Box 9. The management of cyber risks to payment systems

Cyber risks are major challenges to the smooth functioning of contemporary economies, as they can render critical infrastructures, including payment systems, unavailable. In this context, the adequate management of such risks became one of central banks' major concerns.

Among the operational risks, cyber threats are becoming increasingly prevalent, in view of the recent cyber attacks on central banks and credit institutions, with very serious consequences on their financial standing, reputation and availability of services. These attacks were particularly persistent and the attackers had an advanced know-how (state players and organised crime).

Under the circumstances, SWIFT released a set of detailed recommendations for all connected financial institutions (SWIFT Customer Security Controls Framework). In its turn, the European Central Bank published the *Cyber Resilience Oversight Expectations* (*CROE*), addressing the oversight function within central banks, and drafted a methodology for effectively testing cyber resilience to new sophisticated, persistent threats. The methodology, referred to as *Threat Intelligence Based Ethical Red Teaming* (TIBER-EU), addresses all EU financial market infrastructures and the participants therein.

These steps are designed to further an adequate governance framework for promoting digital security and cyber resilience, which is pivotal to preventing cyber threats or successfully withstand such incidents occurring in an increasingly digital and interconnected economic environment.

At the level of the European System of Central Banks there has been an ongoing concern for further strengthening the response and recovery capacity in the event of a cyber attack, by improving business continuity plans and testing the existing modalities to manage incidents and crises. At the same time, efforts have been consistently made to raise awareness of cyber risks.

The National Bank of Romania attaches particular importance to the management of cyber risks, in its capacity as both a national oversight authority for payment systems and an administrator and technical operator of ReGIS payment system. In this context, the NBR complied with SWIFT recommendations, carried out comprehensive tests of cyber resilience for the new technical platform of ReGIS, participated directly in the drafting of CROE and TIBER-EU and has been implementing ISO 27001 standard on information security management. Moreover, the NBR adopted the CROE Guidance in its oversight activity and officially recognised the TIBER-EU framework as a valid methodology for testing cyber resilience.