DEUTSCHE BUNDESBANK
EUROSYSTEM

Implementation of TIBER-DE

December 2022

Version 3.0

Table of contents

Abbreviations

BT	Blue Team
GTL	Generic Threat Landscape
RTP	Red Team Provider
TCT	TIBER Cyber Team
TIP	Threat Intelligence Provider
TKC	TIBER Knowledge Center
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 for this is because stakeholders are becoming 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 production 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 external providers that are specifically qualified to conduct complex red teaming[4] 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 defences, enabling it to enhance its cyber resilience accordingly.

In order to make these threat-led penetration tests available to the German financial sector in a standardised format, the Bundesbank, together with the Federal Ministry of Finance, decided in August 2019 to implement the European TIBER-EU framework in Germany. Since 2020, implementing TIBER-DE has given entities in the German financial sector the opportunity to test their resilience against sophisticated and targeted attacks. A number of tests have been conducted within the target group (see Section 3) since implementation began, and this document has been updated based on what has been learned.

1 See also www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (last accessed: 23 November 2022).
2 See also www.iso.org/isoiec-27001-information-security.html (last accessed: 23 November 2022).
3 See also www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (last accessed: 23 November 2022).
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 or 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: www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf (last accessed: 23 November 2022).

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 external service providers and the TCT. The aim is to bring about lasting improvements through open dialogue. For this reason, 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[6] 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 kept separate from financial supervisors. The TCT provides support during each TIBER-DE test and confirms compliance with the requirements once it has been conducted. The main task – and purpose – of the TCT is to support the entity and the service providers in such a way that the benefits are maximised as far as possible for the entity and the entire test process runs smoothly.

Legal obligations notwithstanding, financial supervisors' involvement during a TIBER-DE test is exclusively via the TCT. The financial supervisors involved by the TCT are a small group of individuals who are familiar with TIBER-DE and have the requisite specialist knowledge to be able to assess the TIBER tests. Overall, with respect to the execution of TIBER-DE tests, the TCT is the point of contact for:

6 In this document, the term "financial supervisors" describes the units at the Federal Financial Supervisory Authority (BaFin), the Bundesbank, the ECB and/or other supervisory authorities responsible for supervising the entities to be tested. In addition, BaFin's GIT 1 Division (Cyber Security and Digitalisation) is also involved as is relevant.

- actual and potential participants;
- other authorities involved in the TIBER-DE test process (e.g. security authorities[7]);
- 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 works to enhance and improve TIBER-DE and define strategic objectives. The Steering Committee defines the priorities on the TCT's work programme, 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 landscape 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 can be involved in the test process in order to assess – as far as legally possible and appropriate – the veracity of the information gathered by TIBER-DE on the threat landscape and the attackers' TTPs and to add to it, if necessary. This is particularly important in the context of preparing and regularly 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 spillover 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 guiding principle 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 not to restrict the flexibility with which voluntary TIBER-DE tests can be conducted. 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.

7 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.

International entities that do not just 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. Joint TIBER tests can be conducted with the TCTs of other MemberStates 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 will serious shortcomings already have been rectified so that attention can be focused on more detailed and entity-specific vulnerabilities.

Ultimately, the objective is 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, attests that they were conducted in accordance with the framework 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. In the case of cross-border TIBER tests, the responsible TCTs in other Member States can be involved in the test. Their involvement ensures that the TIBER test will be accepted in these Member States.
- 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 headed 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 liaises with the TCT's TTM.[8]

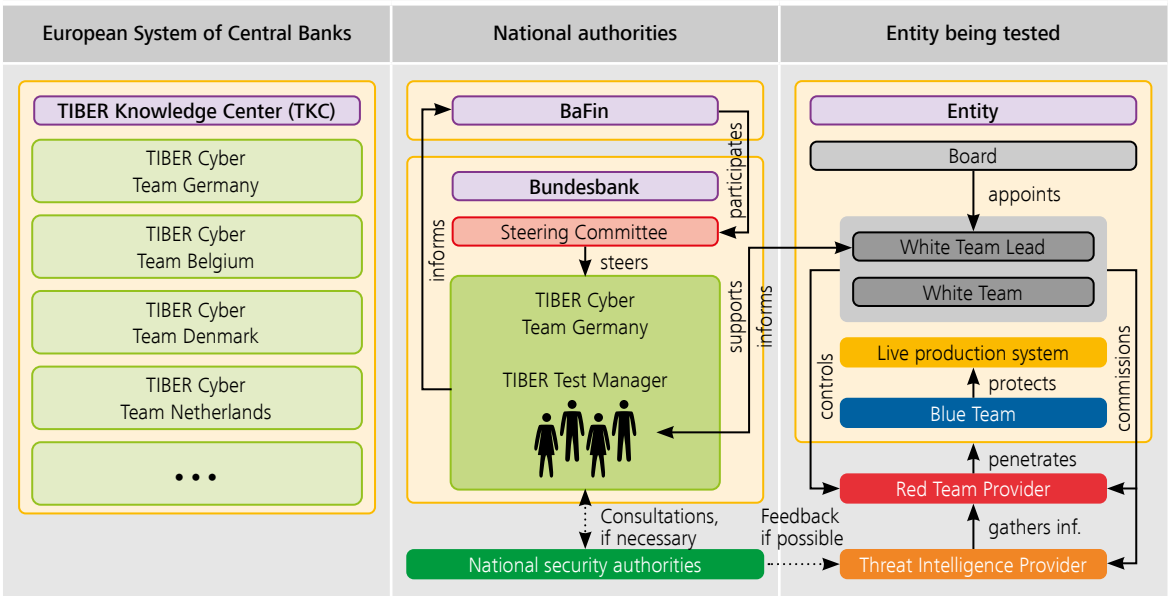
8 Further details on the White Team's tasks are provided in the TIBER-EU framework's White Team Guidance, which is available on the ECB's website: www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (last accessed: 23 November 2022).

- The **Blue Team (BT)** comprises all employees of the entity who are not part of the WT. In practice, however, the BT 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 Provider (RTP)** and **Threat Intelligence Provider (TIP)** are external service providers procured by authorised WT members. The latter conclude contracts with the service providers and oversee the correct execution of the test within the entity by the service providers. While the TIP gathers information on general and entity-specific vulnerabilities and makes these available to the RTP, the RTP carries out the actual attacks. Its objective is to overcome the entity's defences and to penetrate its live production systems. Where legally and organisationally possible, efforts are made in consultation with the TCT to receive feedback from one or more national security authorities on the threat intelligence gathered.

- The **TIBER Knowledge Center (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

Stakeholders involved in TIBER-DE Figure 1



Stakeholders involved in TIBER-DE: TIBER Knowledge Center (TKC), TIBER Cyber Team (TCT), TIBER Test Manager (TTM), White Team (WT), White Team Lead (WTL), Blue Team (BT), Red Team Provider (RTP), Threat Intelligence Provider (TIP), and, if necessary, national security authorities.

Source: Deutsche Bundesbank

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. The Bundesbank's TCT is represented in the TKC and plays an active role in ensuring the high quality of TIBER tests.

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:[9]

- 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 WT responsible for the test, including the WTL, in consultation with the TCT. The WT decides on a pseudonym for the TIBER-DE test. Given the sensitive nature of the test information being exchanged, this pseudonym must be used in place of the entity's real name in all TIBER-related communication.

  – 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 secure communication channels as well as the modalities of further test planning and execution.

  – Financial supervisors are informed by the TCT 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).

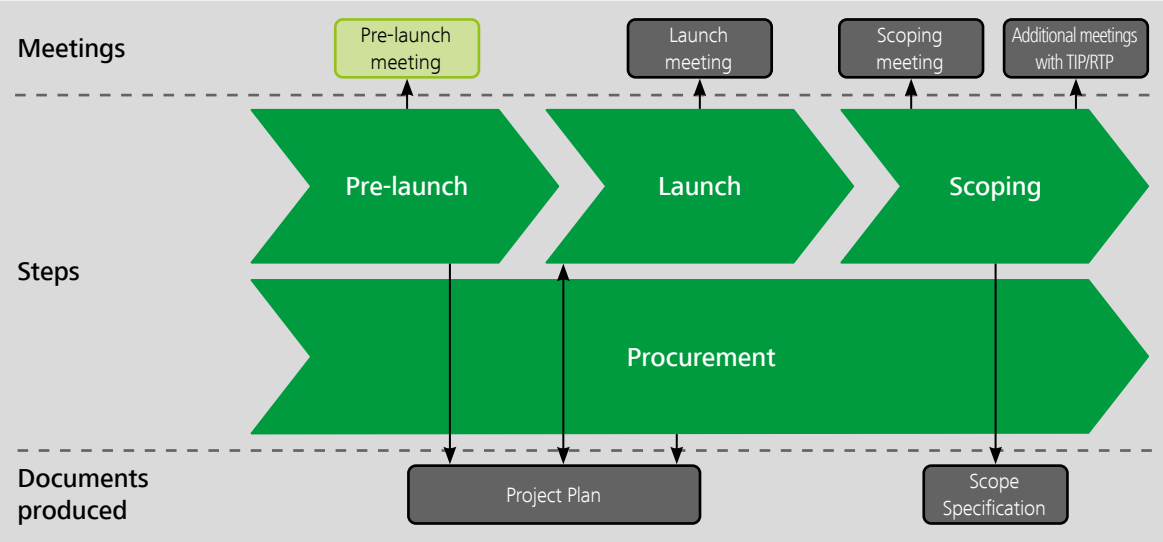
  – In a launch meeting, all relevant stakeholders (if already defined) are briefed on the test procedure, exchange their mutual expectations and determine how to proceed. The basis for the discussion is the Project Plan prepared by the WT, which contains the general timeline including meetings to be organised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

  – The scope of the test is defined. The scope of the test must include all critical functions of the entity and be documented in writing in a Scope Specification document. In a scoping meeting,

9 An overview of all meetings to be held and documents to be produced across all three phases, including all responsible parties and stakeholders involved, can be found in Annexes 1 and 2 (Section 10).

Preparation phase of a TIBER-DE test

Figure 2



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

the Scope Specification document is presented to the TCT, WT, RTP and TIP (if procurement is already complete) and, following their feedback, it is finalised and approved by the entity's board and the TCT. The Scope Specification document is presented to the competent financial supervisors for information purposes prior to the scoping meeting. This allows them to submit any comments via the TCT during the scoping meeting. Following this step, legal obligations notwithstanding, the financial supervisors are generally not involved again until the Test Summary Report is sent to them.

– In the course of procurement, the TIP and RTP 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 given detailed information about the Project Plan and the scope of the test by the WTL. This can already take place in the scoping meeting, and also in additional meetings between the WT, the TIP and the RTP.

• The **testing phase** comprises the steps threat intelligence gathering and Red Team Test execution (see Figure 3). The following activities are carried out during this phase:

– Preparation 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 gathering information is considerably reduced compared with that of real attacks, ex-

plicit provision is made for the report to be augmented by relevant entity-internal information (e.g. overview of existing systems supporting critical functions, risk registers, identified vulnerabilities, examples of recent attacks). The TIP provides the WTL and TTM with regular progress reports on the status of intelligence gathering.

– Discussion of the draft TTI Report prepared by the TIP and outlining, discussing and selecting potential attack scenarios in a scenario workshop.

– Further development of the TTI Report (if desired, involving relevant national security authorities) by the TIP.

– Formulation of the attack scenarios on the entity's critical functions by the RTP (Red Team Test Plan) based on the TTI Report.

  Besides threat-led attack scenarios described in the TTI Report, it is expressly permitted for the Red Team Test Plan to also include novel scenarios that are deemed relevant or to carry out a combination of threat-led and novel attack stages. A "scenario X" is a scenario in which the Red Team, instead of emulating a specific threat actor, can deviate from the threat-driven nature of a TIBER-DE test. In this way, alternative and/or exploratory scenarios can also be included.

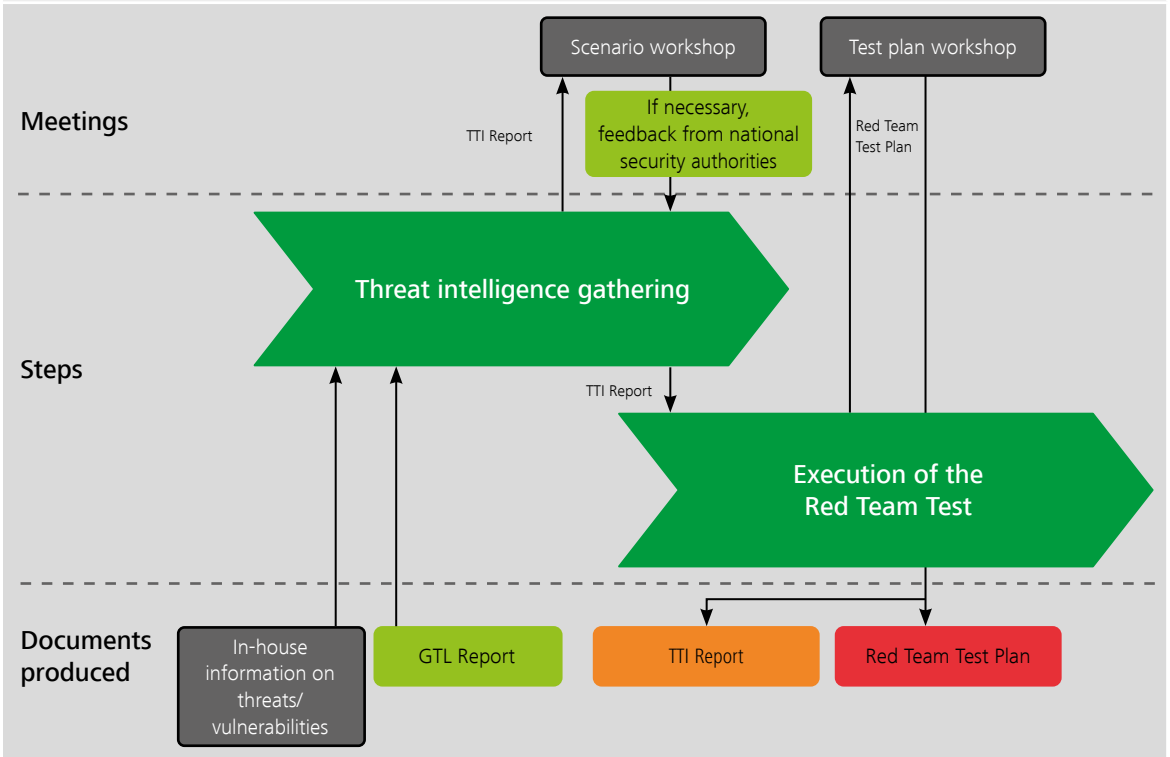
– Discussion of the operational details of the Red Team Test Plan in a test plan workshop. Finalisation of the TTI Report and Red Team Test Plan following the test plan workshop.

– Execution of red teaming by the RTP in line with the specified attack scenarios. 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. The RTP provides the WTL and TTM with regular updates on how the red teaming is progressing.

– An overlap in time between the activities carried out by the TIP and the RTP 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.

  One benefit of involving the RTP at an early stage in developing the attack scenarios as part of the TTI Report is that the information gathered by the TIP can be processed in a more targeted manner. Furthermore, the availability of the TIP during red teaming can ensure the threat-based nature of the attack scenarios, even if adjustments are necessary.

Testing phase of a TIBER-DE test (approx. 18 weeks, of which approx. 6 weeks threat intelligence and approx. 12 weeks red teaming) Figure 3



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

- The **closure phase** comprises the steps of producing the Test Reports, replay, purple teaming and feedback, Remediation Plan and Test Summary Report (including evaluation workshop) as well as attestation and result sharing (see Figure 4). The following activities are carried out during this phase:

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

  – All relevant units in the entity are informed of the test at the start of the closure phase (Blue Team Briefing).

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

– The Red Team Test Report and Blue Team Report are made available to the TTM.[10]

– During a replay workshop, the executed attacks are presented and analysed from the perspectives of the RTP and the BT. Alternative attack and defence possibilities are likewise evaluated in the form of a purple teaming element in which the RTP and the BT discuss differing courses of attack and corresponding defence measures (e.g. as a tabletop exercise). The BT can thus gain an insight into where the RTP was at what point in time and where/how it could have discovered/stopped it.

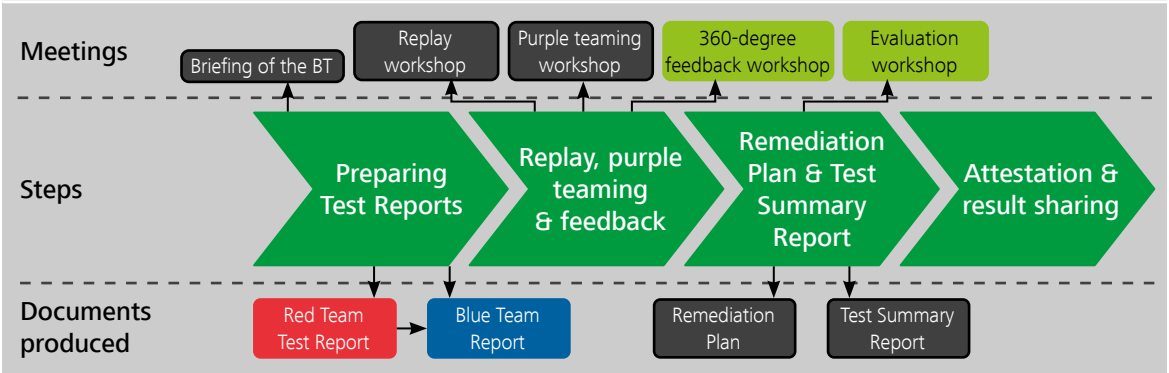
– The stakeholders involved in the test (TCT, WT, RTP and TIP) provide feedback on their experiences of the practical execution of the TIBER-DE test in a 360-degree feedback workshop.

– Based on the test results, the entity produces 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 on these points. The plan is part of a Test Summary Report, also to be produced by the entity, which summarises the test and the insights gained.

– The TCT head 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 facilitate 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 supervisors (see Section 8).

Closure phase of a TIBER-DE test Figure 4



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

10 As these documents are highly confidential, the Red Team Test Report and Blue Team Report are not saved or in any other way stored by the TCT.

6 Risks of a TIBER-DE test

Because TIBER-DE tests are implemented on live production systems and the way they are conducted 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 and 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, the Bundesbank (TCT) provides support during 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 conducting TIBER-DE tests, for the risks arising as a result and for mitigating those risks. It must ensure that risks are adequately identified, analysed and monitored at all times. Some examples of possible measures in this regard are:

- preparing detailed risk analyses and taking corresponding measures to mitigate risk throughout all of the phases of a TIBER-DE test;
- deciding on and exclusively using a pseudonym in place of the real name of the entity being tested;
- ensuring that the contracts with all participating external providers (e.g. TIP and RTP) contain appropriate liability provisions in the event of damage (including insurance, where applicable);
- appropriate seniority level (board level) of at least one member of the WT[11] 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;
- clearly defining the scope, boundaries and timing of the tests in the contracts with all external service providers involved (e.g. TIP and RTP);
- selecting external providers (e.g. TIP and RTP) in line with the TIBER-EU Services Procurement Guidelines[12] and in consultation with the TTM;
- 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 and with the TTM;
- clearly defining which actions the TIP and RTP may take during the TIBER-DE test, i.e. that are permitted by the entity (in the sense of giving factual consent or legal permission) and those they may not – one particular way in which this can be done is by listing actions that are expressly permitted (white list) or may not be taken under any circumstances (black list);
- structuring the test in multiple stages to check regularly how far the RTP has penetrated the systems;
- close involvement of the TTM in all risk-relevant decisions during the test.

11 See also TIBER-EU White Team Guidance: www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf (last accessed: 23 November 2022).
12 The TIBER-EU Services Procurement Guidelines are available on the ECB's website at www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf (last accessed: 23 November 2022).

7 Mandatory and optional 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.[13] In addition to the core elements set out by the TIBER-EU framework, the following aspects are prescribed for the implementation of TIBER-DE (mandatory elements):

- As part of the TIBER-DE tests, provision is made for the competent financial supervisors to read the Scope Specification document 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 8).

- 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. The GTL Report 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 RTP; 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 the law as it currently stands 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 RTP and the TTM.

13 The requirements of the TIBER-EU framework are laid out in the ECB's framework document: www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (last accessed: 23 November 2022).

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 that gathers highly security-relevant information on potentially systemically important agents in the German financial system (concentration risk). This is why TIBER-DE does not provide for 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 supervisors are 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 test has been completed, the entity must send its Test Summary Report, including a Remediation Plan, to the TCT, which then forwards it to the financial supervisors (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. Legal obligations notwithstanding, the exchange of information in the context of TIBER-DE tests between the entity and the relevant financial supervisors takes place solely via the TCT and the established supervisory points of contact who are familiar with the TIBER-DE framework and are thus able to assess the results.

9 Disclaimer

This document describes the implementation of the TIBER-EU framework in Germany (TIBER-DE) and transposes its core elements. The contents of this document are for information purposes only. They do 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 damage 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 party 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.

	Meeting	Responsible party	Mandatory (optional) participation
Preparation phase	Pre-launch meeting	TTM	WTL (WT), TTM
	Launch meeting	WTL	WTL (WT), TTM, (TIP), (RTP), (financial supervisors)
	Scoping meeting	WTL	WTL (WT), TTM, (TIP), (RTP)
Testing phase	Scenario workshop	WTL	WTL (WT), TTM, TIP, RTP
	Test plan workshop	WTL	WTL (WT), TTM, TIP, RTP
	Further meetings with TIP/RTP as required	WTL	WTL (WT), (TTM), TIP, RTP
Closure phase	Replay workshop	WTL	WTL (WT), TTM, RTP, BT, (TIP)
	Purple teaming workshop	WTL	WTL (WT), TTM, RTP, BT, (TIP)
	360-degree feedback workshop	TTM	WTL (WT), TTM, RTP, BT, TIP
	Evaluation workshop	TCT head	TCT head, Steering Committee, WTL, (WT), (TIP), (RTP)

Annex 2: Documents to be produced during a TIBER-DE test, with the party responsible for producing the documents and stakeholders with whom consultation is mandatory.

	Document produced	Responsible party	Mandatory (optional) consultation with
Preparation phase	Project Plan	WTL	TTM, (TIP), (RTP)
	Scope Specification document	WTL	Entity's board, TTM, TIP, RTP, financial supervisors
Testing phase	In-house information on threats/vulnerabilities (as a contribution to the TTI Report)	WTL	TTM
	TTI Report	TIP	WTL, TTM, RTP, (national security authorities)
	Red Team Test Plan	RTP	WTL, TTM, TIP
Closure phase	Red Team Test Report	RTP	WTL, TTM
	Blue Team Report	BT	WTL, TTM
	Remediation Plan	WTL	TTM
	Test Summary Report	WTL	TTM
	TIBER-DE attestation	TTM	TIP, RTP, entity's board

Deutsche Bundesbank
Postfach 10 06 02
60006 Frankfurt am Main
Germany

Internet www.bundesbank.de/en/tasks/payment-systems/tiber-de/tiber-de-817014
Email tiber@bundesbank.de