018. The TIBER-DK tests started in January 2019.

# Annex 2: TIBER-DK Group

The TIBER-DK Group is established to enable the entities to share knowledge and experiences and to contribute to the continued development of TIBER-DK. The tasks of the TIBER-DK Group are to:

- Act as a trusted and confidential forum for discussions and knowledge sharing between the TIBER-DK participants.
- Contribute to the development and optimisation of the programme by providing input aimed at optimising the TIBER-DK Implementation and the TIBER-EU Framework.

The TIBER-DK Group consist of members from each of the entities participating in TIBER-DK. The members should preferably include the entity's respective CTL as well as core CT members. This composition should support open dialogue within the TIBER-DK Group.

The TCT will chair the TIBER-DK Group meetings. In addition, the TCT will act as secretariat of the TIBER-DK Group and will facilitate the meetings, including the preparation of meeting material. The TCT will also be responsible for maintaining participation lists.

The TIBER-DK Group will normally meet two to four times a year. Most meetings will take place virtually and in addition, the TCT will normally host one physical meeting in December at Danmarks Nationalbank. To ensure confidentiality, it is recommended that the number of participating members is kept to only core CT members. Typically, meetings will take point of departure in the generic agenda below:

1. Updates from the TCT
2. Knowledge sharing
3. Input for optimising the frameworks, guidelines, templates etc.

Discussions will be considered confidential. The entities are encouraged to share relevant insights from their experiences with TIBER-DK in the form of presentations at TIBER-DK Group meetings.

The TCT analyses anonymous insights gathered from the TIBER-DK tests, including from Red Team Test Reports reviewed onsite. The across test analyses, including aggregated and anonymised results, and recommendations from TIBER-DK can be shared in the TIBER-DK Group, the Financial Sector forum for Operational Resilience (FSOR) and TIBER Knowledge Centre (TKC) under the TLP protocol as "TLP: AMBER+STRICT", without any formalised process of approval. The purpose of this is to simultaneously support the learning of individual entities along with the collective effort to strengthen cyber resilience across the financial sector in Denmark and Europe.

# Annex 3: Entities under DORA TLPT

As the TLPT authority in Denmark Danmarks Nationalbank (DN) is entrusted with all competences, tasks, and responsibilities connected with DORA TLPT. This includes the identification of entities required to perform TIBER-DK tests under DORA TLPT.

It follows from the Executive Order, Bekendtgørelse om henlæggelse af beføjelser til Danmarks Nationalbank, article 2, that DN designates financial entities required to perform TLPT in accordance with article 26(8) in DORA Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sectors and the RTS TLPT. According to the regulation, DN should identify entities based on an assessment of the following:

(a) impact-related factors, in particular the extent to which disruption of the services provided and activities undertaken by the financial entity would impact the financial sector;

(b) possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;

(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

It follows from article 26(11)(a) of DORA that the criteria used for application of this assessment must be specified in the RTS TLPT. Therefore, the RTS TLPT includes quantitative criteria for specific types of entities aiming to further apply the proportionality principle and identify entities of systemic importance relevant for TLPT. This includes credit institutions (SIFIs), payment institutions, electronic money institutions, CSDs, CCPs, trading venues, and insurance and reinsurance undertakings, who are subject to fulfilling certain criteria or quantitative thresholds.

Through qualitative criteria, DN has also been given the possibility to exclude an entity where an assessment concludes that the impact of the entity, financial stability concerns relating to it or its ICT risk profile does not justify the performance of the TLPT. Additionally, DN has been given the possibility to include an entity taking into account its impact, systemic character and ICT risk profile.

In addition, it also follows from the Danish Executive Order, Bekendtgørelse om henlæggelse af beføjelser til Danmarks Nationalbank, article 2, and the Danish regulation, Lov om finansiel virksomhed, article 333(g)(3), that DN designates operators of financial digital infrastructure designated by the Danish Financial Supervisory Authority, to perform TLPT.

When planning how to conduct the TLPT, the group structure and the setup of ICT systems at group level will be included in the assessment of whether the TLPT should be conducted on an individual basis or at group level.