Box 2.2

TIBER-ES: A FRAMEWORK FOR STRENGTHENING FINANCIAL SECTOR CYBERSECURITY

In a context in which the provision of financial services is fundamentally digital, it is crucial that financial institutions have an adequate level of cybersecurity. In recent years, as the digitalisation of the sector has progressed, cyber attacks have intensified significantly in terms of volume and sophistication. It should not be forgotten that the financial sector is particularly attractive to various types of attackers, from those seeking illicit economic gain to those seeking to destabilise society.

Therefore, institutions need to be constantly prepared to deal with cyber threats. This means improving not only their protection and detection capabilities, but also the capabilities that enable them to respond effectively to a cyber incident. It should be noted that while technical measures are essential, it is no less important to protect the human factor, which is often successfully exploited by cyber attackers. To this end, institutions must provide training and raise awareness among all their employees on the subject of cybersecurity, including senior management. Lastly, institutions need to establish organisational processes that allow for an agile and coordinated response and ensure the necessary communication.

As part of its commitment to improving the financial sector's cybersecurity, the Banco de España has adopted the advanced cybersecurity testing framework, TIBER-ES. This framework constitutes the local adoption of TIBER-EU, published by the European Central Bank, and will allow any financial institution or financial market infrastructure operating in Spain to voluntarily undergo a TIBER-ES test. The National Securities Market Commission and the Directorate General of Insurance and Pension Funds are collaborating in the adoption, and the role of the three authorities is to validate that the tests are carried out in line with the framework's requirements.

Testing under the TIBER-ES framework enables financial institutions to enhance their cybersecurity capabilities. These tests, which are conducted by an external provider without the institution's defensive teams being informed, simulate a sophisticated cyber attack on production systems. The objective is for the institution to detect possible weaknesses in the three above-mentioned factors: technical, human and organisational, which could be exploited by a real attacker. While the sophistication of these tests makes them recommendable only for institutions with the highest level of cybersecurity maturity, TIBER-ES aims to be a catalyst to encourage all institutions to improve their capabilities, until they become candidates to undergo this type of test.