

Implementation of TIBER-DE

July 2025

CONTENT

1	Background	3
2	Regulatory content and scope.	4
3	Role of the Deutsche Bundesbank.	5
4	Financial supervisory involvement.	6
5	Disclaimer	7

1 BACKGROUND

In recent years, the threat posed by cyberattacks has become one of the most significant risks faced by the financial sector and the entities operating within it. This is partly due to the increasing interconnectedness of actors and the growing importance of certain companies in providing critical IT services. Additionally, professional and highly organised attackers pose an increasing danger. To protect against attacks, it is advisable to adhere to current cybersecurity standards (such as the BSI's IT-Grundschutz¹ or the international standard ISO/IEC 27001²) and to raise awareness throughout the entire entity. The success of implementing such measures can usually only be determined in the event of a real attack. Implementation errors or human weaknesses can quickly undermine the security precautions taken.

Threat-led penetration tests address this issue by imitating the methods of real-world attackers, thus enabling a realistic assessment of an entity's cyber resilience under controlled conditions. In order to ensure the standardisation of these tests across Europe, the members of the European System of Central Banks (ESCB) have created a common framework for voluntary threat-led penetration tests: TIBER-EU (Threat Intelligence-based Ethical Red Teaming). 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 simulation.

¹ See also

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (last accessed: 1 July 2025).

² See also <https://www.iso.org/isoiec-27001-information-security.html> (last accessed: 1 July 2025).

2 REGULATORY CONTENT AND SCOPE

In August 2019, the Deutsche Bundesbank, together with the Federal Ministry of Finance, decided to implement the TIBER-EU framework in Germany as TIBER-DE. With the implementation of TIBER-DE, entities in the German financial sector have had the opportunity since 2020 to test their cyber resilience through sophisticated and targeted attacks.

TIBER-DE is primarily aimed at large and critical entities in the German financial sector to strengthen their cyber resilience and reduce spillover effects in the financial sector.

Following the extensive update to the TIBER-EU framework in January 2025, it is no longer necessary to adapt or specify individual test components at a national level, as the regulatory content of the TIBER-EU framework is directly and fully applicable to TIBER-DE tests.³ The process steps to be followed in a TIBER-DE test are published as part of the TIBER-EU framework on the European Central Bank's website,⁴ where further guidelines specifying the individual test components can also be found.

The requirements of the TIBER-EU framework are also fully in line with the provisions of the regulatory technical standard for threat-led penetration tests⁵ (TLPT) according to Regulation (EU) 2022/2254 (Digital Operational Resilience Act, DORA)⁶. TIBER-EU thus forms the operational basis for performing both voluntary TIBER-DE tests and mandatory threat-led penetration tests based on DORA.

³ Under the TIBER-EU framework, a report on the national threat landscape in the financial sector (Generic Threat Landscape, GTL) can be provided by the TCT prior to the preparation phase of a test. The GTL can serve as a basis for creating the entity-specific targeted threat intelligence report. For TIBER-DE tests, the TCT makes use of the option to provide the GTL to tested entities.

⁴ <https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html> (last accessed: 1 July 2025)

⁵ Commission Delegated Regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

⁶ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

3 ROLE OF THE DEUTSCHE BUNDESBANK

The TIBER Cyber Team (TCT) is based at the Deutsche Bundesbank's Directorate General Payments and Settlement Systems as Germany's competence centre for TIBER-DE implementation. The TCT is operationally responsible for both:

- voluntary TIBER-DE tests scheduled via the TCT, and
- TLPTs according to DORA mandated by BaFin, the ECB⁷ or other authorities⁸.

The TCT ensures that all tests are carried out in accordance with the TIBER-EU framework. The TCT continues to be involved in cross-border tests together with the TCTs of other countries.

Contact: tiber@bundesbank.de; tlpt@bundesbank.de

⁷ Insofar as this order by the ECB concerns entities domiciled in Germany and the ECB does not explicitly reserve the right to carry out the test itself.

⁸ In Germany, for example, the stock exchange supervisory authorities of the federal states.

4 FINANCIAL SUPERVISORY INVOLVEMENT

For TLPTs that are mandatory under DORA, the competent financial supervisory authority⁹ is generally involved at predefined stages of the TLPT, without prejudice to legal obligations. It identifies the entities required to undergo testing,¹⁰ validates the test scope, and receives the final report as well as the remediation plan. Communication between the entity and the competent financial supervisors, as well as the forwarding of documents to be shared, is generally conducted via the TCT, unless otherwise agreed or legally stipulated.

For voluntarily conducted TIBER-DE tests, the involvement of the financial supervisory authority and the sharing of documents are based on individually agreed arrangements.

⁹ 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.

¹⁰ In accordance with the European DORA regulation.

5 DISCLAIMER

This document describes the implementation of the TIBER-EU framework in Germany (TIBER-DE). 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 damages arising from the use of this document or from the TIBER-DE tests or TLPT according to DORA conducted by entities.

Deutsche Bundesbank

Postfach 10 06 02
60006 Frankfurt am Main
Germany

Internet <https://www.bundesbank.de/en/tasks/payment-systems/tiber-de>

Email tiber@bundesbank.de, tlpt@bundesbank.de