2025

TIBER – CZ

Implementation document

Version 1.0

CNB CZECH NATIONAL BANK

Table of contents

CNB CZECH NATIONAL BANK

I. INTRODUCTION

I.1 BACKGROUND AND PURPOSE OF TIBER-CZ

The Czech National Bank (CNB) is the central bank of the Czech Republic, the supervisor of the Czech financial market and the Czech resolution authority. It is established under the Constitution of the Czech Republic and carries out its activities in compliance with Act No. 6/1993 Coll., on the Czech National Bank, as amended and other regulations. It is a legal entity under public law having its registered address in Prague. CNB therefore monitors supervised entities to ensure their activities comply with legally binding legislation and that they are in line with sound and appropriate business practices.

One of the CNB's main tasks is to promote a safe, stable, and effective financial system. Financial stability means, among other things, that the financial system is equipped to withstand operational incidents to ensure the availability of capital, credit and payments system. In recent years, cyber risk has risen to become one of the major risks for financial stability. As a result, cyber risk has become part of the CNB´s focus in this respect.

I.2 WHAT IS TIBER-EU?

The European Central Bank (ECB) published the Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) in May 2018[1]. The framework was jointly developed by the ECB and the EU national central banks. TIBER-EU is a framework for conducting intelligence-led red team tests of entities' critical live production systems. It was produced with the financial sector in mind but can be used in other markets. TIBER-EU therefore has the following core objectives:

- enhance the cyber resilience of entities and of the financial sector;
- standardise and harmonise how intelligence-led red team tests are performed in the EU, while also allowing each jurisdiction a degree of flexibility in the implementation of the framework by adding its national specificities;
- provide guidance to authorities on how they might implement and manage this form of testing at a national or European level;
- help entities and authorities to fulfil the requirements to perform Threat-Led Penetration Tests (TLPT) as per established regulation(s) in a safe manner, through the use of TIBER-EU. For example, Regulation (EU) 2022/2554, referred to as the Digital Operational Resilience Act (DORA). The TLPT-related requirements under DORA are included in the detailed TIBER-EU testing process, so that financial entities completing a test under a national or European-level implementation of the TIBER-EU framework will be DORA TLPT-compliant, assuming they fulfil the formal TLPT-related requirements set by the competent authorities. The TIBER-EU framework may be used as a handbook or set of detailed guidelines on how to complete DORA TLPT in a qualitative, controlled and safe manner – one which is consistent and uniform throughout the EU[2];
- support cross-border, cross-framework intelligence-led red team testing for multi-jurisdictional entities;
- foster mutual recognition of tests across the EU jurisdictions, by relying on test results and collaborating on joint tests, thereby reducing the regulatory burden on entities and authorities;
- catalyse information sharing and the joint analysis of test results.

---

[1] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[2] See for further information: 'Adopting TIBER-EU will help fulfil DORA requirements', September 2024, available at: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf

II. ABOUT TIBER-CZ

CNB has decided to adopt TIBER-EU framework as the TIBER-CZ program.[3] The overall aim of TIBER-CZ is to enhance cyber resilience in the Czech financial sector and thus promote financial stability. Following the implementation, the CNB is the lead authority of the TIBER-CZ.

In this implementation document, the CNB describes the TIBER-CZ program, with the aim to enhance the cyber resilience of entities critical to the Czech financial system. As cyber risk has the potential to become a systemic risk, a further important purpose of TIBER-CZ is to increase resilience toward cyber risk in the Czech financial system. TIBER-CZ is used for testing obligations stemming from relevant legislation, it is not meant as a supervision tool (as the learning effect of the test should prevail).

III. THE TARGET SECTORS IN SCOPE OF TESTING

In accordance with Act No. 6/1993 Coll., on the Czech National Bank, the CNB is a supervisory authority of the financial market in the Czech Republic. The CNB therefore supervises the banking sector, the capital market, the insurance industry, pension funds, credit unions, bureaux-de-change, payment institutions and other financial institutions. The CNB lays down rules safeguarding the stability of the banking sector, the capital market, the insurance industry and the pension scheme industry. It systematically regulates, supervises and, where appropriate, issues penalties for non-compliance with these rules.

When determining the target sector for testing, the CNB decision will be based on the requirements of Regulation (EU) 2022/2554 on digital operational resilience for TLPT. Therefore, it will concern mainly "other systemically important institutions", in which the risks are connected with potential destabilization, which could have significant adverse effects on the financial system and the economy as a whole.[4] They are the most important credit institutions in the Czech financial market. Furthermore, institutions such as central securities depositories and trading venues may be included in the tests in accordance with the requirements of Regulation DORA for TLPT. The TIBER-CZ framework will be used as well in case of undertaking threat-led penetration testing on voluntarily basis as a recommended testing standard.

IV. THE CNB´S ROLE AND RESPONSIBILITIES IN TIBER-CZ

The CNB implements the TIBER-CZ program for entities critical to the Czech financial system. The CNB supports the entities by providing guidance and Test Manager Support services. The CNB is the lead authority of TIBER-CZ and Financial Market Supervision Department of the CNB has formal ownership of the program.

IV.1 TIBER-CZ CYBER TEAM

The CNB is responsible for the establishment and operation of the TIBER-CZ Cyber Team, TCT, which has been set up within the CNB.[5] The role of the TCT is twofold:

- Manage the TIBER-CZ program, maintain the national implementation document, and act as a contact for other TCTs and the TIBER-EU Knowledge Centre (TKC).
- Ensure uniform, high-quality tests by the entities that fulfill the requirements of TIBER-CZ. A key part of the TCT is the Test Manager (TM), who manages the tests from the TCT's side.

---

[3] This decision was published publicly on the website CNB https://www.cnb.cz/cs/dohled-financni-trh/novinky/cnb-pristupuje-k-ramci-tiber-eu/index.html

[4] List of other systemically important institutions https://www.cnb.cz/en/financial-stability/macroprudential-policy/list-of-other-systemically-important-institutions/

[5] The TCT is located in the Financial Market Supervision Department, Financial Market On-Site Inspection Division III.

During a TIBER-CZ 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-CZ principles or the requirements of the TIBER-EU framework. The CNB is responsible for ensuring that the TCT has adequate resources and skills to carry out its assignment.

IV.2 CONTACTS WITHIN TCT

Email adress : Tiber-CZ@cnb.cz

V. REFERENCES TO TIBER – EU DOCUMENTATION

TIBER-CZ will solely use the TIBER-EU documentation for the conducts of the test. The link to the TIBER-EU webpage is provided below. This website contains links to the complete documentation of TIBER-EU framework.

https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

VI. LIST OF ABBREVIATIONS

CNB	Czech National Bank
TIBER	Threat Intelligence-Based Ethical Red Teaming
TCT	TIBER Cyber Team

Issued by:
CZECH NATIONAL BANK
Na Příkopě 28
115 03 Praha 1
Czech Republic