18 April 2020

DANMARKS
NATIONALBANK

TIBER-DK General Implementation Guide

DANMARKS
NATIONALBANK

DANMARKS
NATIONALBANK

TIBER-DK General Implementation Guide

Contents

Introduction

Background
In 2016, Danmarks Nationalbank established the Financial Sector forum for Operational Robustness, FSOR, in order 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, Danmarks Nationalbank 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 institutions.

FSOR is a forum for collaboration between authorities and key financial sector participants and can be described as a public/private partnership forum. The participants in FSOR are a combination of the largest banks and mortgage banks in Denmark and also include data centres, payment and securities systems, relevant industry associations and authorities. Danmarks Nationalbank 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 participants 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 Danmarks Nationalbank's dialogue with the Bank of England and De Nederlandsche Bank on their experiences with the CBEST programme and the TIBER-NL[1], Danmarks Nationalbank, 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 tested institution'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 participants 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 TIBER-EU – issued in May 2018 – in which Danmarks Nationalbank also participated. As a consequence, it was decided that the framework for the Danish red team test programme should be based on TIBER-EU. Then the process of establishing TIBER-DK was started and resulted in the TIBER-DK framework version 1.0 in December 2018.

In TIBER-EU, it is stated that "if a jurisdiction decides to adopt the TIBER-EU framework, its national implementation must be formally adopted by the board of an authority, ideally the central bank of the European System of Central Banks (ESCB)". The Board of Governors at Danmarks Nationalbank has adopted TIBER-EU and, with it, the national implementation of TIBER-DK.

The TIBER-DK tests started in January 2019 and based on the experiences and learnings from these first TIBER-DK tests, the TIBER-DK framework has now been updated to version 2.0.

What is TIBER-EU?
TIBER-EU is a common European framework developed by the ECB which delivers a controlled, bespoke, threat intelligence-led red team test of entities' critical live production systems. Threat intelligence-led red team tests mimic the tactics, techniques and procedures of

[1] TIBER stands for Threat Intelligence-Based Ethical Red teaming.

real-life threat actors who, on the basis of 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 institution's critical functions and underlying systems, i.e. people, processes and technologies. It helps an entity to assess its protection, detection and response capabilities.

TIBER-EU therefore has the following core objectives:

- enhance the cyber resilience of entities and of the financial sector more generally;
- standardise and harmonise the way entities perform threat intelligence-led red team tests across the EU, while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities;
- provide guidance to authorities on how they might establish, implement and manage this form of testing at a national or European level;
- support cross-border, cross-jurisdictional threat intelligence-led red team testing for multinational entities;
- enable supervisory and/or oversight equivalence discussions where authorities seek to rely on each other's assessments carried out using TIBER-EU, thereby reducing the regulatory burden on entities and fostering mutual recognition of tests across the EU;
- create the protocol for cross-authority/cross-border collaboration, result sharing and analysis.

Principles of TIBER-DK

There are six principles of TIBER-DK that all support the core objective of TIBER-EU to enhance the cyber resilience of entities and of the financial sector more generally. The principles will also help the test participants to obtain a successful test:

- Learn and evolve (common TIBER-EU principle):
  Being resilient to advanced cyber threats requires practice. TIBER-DK trains institutions' protect, detect and respond capabilities, identifies weaknesses and raises awareness at all organisational levels.
- Be responsible:
  Testing the cyber resilience of some of society's most critical functions in live production systems entails a great responsibility and requires very careful planning and risk management as well as competent and controlled execution by all parties involved. Also, strong ethical behaviour is paramount.
- 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 C-level management. This shift entails a more 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 big and think holistically:
  TIBER-DK targets the core functions that are critical to both the business and to society, and the scenarios played out could have a systemic impact on financial stability. TIBER-DK tests are not only technical – both people, processes and systems are in scope.
- Share experiences:
  By creating a trusted community where TIBER-DK participants learn from each other, each test contributes to making the financial sector more cyber resilient.

The purpose of this guide

It is stated in TIBER-EU that "the authority that owns the TIBER-XX framework within its jurisdiction must publish on its website the official TIBER-XX Implementation Guide applicable to its jurisdiction and take measures to explain the adoption of the framework to the relevant market participants".

This guide, the TIBER-DK General Implementation Guide, is developed and published by Danmarks Nationalbank to describe how the requirements in TIBER-EU are adopted and implemented in a Danish context. The guide begins with an explanation of Danmarks Nationalbank's role and responsibilities in TIBER-DK, followed by a description of each of the other direct stakeholders in a TIBER-DK test. Finally, the general guide gives a high-level introduction to the TIBER-DK test process, including a short section on how the stakeholders are expected to interact during the test.

The TIBER-DK General Implementation Guide is supplemented by other guiding documents, and collectively they represent the TIBER-DK framework. The TIBER-DK Operational Guide provides a step-by-step description of each of the elements in 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 a number of documents common to all the jurisdictions that have adopted TIBER-EU. An overview of the TIBER documents can be found in the TIBER-DK Test Process Overview.

Enquiries about TIBER-DK or requests for some of the documentation should be directed to:
TIBER-DK@nationalbanken.dk

Danmarks Nationalbank's role and responsibilities in TIBER-DK

The TIBER-DK programme is implemented by Danmarks Nationalbank for the key players in the Danish financial sector. The aim of TIBER-DK is to strengthen the sector cyber resilience and thus contribute to the stability of the Danish financial system. The TIBER-DK programme is voluntary, but once a critical financial institution has agreed to participate in TIBER-DK, then this agreement is considered binding.

Danmarks Nationalbank is the lead authority of TIBER-DK, and the ownership of the programme is formally placed with Danmarks Nationalbank at board level. No other national authorities in Denmark are involved in the management of the programme.

Legal and compliance
As part of the implementation of TIBER-EU in Denmark, Danmarks Nationalbank has conducted a review of existing laws and regulations at a national and European level and concluded that the requirements, methodologies and processes contained in the TIBER-DK framework do not contravene any national or European laws or regulations, and that the implementation of the framework is legally compliant. Danmarks Nationalbank will revisit this opinion continuously in order to ensure legal compliance throughout the lifetime of the TIBER-DK programme.

In regard to the red team tests, it is important to emphasise that it is the responsibility of the tested institutions and the third-party providers to ensure that they conduct the test within the remit of all laws and regulations, and that appropriate risk management controls are in place to enforce this. Thus, the tested institutions are required to carry out their own legal reviews ahead of conducting their red team tests and cannot rely on the legal review of the TIBER-DK framework.

TIBER-DK Cyber Team
Danmarks Nationalbank is responsible for setting up an appropriate governance structure of TIBER-DK. This includes establishing a centralised TIBER-DK Cyber Team, TCT, at Danmarks Nationalbank. The role of the TCT is to manage, operationalise and monitor the TIBER-DK programme and each of the TIBER-DK tests carried out in the programme. Most importantly, the TCT will act as an operational control to ensure uniform, high-quality tests containing all the mandatory elements defined in the TIBER-DK framework. In addition, the TCT is responsible for continuously updating the TIBER-DK framework in light of lessons learnt from its implementation and the tests carried out. This will be done on a continuous basis in collaboration with the institutions participating in TIBER-DK, but also with authorities in other jurisdictions that have adopted TIBER-EU, including the ECB. The TCT at Danmarks Nationalbank participates in the knowledge sharing forum for TIBER authorities, TIBER Knowledge Centre (TKC). The TCT also facilitates two Danish sector groups for the purpose of sharing knowledge, experiences and learnings. These are the TIBER-DK GROUP (where all TIBER-DK participants are represented by their foreseen White Team lead) and the TIBER-DK SUBGROUP (for a smaller number of ongoing TIBER-DK tests).

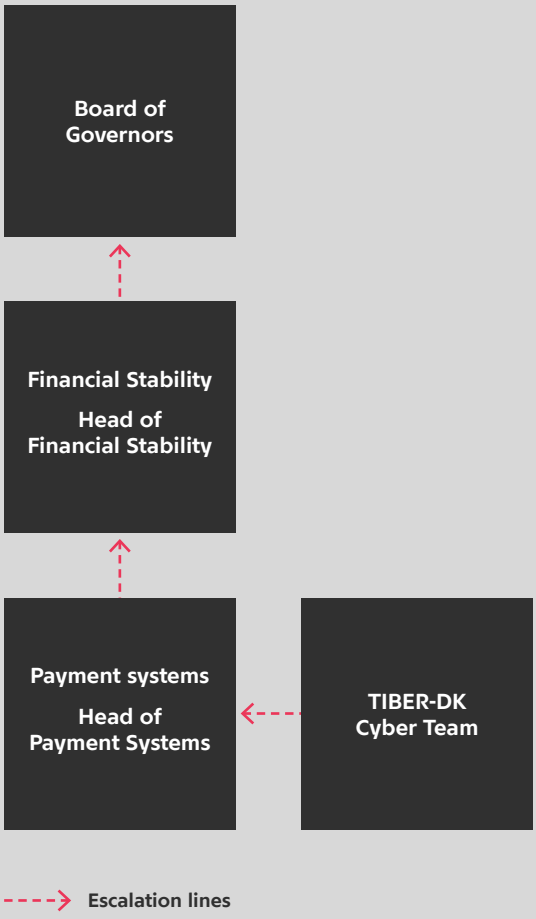
At Danmarks Nationalbank, the TCT is organisationally placed in the Payment Systems section under the Financial Stability department. The formal ownership of TIBER-DK rests with Danmarks Nationalbank's Board of Governors. The organisation described here is also the formal chain of command used during the test in cases where escalation is deemed necessary. Throughout the lifetime of the TIBER-DK programme, Danmarks Nationalbank will

make sure that the TCT consists of an adequate number of staff members with the necessary skills, e.g. in the areas of project management, cyber security and specialised knowledge of the Danish financial infrastructure.

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

Chart 1

TIBER-DK organisation at Danmarks Nationalbank



Cooperation with other authorities

TIBER-DK is not a regulatory requirement. Danmarks Nationalbank decided to be the lead authority of TIBER-DK because the programme supports one of Danmarks Nationalbank's core objectives: to enhance the financial stability of the Danish financial system. It is in the capacity of lead authority of TIBER-DK that the TCT will oversee each TIBER-DK test to ensure that the test meets the requirements in the TIBER framework and thus can be recognised as a TIBER test. This requires that the TCT is able to review and approve all the relevant material prepared in the test process. The TCT will not share information with any other authority about a TIBER test without having specific consent from the tested institution. Furthermore, the tested institution is the legal owner of all the material produced during the test and is responsible for sharing the material with its competent authorities, if required.

When testing cross-border institutions participating in TIBER-DK, the TCT can – upon request – enter into cooperation with authorities in other jurisdictions, cf. below, but such cooperation will require specific consent from the tested institution and must be entered into in accordance with the conditions described in this section.

Cross-jurisdictional cooperation

The harmonised and standardised approach in TIBER-EU enables cross-border, cross-jurisdictional threat intelligence-led red team testing for multinational institutions. It is therefore the responsibility of the TCT to liaise with authorities in other jurisdictions that potentially are relevant for the test of such a multinational institution. Before each test, the TCT will identify such authorities and reach out to the relevant ones with the aim of either 1) establishing cross-jurisdictional collaboration for a test of the institution, or 2) thoroughly explaining and documenting the procedures in

the TIBER-DK test process to promote cross-jurisdictional recognition of the test results.

Generic threat intelligence
In the TIBER-EU framework, it is recommended that national jurisdictions should produce a national generic threat landscape report for the financial sector to complement the more specific targeted threat intelligence reports that each of the institutions participating in TIBER-DK will produce. In TIBER-DK, it has been chosen to follow this recommendation, since experiences from other countries have shown that it is effective to gather the generic intelligence in one consolidated report, in relation to both reducing costs and promoting knowledge sharing in the programmes. The TCT has the overall responsibility for ensuring that such a report is available to the test participants and also to ensure that the Centre for Cyber Security (link) and also the Nordic Financial CERT (link) are involved in the process for validation, feedback and further enrichment of the report. The report will be updated regularly to ensure that the content is up to date.

Stakeholders in the TIBER-DK test process

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

- Danmarks Nationalbank, in particular the TCT, cf. above
- A critical financial institution in the Danish financial sector
- Third-party providers of threat intelligence and red team testing.

Critical financial institution

The participants in the TIBER-DK programme are critical financial institutions. Each institution is responsible for its own management and organisation of the test, including hiring the external third-party providers, and for implementing appropriate controls, processes and procedures to ensure that the test lives up to best practices and that risks are mitigated properly.

For each TIBER-DK test, the tested institution must establish a White Team, with a dedicated White Team lead from the institution. The White Team lead coordinates all test activity, including engagement with the Threat Intelligence provider and the Red Team provider. *More details on the roles, responsibilities and ideal composition of the White Team can be found in the TIBER-EU White Team Guidance (link)*. All staff members who are not part of the White Team are – in the context of a TIBER-DK test – referred to as the Blue Team. It is critical that all the members of the Blue Team are excluded from the information, the preparation and the conduct of the TIBER-DK test. In the Closure phase – when the test has been executed – the Blue Team is informed about the test, and the relevant and most appropriate members of the Blue Team should participate in the replay and follow-up.

Prior to the execution of the test, the tested institution's board/executive management must agree and attest to the scope of the test, as a means of qualifying the test for mutual recognition among other relevant authorities. When the test process is completed, the board/executive management must also sign an attestation confirming that the test was conducted in accordance with the requirements of the TIBER-DK framework. These attestations must be shared with the TCT.

Third-party providers

In TIBER-EU, it is pointed out that a test will only be recognised if it is conducted by an independent third-party provider. This requirement also applies to TIBER-DK. Several entities already conduct red team testing with dedicated internal red teams, and although the practice of internal red teams is encouraged, there are clear advantages in procuring an external party to conduct a test. For example, an external tester provides a fresh and independent perspective, which may not always be feasible with internal teams that have grown accustomed to the internal systems, people and processes. Furthermore, external providers might have more resources and up-to-date skills to deploy, which would add value to the entity.

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

- The Threat Intelligence provider should provide threat intelligence and develop threat scenarios for the tested institution in the form of a targeted threat intelligence report. These providers should use multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible.
- The Red Team provider plans and executes a TIBER-DK test of the target systems and services which are agreed in the scope of the test. This is followed by a review of the

test and the issues arising, culminating in a red team test report drafted by the provider.

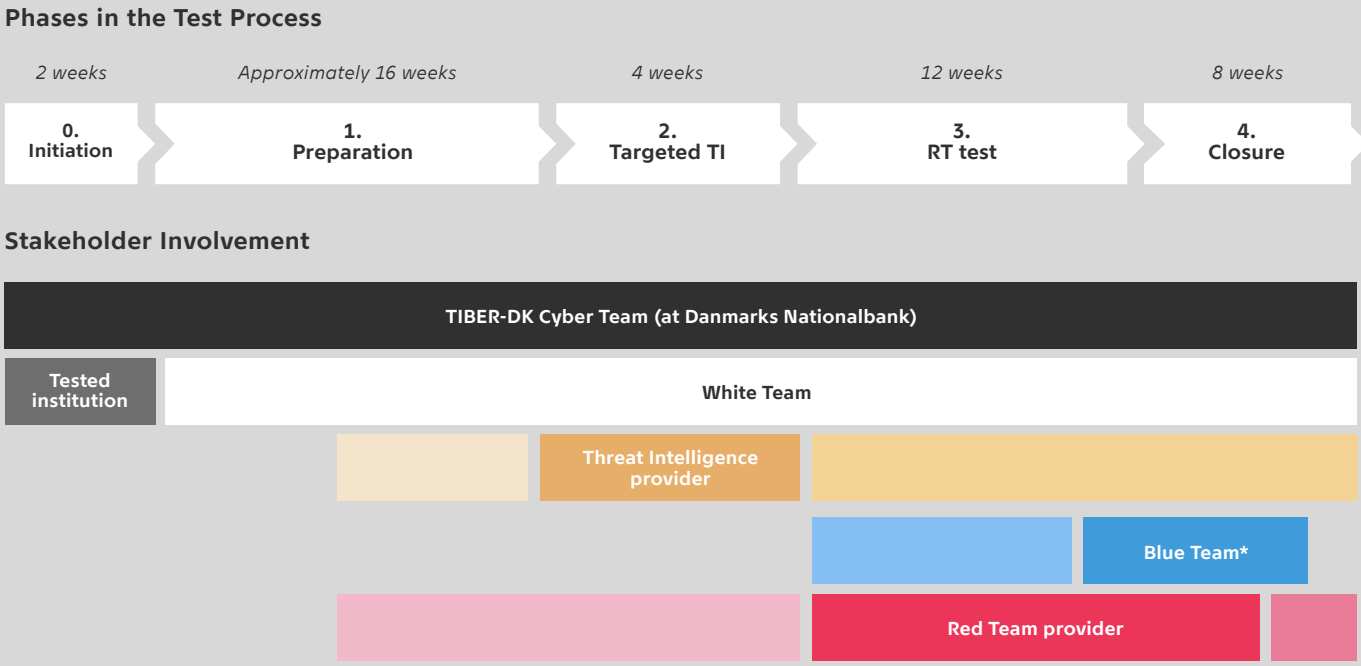
When hiring Threat Intelligence and Red Team providers, the responsible institution should make sure that there is a mutual agreement on at least the following aspects: the scope of the test; boundaries; timing and availability of the providers; contracts; actions to be taken; and liability (including insurance where applicable). The contracts with the providers should include:

- that the providers must meet security and confidentiality requirements that are at least as stringent as those followed by the underlying entity for confidentiality requirements;
- protection of those involved (e.g. indemnifications);
- a clause related to data destruction requirements and breach notification provisions;
- a determination of activities not allowed during the test, such as: destruction of equipment; uncontrolled modification of data/programs; jeopardising the continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results.

A key means of managing the risks associated with the TIBER-DK test is to use the most competent, qualified and skilled Threat Intelligence and Red Team providers with the requisite experience to conduct such tests. *Consequently, prior to engagement the tested institution must ensure that the providers meet the minimum requirements, which are set out in the TIBER-EU Services Procurement Guidelines (link).*

Chart 2

TIBER-DK test process, high-level overview



* The Blue Team at the financial institution is only allowed to know about the test in the Closure phase.

High-level overview of the TIBER-DK test process

This section gives a high-level description of the TIBER-DK test process, and more detailed overviews can be found in the TIBER-DK Test Process Overview. A step-by-step guide to each of the elements in the TIBER-DK test process can be found in the TIBER-DK Operational Guide.[2]

Generic Threat Landscape Report

The TCT will ensure that the Generic Threat Landscape Report is produced and shared with all the institutions in TIBER-DK in advance of the test. The report will contain information on the geopolitical and criminal threats to the key institutions in the Danish financial sector. This entails a description of relevant high-level threat groups, including their motives/modus operandi and the tactics, techniques and procedures they use to attack. Furthermore, a description of which types of financial institutions the threat actors are targeting (wholesale/retail banking, clearing/settlement, asset management, payment services, etc.) will be included. The purpose of the report is to provide a basis for the targeted threat intelligence produced in a later phase of the test process.

0. Initiation phase

Once an institution has agreed to participate in the TIBER-DK programme, the TCT will make all the relevant documents in TIBER-DK available. In the Initiation phase, the TCT will provide a suggestion for dates in a draft TIBER-DK Test Process Overview, including a preliminary date for the launch of the test process. Hereafter, the institution will begin its preplanning of the test, which includes conducting an initial stakeholder

[2] The TIBER-DK Operational Guide and the TIBER-DK Test Process Overview are available to TIBER-DK participants and relevant third-party providers on request.

analysis where it is considered which stakeholders – besides the TCT and the third-party providers – need to be involved in the test, e.g. critical service providers, data centres or similar. As part of the Initiation phase, the institution should also begin establishing its internal organisation of the TIBER-DK test. This includes establishing the White Team, including the appointment of a White Team. The preplanning could also include a pre-look at the market for possible third-party providers and/or legal issues which need to be analysed in advance of the test. Finally, the institution should consider its critical functions and the systems that support it at an early stage and thereby take the initial steps towards the creation of a test scope.

1. Preparation phase

The kick-off of the Preparation phase is a pre-launch meeting between the TCT and the White Team, which is to be held at least three months prior to the agreed launch date to allow for enough time for the procurement process. At the meeting, the TCT will ensure that the White Team is well-acquainted with the requirements of TIBER-DK, and the TCT and the White Team will agree on the dates in the TIBER-DK Test Process Overview. Regular status meetings during the Preparation phase are also set up by the TCT. Furthermore, the TCT will ensure that the White Team has set preparation initiatives in motion. These preparation initiatives entail: the overall project planning based on the agreed dates, a process for procurement of the third-party Threat Intelligence and Red Team providers, risk management and setting the scope of the test. The scope of the TIBER-DK test should at a minimum include the financial institution's critical functions defined as:

"the people, processes and technologies required by the tested institution to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the institution's safety and soundness, the institution's customer base or the institution's market conduct."

The White Team and the TCT should agree on the scope and ensure that the test is executed according to plan and that it conforms to the TIBER-DK test standards and all relevant requirements which are important for possible recognition by other jurisdictions.

During the Preparation phase, three meetings are held between the TCT, the White Team, the Threat Intelligence provider and the Red Team provider. These meetings are: 1) a Launch meeting, where the White Team, the TCT, the Threat Intelligence provider and the Red Team provider introduce the teams and their methodology, and all stakeholders discuss the test process and their expectations as well as the project plan; and 2) a Scope meeting, where the proposed scope of the test is discussed and finalised, i.e. a common agreement on how the "flags" – i.e. the targets and objectives of the test – are set in the scope; and 3) a Risk management meeting where the White Team presents the risk management controls, processes and procedures implemented to manage the risks of the TIBER-DK test.

1.a Risk management

Since the TIBER-DK test harbours elements of risk for all parties, it is of the utmost importance that the White Team has implemented appropriate controls, processes and procedures to ensure that the test is carried out with sufficient assurances for all stakeholders in order for risks to be identified, analysed and mitigated according to the institution's practices regarding risk management. In the Preparation phase, a risk assessment must therefore be conducted prior to the test to ensure that the right risk management precautions are taken in line with the institution's existing risk management framework. It is the responsibility of the White Team to ensure that the identified precautions

are taken during the entirety of the TIBER-DK testing process.

2. Targeted threat intelligence
The TIBER-DK process is designed to create realistic threat scenarios describing attacks against a critical institution's critical functions. Real-world threat actors may have months to prepare an attack and therefore, to make intelligence gathering as efficient as possible given the time and resource constraints, the tested institution will provide information in advance to the Threat Intelligence provider, including a business and a technical overview of each critical function-supporting system in the scope and current threat assessment and/or threat register and examples of recent attacks.

The Generic Threat Landscape Report is also shared with the Threat Intelligence provider. The report is used to define the specific threat actors targeting the different types of entities, it complements the production of the targeted threat intelligence and it provides the basis for later scenario development.

Subsequently, the Threat Intelligence provider collects, analyses and disseminates intelligence from other sources (e.g. open source (OSINT) and human intelligence (HUMINT)) about relevant threat actors and probable threat scenarios for the specific institution. All the collected information is used by the Threat Intelligence provider to produce a targeted threat intelligence report. Threat scenarios are developed in close cooperation between the institution, the Threat Intelligence provider, the TCT and possibly also the Red Team provider. The final scenarios are reviewed, commented and agreed upon by the TCT.

2.a Threat Intelligence provider
The Threat Intelligence provider must demonstrate willingness and the ability to share its deliverables (once approved by the entity) with its Red Team counterpart for review and comment and demonstrate willingness to work with the Red Team provider during the remainder of the TIBER-DK test. This includes helping to develop the attack scenarios for the red team test and ensure that they are threat intelligence-led, also during the actual execution, as well as providing information on any new intelligence requirements that occur as the red team test progresses. The Threat Intelligence provider is expected to provide input into the final red team test report issued to the entity.

3. Red team test
Initially in the Red Team test phase, the Threat Intelligence provider hands over a detailed explanation of the targeted threat intelligence report to the Red Team provider with the proposed threat scenarios for the testing. The Red Team provider then develops the attack scenarios written from the attacker's point of view. The attack scenarios should be threat intelligence-led and define the concrete targets to be reached, i.e. the flags to be captured from the scope.

When the institution and the Red Team provider have agreed on the attack scenarios, the Red Team provider will execute a threat intelligence-led red team test of specified critical live production systems, people and processes that underpin the institution's critical functions. The Red Team provider should deploy a range of techniques, tactics and procedures during the test and should follow a rigorous and ethical red team testing methodology. Irrespective of the methodology, the test should be conducted in a controlled manner, taking a stage-by-stage approach and in a way which does not bring risks to the institution and its critical functions, or any other party dependent on services provided by the functions. In case a real attack is detected during the TIBER test, the TIBER test can immediately be put on hold.

In general, the time allocated to testing should be proportionate to the scope, although, based on experience, it is envisaged that 10-12 weeks would be a reasonable amount of time for the Red Team testing phase. The time allocated to the test execution should be used as effectively as possible, with the main focus being on maximising the tested institution's learning from the testing experience in collaboration with the Red Team provider.

3.a Red team test provider

The Red Team provider must demonstrate willingness to work closely with the Threat Intelligence provider, which includes reviewing and commenting on the intelligence deliverables as well as transforming the threat scenarios into a cohesive and tractable red team test plan. Furthermore, the Red Team provider is expected to liaise and work with the Threat Intelligence provider throughout the execution of the test in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. Lastly, the Red Team provider is expected to collect input from the Threat Intelligence provider for the final red team test report.

The TIBER-EU framework requires Red Team providers to meet specific requirements, also to ensure that the test can be recognised by the relevant authorities. The core requirements are defined in the TIBER-EU Services Procurement Guidelines and are set to ensure that only the highest-quality providers, with sufficient experience and capability, can contribute to red team tests on the most critical functions of entities.

4. Closure phase

During this phase, the Red Team provider drafts a red team test report, which will include details of the approach taken to the testing and the findings and observations from the test. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The Blue Team will now be aware of the test. The Blue Team should draft a blue team report and will be involved in a replay of the executed scenarios and in the discussion of the issues uncovered during the test. The tested institution will take note of the findings and finalise a remediation plan. A test summary report describing the overall test process and results (including the remediation plan) will be shared with the TCT. Also, a 360^{O} feedback meeting will be held with all stakeholders.

Interactions during a TIBER-DK test

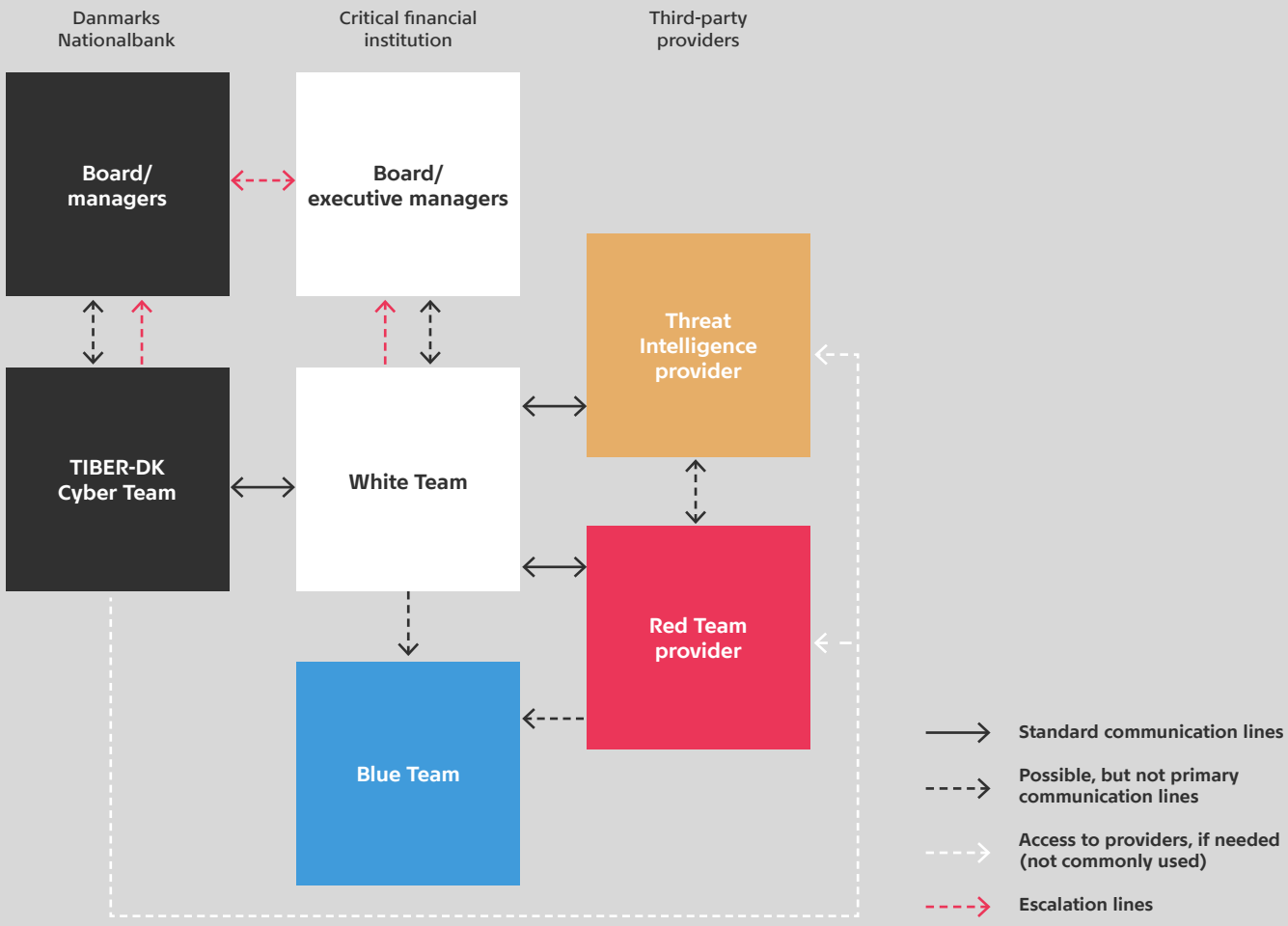
While the above describes the different phases in a test process and also points out the roles of the stakeholders in the phases, this section gives more general information on the interactions during a test addressing several or all phases.

All parties involved in a TIBER-DK test should take a collaborative, transparent and flexible approach to the work. A prerequisite for a successful test is close cooperation between the White Team lead and the TCT during all phases of the test.

Responsibility for the overall planning and management of the test lies with the tested institution. The White Team lead is responsible for determining and finalising the scope, scenarios and risk management controls for the test, ensuring that they have been approved and validated by the TCT. The scope should also be attested by the institution's board/executive management. In addition, the White Team lead should coordinate all test activity, including engagement with the third-party providers. The White Team lead should ensure that the providers' project plans are factored into the institution's overall project planning for the TIBER-DK test. In the Closure phase, the White Team lead is responsible for involving relevant members of the Blue Team in the test replay and follow-up. All parties must

Chart 3

TIBER-DK test process interaction flow



also sign attestations regarding the conduct of the test.

If there are deviations in the original planning, these should be discussed with the TCT. It is critical that all relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any issues, resource constraints, etc., can be addressed in a timely fashion. Although the White Team lead is the primary contact for the third-party providers, the TCT should also have access to the providers. Where there are crucial decisions to be made (e.g. deviations during the test from the agreed scope), or where differences of opinion arise, both the White Team lead and the TCT should have a formal escalation line to their respective superiors and between the superiors.

Abbreviations

Term	
CBEST	Bank of England's threat intelligence-led red team testing programme
ECB	European Central Bank
HUMINT	Human intelligence
OSINT	Open-source intelligence
TCT	TIBER-DK Cyber Team
TIBER	Threat Intelligence-Based Ethical Red-teaming
TIBER-EU	Common European framework for threat intelligence-based ethical red teaming
TIBER-DK	TIBER programme in Denmark
TIBER-NL	TIBER programme in the Netherlands
TKC	TIBER Knowledge Centre, the knowledge sharing forum for TIBER authorities