Implementation of the TIBER-IT National Guide

The increasing sophistication and pervasiveness of the cyber threat in modern economies, in part as a result of their rapid digitalisation and the deep interconnection among different stakeholders and countries, has placed cyber resilience[1] among the priorities for action by governments, international bodies and authorities. Recent developments have shown that the cyber resilience of vital infrastructures and financial operators needs to be increasingly monitored at various levels, in order to ensure the continuity of economic activities and the services provided to the community as well as their security and reliability, in line with the digital development of the economy and society.

The cyber threat is particularly marked for the financial sector, due to the economic motivations of attackers, the number and diversification of relevant parties operating in this context, the close interconnection between different nodes of the system. There is a fair chance that a disruption or a major attack on a single operator may pose contagion risks to others and that, in this way, the stability and efficiency of the financial system, the continuity of financial, banking and insurance services, the security of the payments system and the trust of citizens and businesses could be jeopardised.

Regulatory and standardisation bodies at international and European level and the authorities of the financial sector have adopted and are improving several measures to strengthen prevention, defence and response capabilities against cyber threats to single operators and to the financial system as a whole.

In this context, the objective of strengthening the proactive defence capabilities of financial entities is particularly important, also by means of advanced penetration tests, based on the relevance and the complexity of risk scenarios and the financial entity's business and operating model.

The various methodological guides, recommendations and regulations issued at international and European level are addressed to these issues,[2] and are also aimed at fostering harmonised and comparable methodologies for carrying out such tests, due to the links between the different components of the financial system and to its interconnections

---

[1] "*The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents." (FSB Cyber Lexicon, 2018).*

[2] *G7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT), G7 Cyber Expert Group, 2018; G7 Fundamental elements for cyber security in the financial sector (G7FE), G7 Cyber Expert Group, 2016; Guidance of Cyber Resilience for Financial Market Infrastructures, CPMI-IOSCO, 2016. At European level, the following must be taken into account: i) the Proposal for a Regulation on digital operational resilience for the financial sector by European Commission, ii) the Guidelines on information and communication technology security and governance by EIOPA (EIOPA-BoS-20/600); iii) the Guidelines on ICT and security risk management by EBA (EBA/GL/2019/04); iv) the Guidelines on outsourcing to cloud service providers by ESMA (ESMA50-164-4285); and v) the Joint Advice on the costs and benefits of a coherent cyber resilience testing framework by the three ESAs.*

at international level. At European level, the reference model for performing such tests is the Threat Intelligence-Based Ethical Red Teaming or TIBER-EU, adopted by the ECB[3] in 2018.

The TIBER-EU framework is implemented through the attached TIBER-IT National Guidance, which has been adopted by the Bank of Italy, Consob and IVASS, in order to provide the Italian financial system with a methodology for financial entities to conduct, on a voluntary basis, advanced cybersecurity tests led by threat intelligence.

In line with the goals of the joint strategy for cybersecurity in the Italian financial sector issued by the Bank of Italy and Consob,[4] the adoption of this Guidance will improve the cyber resilience of the Italian financial system and, as a consequence, its overall stability.

TIBER-IT is addressed to several types of Italian financial entities: market infrastructures, payment systems and the supporting technological or network infrastructures, trading venues, banks, payment and electronic money institutions, financial intermediaries pursuant to Article 106 of Legislative Decree 385/1993 (as amended), referred to as the Consolidated Law on Banking (TUB), insurance undertakings and intermediaries. Tests may be conducted by financial entities on a voluntary basis, taking into account their level of cyber maturity; the final decision to undergo the test lies with the financial entity, which is responsible for the management of all risks relating to the test execution, which is carried out by external service providers chosen by the tested entity. The three Authorities address test planning, taking into account the evolution of risk scenarios and the importance of financial entities for the sector business continuity.

Specifically, the TIBER-IT National Guidance: a) defines the methodology and operating model for the execution of TLPT tests by Italian financial entities; b) outlines the different phases of the testing process; and c) defines the roles, responsibilities and activities of the various stakeholders involved (Authority, tested entity and external providers).

To support financial entities in the use of this methodology and in the testing activities, the three Authorities provide a specific centre of competence: the TIBER Cyber Team Italy (TCT). Experts from the Bank of Italy, in close collaboration with experts from Consob and IVASS, ensure TCT operations.

The TCT can be contacted at the following e-mail address: tiber-it@bancaditalia.it.

It is expected that the leading Italian financial entities will endorse the new TIBER-IT and will proactively perform TLPT tests, as a further step towards strengthening the management of the main and emerging risks.

[3] The ECB requires mandatory TIBER-EU tests for systemically important European payment systems (SIPS); at national level, competent authorities have been allowed to adopt similar methodologies on a compulsory or voluntary basis.

[4] https://www.bancaditalia.it/media/comunicati/documenti/2020-01/cS_BIConsob_20200116_ENG.pdf.

This note and the TIBER-IT National Guidance have been published on the websites of the Bank of Italy, Consob and IVASS.

For Consob The President	For IVASS The President	For Bank of Italy The Governor
Paolo Savona	*Luigi Federico Signorini*	*Ignazio Visco*