DEUTSCHE BUNDESBANK
EUROSYSTEM

Implementation of TIBER-DE

8 July 2020

Version 1.0

Contents

Abbreviations

BT	Blue Team
GTL	Generic Threat Landscape
RT	Red Team
TCT	TIBER Cyber Team
TIP	Threat Intelligence Provider
TKC	TIBER-EU Knowledge Centre
TTM	TIBER Test Manager
WT	White Team
WTL	White Team Lead

1 Introduction and background

In recent years, the threat posed by cyber attacks has become one of the most pertinent risks faced by the financial sector and the entities operating within it. One reason is because stakeholders are increasingly interconnected and IT services concentrated in the hands of just a few providers. In addition, however, professional and highly organised attacks known as Advanced Persistent Threats (or APTs) also represent a growing threat. In order to protect against attacks, it is prudent to comply with the latest cyber security standards (such as the BSI's IT-Grundschutz[1] or the international ISO/IEC 27001 standard[2]) and to raise awareness throughout the entity. However, whether this has the desired effect can usually only be determined once an actual attack has taken place. For example, flawed implementation or human error can quickly undo the benefits of any security measures taken.

Threat-led penetration tests address this issue by emulating the Tactics, Techniques and Procedures (TTPs) of real-world attackers, making it possible to deliver a realistic assessment of an entity's cyber resilience under controlled conditions. In order to ensure the standardisation of these tests across Europe, the central banks of the European System of Central Banks (ESCB) have created a common framework for threat-led penetration tests: TIBER-EU (Threat Intelligence-based Ethical Red Teaming).[3] The requirements set out in the TIBER-EU framework relating to the scope and execution of such tests are stringent in order to ensure high-quality tests that deliver realistic simulations. TIBER tests must be carried out on entities' live systems. Furthermore, the scope of the TIBER tests must generally include all of the entities' critical functions. Another requirement is for the tests to be carried out by independent third-party providers that are specifically qualified to conduct complex red teaming[4] penetration tests.[5] The rationale for conducting a TIBER test is not to successfully defend against an attack, but to identify weaknesses in an entity's defence mechanisms and measures. A successful TIBER test provides the entity with information on how attackers could successfully breach its security, enabling it to enhance its cyber defences accordingly.

In order to make such a standardised version of threat-led penetration tests available to the German financial sector, the Bundesbank, together with the Federal Ministry of Finance, decided in August 2019 to implement the European TIBER-EU framework in Germany. Implementing TIBER-DE gives entities in the German financial sector the opportunity to test their resilience against sophisticated and targeted attacks. TIBER-DE tests are always carried out by the entities themselves with the involvement of the appropriate service providers and supported by Germany's competence centre (the TIBER Cyber Team, or TCT), which is based at the Bundesbank.

The key to a successful TIBER test is the entity's close cooperation with third-party service providers and the TCT. The aim is to bring about lasting changes/improvements through open dialogue. For this rea-

1 See also https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (last accessed: 16 January 2020).
2 See also https://www.iso.org/isoiec-27001-information-security.html (last accessed: 8 January 2020).
3 See also https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (last accessed: 6 March 2020).
4 red teaming refers to the attempt by professional attackers commissioned by the entity being tested to hack into its systems. However, such attacks do not cross ethical and legal lines. red teaming simulations are considered to be an extremely realistic way for an entity to assess its defences.
5 See Services Procurement Guide: https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf (last accessed: 6 March 2020).

son, participation in TIBER-DE is voluntary for the entities and is based on a cooperative approach. TIBER tests thus effectively complement the many and varied efforts undertaken by entities and their supervisors, regulators and overseers in this field to date and make an important contribution to sustainably enhancing the cyber resilience of Germany's financial sector.

2 TIBER-DE overview

The TIBER-EU framework specifies a number of core elements to be followed in all TIBER tests. This document on TIBER-DE implements all of these core elements without explicitly repeating them here. It sets out TIBER-DE within the framework established by TIBER-EU and defines which optional elements are to be adopted.

The Bundesbank and the Federal Ministry of Finance have decided to take a voluntary, cooperative approach to the implementation of TIBER-DE. It is not a measure prescribed by financial supervisors, and it encourages entities to independently and self-critically assess the cyber resilience of their systems. Much like in other European countries, Germany's implementation of TIBER-EU therefore comprises an organisational structure that – legal obligations notwithstanding – involves financial supervisors at certain points (see Sections 5 and 8) but also gives entities a large degree of freedom and independence in testing and enhancing their own critical functions.

Within this structure, Germany's competence centre – the TIBER Cyber Team (TCT) – is based at the Bundesbank's Directorate General Payments and Settlement Systems and is thus firmly ring-fenced from the Bank's financial supervision units. The TCT supports each TIBER-DE test and confirms compliance with the requirements once it has been conducted.

Legal obligations notwithstanding, financial supervisors' involvement during a TIBER-DE Test is generally limited. Any involvement of financial supervisors shall be done via the TCT, which serves as the point of contact for the Federal Financial Supervisory Authority (BaFin, in particular its IT supervision group GIT). BaFin then acts as the contact point for all other financial supervisory bodies. Overall, with respect to the (planned) execution of TIBER-DE tests, the TCT is the point of contact for:

- actual and potential participants;
- other authorities involved in the TIBER-DE test process (e.g. security authorities[6]);
- other TIBER implementations in Europe;
- red teaming and threat intelligence providers (see Section 4);
- the Federal Government and its ministries as well as other bodies – such as the German Financial Stability Committee.

A Steering Committee comprising representatives from the Bundesbank and BaFin has been established to enhance and improve TIBER-DE and define strategic

6 For the purposes of this document, "security authorities" are, for example, those authorities that are members of the National Cyber Response Centre. The following is a non-exhaustive list of the authorities represented in the National Cyber Response Centre: Federal Office for Information Security, Federal Office for the Protection of the Constitution, Federal Office for Civil Protection and Disaster Assistance, Federal Criminal Police Office, Federal Intelligence Service, Federal Police, Military Counterintelligence Service, Customs Investigation Bureau.

objectives. The Steering Committee defines the priorities on the TCT's work agenda, evaluates the extent to which the TCT has achieved the objectives it has been set and, at least once a year, assesses whether changes to TIBER-EU framework requirements, the threat level or the market environment have made it necessary to adjust TIBER-DE. The TCT provides the Steering Committee with a general overview of its activities and key findings.

In addition to the TCT, security authorities should, where possible, be involved in the test process in order to assess – as far as legally possible and appropriate – the veracity of the information collected by TIBER-DE on the threat level and the attackers' TTPs and to add to it, if necessary. This is particularly important in the context of preparing and regular updating the Generic Threat Landscape (GTL) Report and in the context of an entity's Targeted Threat Intelligence (TTI) Report (see Section 5).

3 Target group

TIBER-DE is primarily aimed at critical financial sector entities to strengthen their cyber resilience and reduce domino effects in the financial sector. In particular, the target group includes the following entities:

- large banks operating in Germany;
- large insurance companies operating in Germany;
- financial market infrastructures operating in Germany;
- IT service providers operating in Germany and critical for the functioning of the financial sector.

As a rule of thumb for entities, they should consider whether the failure of any of their individual functions could result in significant disruptions to, or a lasting detrimental impact on, the financial sector or financial stability, public safety or other critical sectors. The definition of the target group is deliberately broad to allow for case-specific one-off assessments and so as to not restrict the flexibility with which voluntary TIBER-DE tests can be conducted by rigidly defining the target group. Only a holistic analysis of an entity, its internal structure and its interconnectedness with external service providers can ultimately shed light on whether a TIBER test is advisable. In this context, the TCT will approach those entities it considers relevant in order to jointly discuss the possibility of conducting a TIBER-DE test.

International entities that do not operate primarily in Germany can also undergo a TIBER-DE test. In such cases, however, it may be necessary to consult the designated TIBER authority in the entity's home country. In such instances, joint TIBER tests can be conducted with the TCTs of other Member States responsible for TIBER or with the European Central Bank to avoid duplication of work.

In order to be able to participate in a TIBER test, an entity must possess a certain level of cyber maturity. Although major gaps in an entity's basic security do not necessarily constitute an obstacle to executing the test, the full benefits of a TIBER test can only be reaped once a certain minimum level of cyber security has been reached. Only then serious shortcomings will already have been rectified so that attention can be focused on more detailed and entity-specific vulnerabilities.

The objective is thus to establish a network of German entities belonging to the target group in order to, jointly and by conducting TIBER-DE tests, enhance the cyber resilience of the financial sector sustainably and on a cooperative basis.

4 Stakeholders

The following stakeholders are involved in a TIBER test (see Figure 1):

- The **TCT** is the national competence centre for TIBER implementation. In Germany, the TCT is based at the Bundesbank (see Section 2). It supports the TIBER tests carried out by entities throughout all phases, provides necessary expert knowledge, ensures compliance with TIBER test requirements, certifies their alignment with the framework once they have been completed and acts as the contact point for all external enquiries. The TCT can classify a test as not being TIBER-compliant if it has not been carried out in accordance with the TIBER requirements.

- The **TIBER Test Manager (TTM)** is a member of the TCT who is responsible for a specific entity and serves as the entity's liaison. The TTM supports the entity through all phases of the TIBER test process and, as a general rule, is involved in all meetings and agreements between the stakeholders. This is always the case even for routine telephone calls, e.g. calls to coordinate current attack stages during the testing phase.

- The **White Team (WT),** which is represented by the **White Team Lead (WTL),** is the body within an entity responsible for performing a TIBER test. The WTL is appointed by the entity's board under the requirements set out in the framework and interfaces with the TCT's TTM. The WT members are authorised by the entity's board to commission the external attackers (see Red Team) and the external threat intelligence procurement team (see threat intelligence provider), i.e. they enter into contracts with them and supervise their execution.[7]

- The **Blue Team (BT)** comprises all employees of the entity who are not part of the WT. In practice, however, the Blue Team is usually represented by employees of the units responsible for corporate security (e.g. Security Operations Centre, Computer Emergency Response Team, etc.). The BT must not be informed that a TIBER test is being performed.

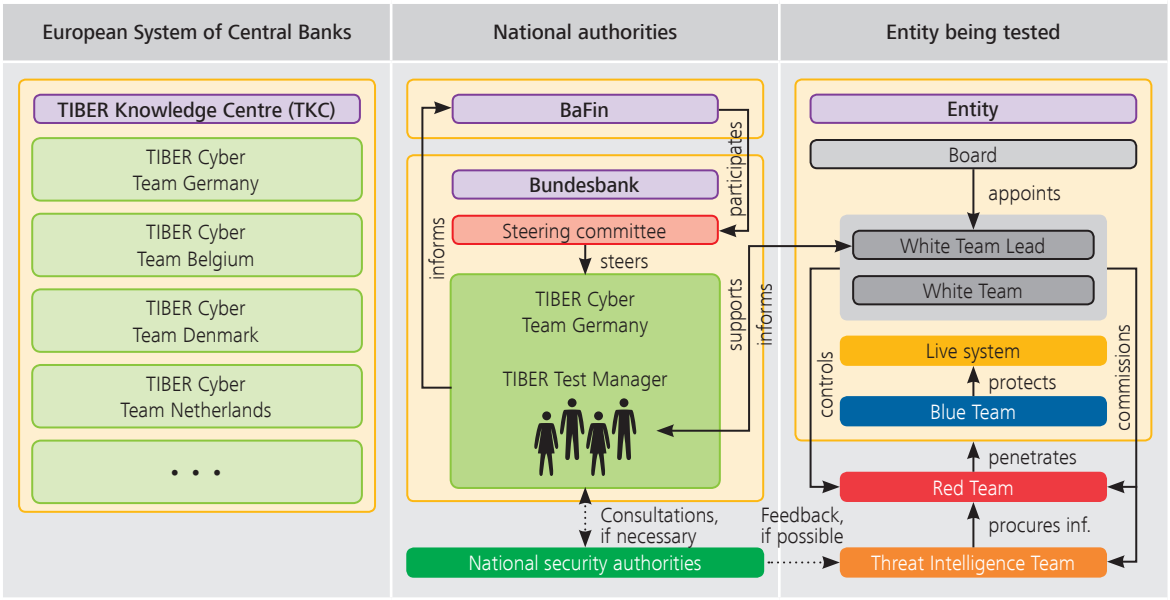
- The **Red Team (RT)** and **Threat Intelligence Provider (TIP)** are externally recruited by the authorised members of the WT. While the TIP collects information on general and entity-specific vulnerabilities and makes these available to the RT, the RT carries out the actual attacks. Its objective is to overcome the entity's defences and to penetrate the live systems. Where legally and organisationally possible, it is envisaged that one or more national security authorities provide feedback on the information collected on the threat situation in consultation with the TCT.

- The **TIBER Knowledge Centre (TKC)** is the European centre of expertise for all national TIBER implementations. It comprises representatives of the national TCTs of those EU Member States in which the TIBER-EU framework has been implemented. In addition to enhancing and improving TIBER-EU, the TKC's objective is to support the TCTs of all Member States in their TIBER implementations. To this end, it provides relevant documents and training courses, enables the exchange of experience and cooperation between countries, and ensures that the methodology and quality of the national implementations are comparable. However, no specific results are shared and no detailed information on the individual tests is passed on.

7 Further details on the White Team's tasks are provided in the TIBER-EU framework's White Team Guidance, which is available on the ECB's website: https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (last accessed: 28 October 2019).

Stakeholders involved in TIBER-DE

Figure 1



Stakeholders involved in TIBER-DE: TIBER Knowledge Centre (TKC), TIBER Cyber Team (TCT), TIBER Test Manager (TTM), White Team (WT), White Team Lead (WTL), Blue Team (BT), Red Team (RT), Threat Intelligence Provider (TIP), and, if applicable, national security authorities.
Source: Deutsche Bundesbank

5 The TIBER-DE test procedure

For the purpose of conducting TIBER-DE tests, the TCT provides a GTL Report, which serves as a starting point for all entities testing themselves. This report describes the general, non-entity specific threat situation of the national financial sector and should be updated regularly.

A TIBER-DE test consists of three phases:

- The **preparation phase** comprises the steps pre-launch, launch, scoping and procurement (see Figure 2). The following activities are carried out during this phase.

  – The entity and the TCT formally agree to perform a TIBER-DE test. The entity determines the White Team (WT) responsible for the test, including the White Team Lead (WTL), in consultation with the TCT.

  – In a pre-launch meeting, the TTM briefs the WT on the TIBER-DE test process, the stakeholders involved and their responsibilities, security protocols and the modalities of further test planning and execution. Participants may be asked to sign a non-disclosure agreement (NDA) to facilitate the efficient, safe and secure flow of information.

  – Financial supervisors are informed of the intention to perform a TIBER-DE test.

  – Necessary risk management measures, including requisite risk management controls and processes, are established by the WT in order to ensure that the test is conducted in a controlled and secure manner (see also Section 6).

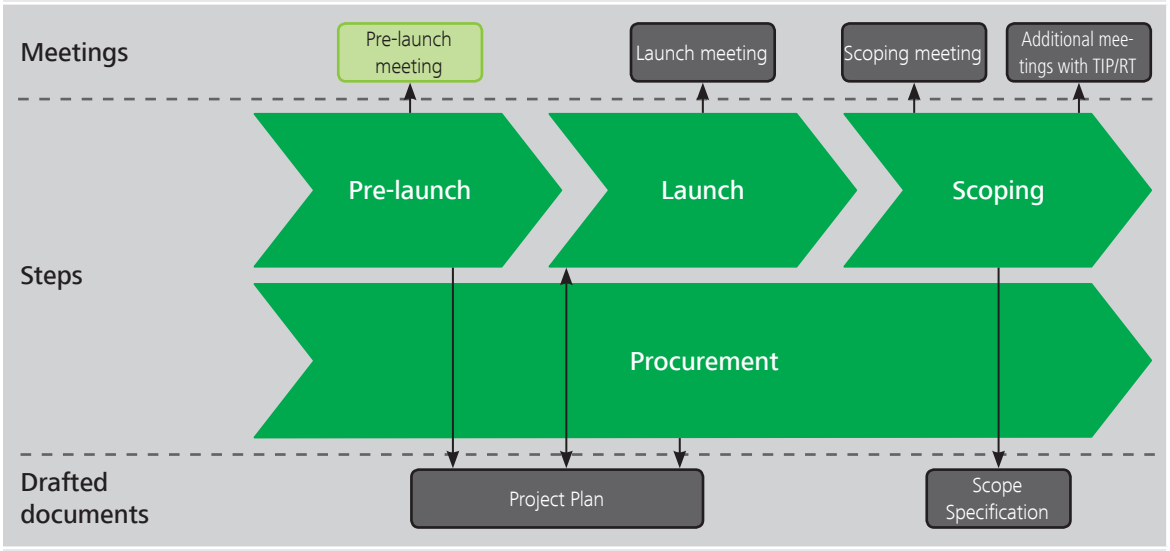
  – In a launch meeting, all stakeholders involved (if already defined) are briefed on the test procedure, exchange their mutual expectations and determine how to proceed. The basis for the discussion is a first version of the Project Plan prepared by the WT, which contains the general timeline including meetings to be organised and documents to be drafted, and which is adapted if necessary. Financial supervisors may also attend the launch meeting if desired.

  – The scope of the test is defined and approved by the entity's board and the TCT. The scope of the test must include all critical functions of the entity and be documented in writing in a Scope Specification document. The Scope Specification document is submitted to the competent financial supervisors for information purposes. Following this step, legal obligations notwithstanding, financial supervisors are generally not involved again until the Test Summary Report is sent.

  – In a scoping meeting, the Scope Specification document is presented to the TCT, WT, TIP and RT (if the tender and award procedure has already been completed) and finalised following their feedback.

  – The TI and RT providers are selected by the entity, and the entity enters into contracts with them (procurement; in principle, one provider may provide both teams, but the teams must consist of different people). Both teams are to be informed comprehensively by the WTL about the Project Plan and the scope of the test. This can already take place in the scoping meeting, and also in additional meetings between the WT, the TIP and the RT.

Preparation phase of a TIBER-DE test (approx. 4–6 weeks) Figure 2



Responsibilities colour-coded: WTL (grey), TTM (light green).
Source: Deutsche Bundesbank

- The **testing phase** comprises the steps threat intelligence collection and red team test execution (see Figure 3). The following activities are carried out during this phase:

  – Drafting of a TTI Report by the TIP, which is based on the GTL Report and which details additional entity-specific threats, vulnerabilities and attack scenarios. Due to the fact that the time frame for collecting information is considerably reduced compared with that of real attacks, it is explicitly envisaged that the report is augmented by relevant entity-internal information (e.g. overview of existing systems supporting critical functions, risk registers, identified vulnerabilities, examples of recent attacks).

  – Discussion of the draft TTI Report prepared by the TIP (if possible, involving relevant national security authorities) and the draft Red Team Test Plan prepared by the Red Team (outlining potential attack scenarios), in a threat intelligence/scenario workshop.

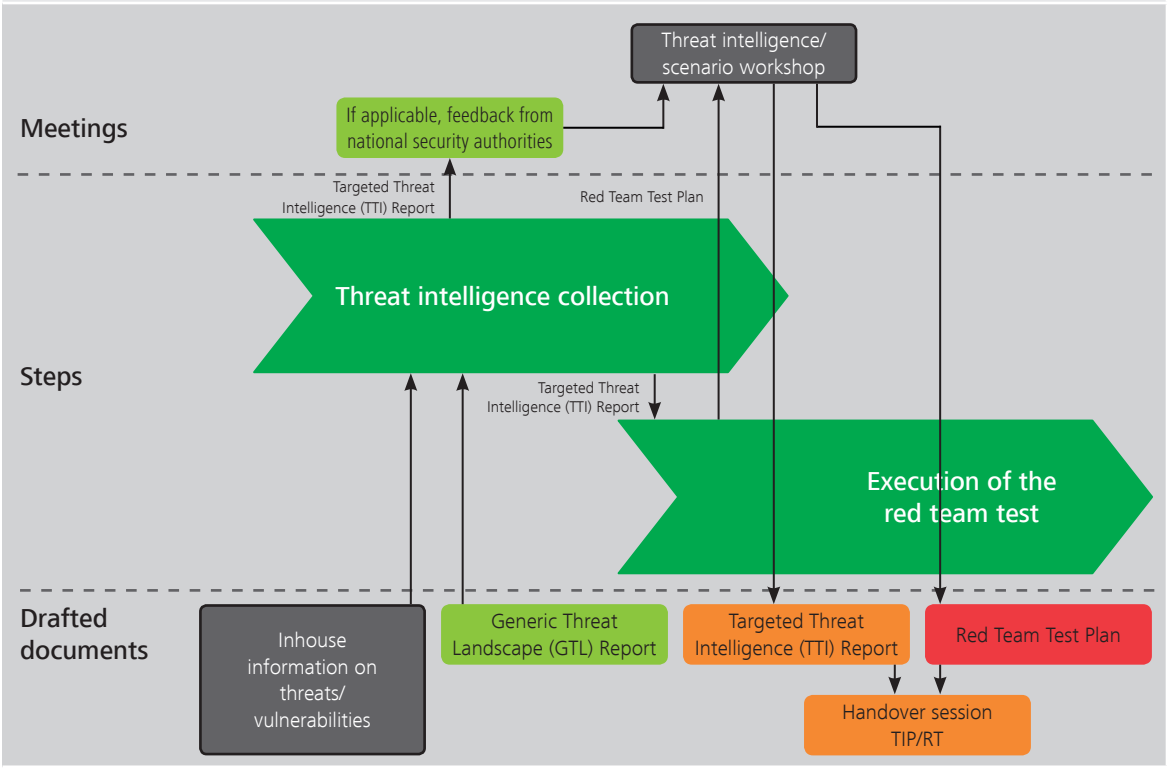
  – Finalisation of the TTI Report and the Red Team Test Plan, including the final attack scenarios on the entity's critical functions to be tested. Besides scenarios based on the threat-led attack vectors described in the TTI Report, it is expressly permitted to also include novel scenarios that are deemed relevant or to carry out a combination of threat-led and novel attack stages.

  – Discussion of the operational details of the finalised TTI Report and Red Team Test Plan in a handover session between the TIP and the RT.

  – Execution of the specified test scenarios by the RT. On the basis of insights gained in the meantime and in consultation with the TTM, adjustments can be made to the Red Team Test Plan at short notice or assistance (leg-ups) may be given.

– A temporal overlap of the activities carried out by the TIP and the RT is possible, i.e. the threat intelligence provided by the TIP can be adapted and further enhanced during the planning and execution of the attacks.

Testing phase of a TIBER-DE test (approx. 16–18 weeks) Figure 3



Responsibilities colour-coded: WTL (grey), TTM (light green), TIP (orange), RT (red).
Source: Deutsche Bundesbank

- The **closure phase** comprises the steps drafting of the Test Reports, replay and feedback, Remediation Plan and Test Summary Report as well as attestation and result sharing. The following activities are carried out during this phase:

  – The RT drafts a Test Report (Red Team Test Report) describing the specific procedures applied during the attacks, as well as their results and other observations. If necessary, the report should also contain detailed information on ways to improve the respective defence mechanisms (e.g. with regard to physical or technical security measures, entity policies and procedures, employee awareness and training, etc.).

  – All relevant units in the entity are informed about the test.

  – The BT drafts its own Test Report (Blue Team Report), based on the Red Team Test Report, detailing the countermeasures taken by the entity.

– The executed attacks are presented and analysed from the perspectives of the RT and the BT during a replay workshop. The Blue Team can thus gain an insight into where the Red Team was at what point in time and where/how it could have stopped/discovered it. Alternative attack and defence possibilities are likewise evaluated in this workshop in the form of a Purple Teaming element in which the RT and the BT discuss varying courses of attack and corresponding defence measures.

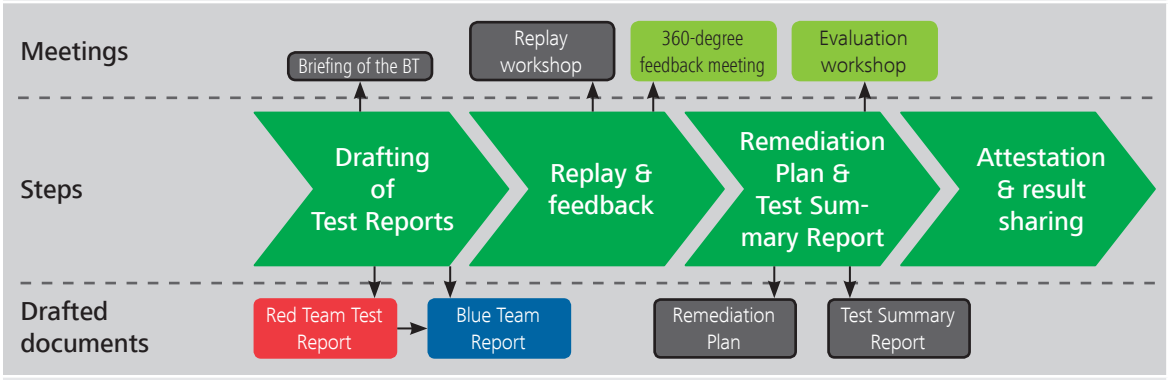
– The stakeholders involved in the test (TCT, WT, RT and TIP) provide feedback on their experiences of the practical execution of the TIBER-DE test (360-degree feedback) in a 360-degree feedback meeting.

– Based on the test results, the entity drafts a Remediation Plan at an appropriate level of abstraction, which lists the measures to be taken and a timeline for mitigating the vulnerabilities, but which does not include any detailed technical information. The plan is part of a Test Summary Report, also to be drafted by the entity, which summarises the test and the insights gained.

– The TCT usually organises a supplementary evaluation workshop between the entity and the members of the TIBER-DE steering committee (see Section 2). Its aim is to ensure the efficiency of TIBER-DE, to identify areas for improvement in TCT activities and to ensure the continued evolution of TIBER-DE.

– The TCT provides an attestation confirming that the TIBER-DE test was conducted in accordance with the framework. The entity sends the Test Summary Report including the Remediation Plan to the TCT, which then forwards it to the responsible financial supervision unit (see Section 8).

Closure phase of a TIBER-DE test (approx. 4 weeks) Figure 4



Responsibilities colour-coded: WTL (grey), TTM (light green), RT (red), BT (blue).
Source: Deutsche Bundesbank

6 Risks of a TIBER-DE test

Because TIBER-DE tests are implemented on live systems and their approach is highly flexible, they make it possible to perform a realistic analysis of an entity's cyber resilience. However, this also entails risks regarding the confidentiality, integrity or availability of data or systems. For example, if the tests are not carried out correctly, systems may be damaged or caused to fail, and data may be deleted or disclosed unlawfully. The testing entities should therefore first conduct a detailed analysis of the risks that could crop up during the test and then take appropriate action to mitigate these risks before, during and after the test.

As part of its activities as a national competence centre (TCT), the Bundesbank monitors all TIBER-DE tests, but does not accept any liability for any damage caused by entities conducting TIBER-DE tests. The WT is responsible for mitigating the risks of conducting a TIBER-DE test. It must ensure that risks have been adequately identified, analysed and mitigated at all times. Some examples of possible measures in this regard are:

- structuring the test in multiple stages to check regularly how far the RT has penetrated the systems;
- preparing detailed risk analyses and taking corresponding measures to mitigate risk throughout all of the phases of a TIBER-DE test;
- ensuring that the contracts with all participating external providers (e.g. TI and RT providers) contain appropriate liability provisions in the event of damage (including insurance, where applicable);
- clearly defining the scope, boundaries and timing of the tests in the contracts with all external service providers involved (e.g. TI and RT providers);
- clear escalation chains and designating of appropriate contact persons for emergencies between the entity and the external providers as well as within the entity itself;
- selecting external providers (e.g. TI and RT providers) in line with the TIBER-EU Services Procurement Guidelines[8] and in consultation with the TTM;
- close involvement of the TTM in all risk-relevant decisions during the tests;
- appropriate seniority level (C-level) of at least one member of the WT[9] to ensure the WT's decision-making capacity and direct communication with the board;
- clear authority and mandate of the WT to order a halt to the tests in the event of a heightened risk of damage in order to determine the next course of action in consultation with the providers and the TTM;
- defining actions not permitted by the TI and RT providers during the TIBER-DE test (e.g. forced entry, destruction of equipment, building parts or objects, uncontrolled modification of data and programs, extortion, threats, physical harm or bribery of employees, jeopardising continuity of services and disclosure of identified vulnerabilities).

8 The TIBER-EU Services Procurement Guidelines are available on the ECB's website at https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf (last accessed: 28 October 2019).
9 See also TIBER-EU White Team Guidance: https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (last accessed: 6 March 2020).

7 Mandatory and voluntary elements

The TIBER-EU framework defines most of the elements that are to be implemented, but also gives national implementations and entities some flexibility in its configuration.[10] In addition to the core elements envisaged by the TIBER-EU framework, the following aspects are prescribed for the implementation of TIBER-DE (mandatory elements):

- During the TIBER-DE tests, provision is made for the competent financial supervisors to read the Scope Specification as well as optionally participate in the launch meeting to receive transparent information on the implementation and scope of the test. Legal obligations notwithstanding, the relevant financial supervisors are generally not involved again until the test has been completed and the final Test Summary Report, including a Remediation Plan is presented (see Section 3).

- The TIBER-EU framework provides the option of drawing up a GTL Report on the financial sector, which is available to all entities conducting a TIBER-DE test and serves as the basis for preparing the TIP's TTI Report. A report of this kind is prepared during the implementation of TIBER-DE and updated at regular intervals. If possible, the report should be discussed with the national security authorities in order to increase its reliability.

- The analysis of the tests by a Purple Team (Purple Team = Red Team + Blue Team; see Section 5) is a prescribed element of a TIBER-DE test due to its associated learning effect.

Furthermore, each entity is free to address the following optional elements of the TIBER-EU framework in a TIBER-DE test (voluntary elements):

- Beyond its critical functions, the entity is free to specify other processes to be examined during a TIBER-DE test.

- It may make sense under certain circumstances for the TIP to remain continuously involved even after the start of the attacks by the RT; this shall be at the discretion of the entity.

- The inclusion of physical testing methods (e.g. physical access to the network, planting of an attacker's device at the entity) is generally desirable and encouraged, provided that the entity has expressly permitted this and this does not conflict with current legislation or the entity's security requirements.

- When conducting the replay workshop, the entity is free to decide which external participants are to be involved in addition to the RT and the TTM.

10 The requirements of THE TIBER-EU framework are laid out in the ECB's framework document: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (last accessed: 28 October 2019).

8 Results and use in financial supervision

The detailed results of the TIBER-DE test and information about identified vulnerabilities will remain exclusively with the tested entity. For security reasons, such sensitive information may not be passed on or disclosed. Furthermore, no centralised unit may be created to collect such highly security-relevant information on potentially systemically important agents in the German financial system (concentration risk). This is why TIBER-DE does not envisage the automatic transmission of detailed test results, legal obligations notwithstanding. The TCT does not store or retain any of this information, either.

Legal obligations notwithstanding, the competent financial supervisor is generally involved in the TIBER-DE test at predefined points. As outlined above, financial supervisors must be informed of the conduct of a TIBER-DE test, may take part in the launch meeting if desired and receive information on the test's Scope Specification. Furthermore, once the tests have been completed, the entity must send the Test Summary Report, including a Remediation Plan to the TCT, which then forwards it to the responsible financial supervision unit (see Section 5). The report should include concrete improvements (with timeline) at an appropriate level of abstraction as well as general experience from the TIBER-DE test. Information is exchanged between the entity and the relevant financial supervisors solely via the TCT and the financial supervision contact specified in Section 2.

9 Disclaimer

This document describes the implementation of the TIBER-EU framework in Germany (TIBER-DE) and transposes its core elements. The information contained in this document is for information purposes only. It does not constitute a legal or any other kind of expert assessment. The entity shall remain responsible for the independent legal and expert assessment of the intended test projects. The Bundesbank shall not be liable for any damages arising from the use of this document or from the TIBER-DE tests conducted by entities.

10 Annex

Annex 1: Meetings to be held during a TIBER-DE test with the responsible team and mandatory participants. The TTM is generally involved in all meetings and agreements between the participants. In addition to the meetings listed here, regular meetings or telephone calls are to be organised for information and coordination purposes.

	Meetings	Responsible person/team	Mandatory (voluntary) participation
preparation phase	Pre-Launch Meeting	TTM	WTL (WT), TTM
	Launch meeting	WTL	WTL (WT), TTM, (TIP), (RT), (Finanzaufsicht)
	Scoping meeting	WTL	WTL (WT), TTM, (TIP), (RT)
testing phase	Threat intelligence/ scenario workshop	WTL	WTL (WT), TTM, TIP, RT
	Handover session TIP/RT	TIP	RT, WTL (WT), TTM
	Further meetings with TIP/RT as required	WTL	WTL (WT), (TTM), TIP, RT
closure phase	Replay workshop	WTL	WTL (WT), TTM, RT, BT, (TIP)
	360-degree feedback meeting	TTM	WTL (WT), TTM, RT, BT, TIP
	Evaluation workshop	TTM	TTM, Steering Committee, WTL, (WT), (TIP), (RT)

Annex 2: Documents to be created during a TIBER-DE test with the entity responsible for creating the documents and participants with which consultation is mandatory

	Created document	Responsible for creating/ providing	Mandatory (voluntary) consultation with
preparation phase	Project Plan	WTL	TTM, (TIP), (RT)
	Scope Specification	WTL	Entity's board, TTM, TIP, RT, financial supervision
	Generic Threat Landscape Report	TCT	(National security authorities)
testing phase	In-house information on threats/vulnerabilities (as a contribution to the Targeted Threat Intelligence Report)	WTL	TTM
	Targeted Threat Intelligence Report	TIP	WTL, TTM, RT, (national security authorities)
	Red Team Test Plan	RT	WTL, TTM, TIP
closure phase	RT Test Report	RT	
	BT Report	BT	
	Remediation Plan	WTL	TTM
	Test Summary Report	WTL	TTM
	TIBER-DE attestation	TTM	TIP, RT, entity's board

Deutsche Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main

Postfach 10 06 02
60006 Frankfurt am Main

Telefon 069 9566-0
Telefax 069 5601071
Internet https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/serviceangebot/tiber-de/
E-Mail tiber@bundesbank.de