

ECB Operations Managers Group
Thursday, 21 March 2024

Summary

1. Introduction

Emily Witt (Chair of the ECB Operations Managers Group) welcomed Jérémy Bernardi as new member from Société Générale Corporate and Investment Banking. The participants approved the agenda of the meeting.

2. Cyber Security in Finance

Rossen Naydenov from the European Union Agency for Cybersecurity (ENISA) presented key cyber security aspects important for the financial industry. He explained the cyber security regulatory framework and the various new legislative tasks or roles his institution is charged with. Rossen outlined the legislations impacting the finance and focussed on NIS2 (Network and Information Security Directive 2) and DORA (Digital Operational Resilience Act). He emphasised current efforts aimed at addressing existing regulatory fragmentation and duplication to ensure consistency and better alignment of horizontal and sector-specific rules and reporting. Outlining last years' evolution of the threat landscape, Rossen observed that threat actors are consolidating their efforts and cyber-attacks are becoming more sophisticated, shifting from malware, Denial of Service (DoS) or cryptojacking to targeted threats on sectors/groups, vulnerability exploitation targeting supply chains, hybrid threats and information manipulation using deep fake to generate fake voice and videos. Looking at the regulatory reporting on significant network and information security (NIS) incidents, Rossen noted an increase in the number of incidents affecting energy and transportation sectors and highlighted the criticality of Telecoms, electricity and Finance that are the key targets, especially following the Russian invasion in Ukraine, with Telecoms and Finance also having a very high cyber maturity. The incidents occurred mainly due to system failures and malicious actions. Finally, Rossen analysed cyber security investments and noted that the number of FTEs invested in cyber securities has been decreasing from 2020 to 2022. He also indicated that third-party risk management is currently a key area of policy attention.

3. Cyber Security: Cyber Ops and Stress Testing

Sven Bollingh (KBC) presented cyber security from a bank perspective and recalled the main concepts and evolution of cyber security responsibilities both within IT and business. Referring to the NIST framework he described different types of cyber-attacks and ways to address them in line with NIST functions, which are identifying, protecting, detecting, responding, and recovering.

Sven emphasised the role of recovery capabilities from cold back up requiring sound business processes to recover from data losses, and the crucial role of extensive detection and protection capabilities. He highlighted that the sophistication of attacks increased with deep fakes and social engineering benefiting from Artificial Intelligence and cloud and stressed the importance of appropriately protecting Robotic Process Automations, e.g. by segregating their execution in different environments, which are otherwise particularly vulnerable for cyber-attacks.

4. New technologies for wholesale central bank money settlement

Paul Gardin from the ECB's Market Infrastructure and Payment Directorate General summarised the current ECB work on new technologies for wholesale central bank money settlement.

According to feedback received from the market stakeholders in 2022, the market expects significant distributed ledger technology (DLT) based developments in trading and settlement of wholesale transactions within 5-10 years. Despite clear expectations towards the needs that DLT should address, there are still some important questions on its overall impact on the market, adequacy of DLT compared with other technologies or policy changes to meet these needs and required adjustments to the way the financial market functions today.

With its on-going exploratory work, the Eurosystem is exploring concretely these questions further with market stakeholders to contribute to digital innovation and standardisation and to safeguard the role of central bank money while assessing the future role of central bank involvement in potential DLT market structures.

From May until end November 2024, the Eurosystem experiments and trials will further explore the feasibility and desirability of different approaches enabling central bank money settlement of DLT-based transactions, with a focus on cross-platform settlement approaches and the interoperability-type solutions. Other approaches of multiple-asset platforms will be further analysed in parallel to trials and experiments by the Eurosystem.

5. Tour de table questions

In the tour de table, the ECB OMG members discussed cyber security and new technologies for wholesale central bank money settlement, emphasising the following aspects:

A. Cyber Security: Cyber Ops and Stress Testing

ECB OMG members highlighted the importance to focus preventive cyber risk measures not only on internal procedures, systems, and staff, but also on third parties and vendors. In addition to the existing cyber threats encompassing in particular (Distributed) Denial of Services - (D)DoS, ransomware and phishing attacks, ECB OMG members noted rapidly growing occurrences of difficult to detect cyber-attacks applying AI and using deep fake emails/voice messages combined with intelligent social engineering. The participants reported about the value of regular cyber stress testing activities, which include real scenarios, penetration, and resilience tests. The tests also include simulated attacks by external companies, and various exercises together with national central banks, regulatory authorities, and the ECB (e.g. 2024 SSM Thematic Cyber Resilience Stress Test). Cyber security prevention measures include strong management involvement and regular test-phishing exercises, cyber security and resilience trainings and sessions. Some participants indicated that staff members failing in the test-phishing exercises face follow-up actions, such as additional mandatory training or disciplinary measures.

As concerns recovery measures, the members reported business continuity plans that cater specifically for various scenarios involving the loss of availability and integrity of the data with a particular focus on staff awareness, efficient communication channels and assessment of recovery times for systems and infrastructures. Particularly crucial are regular testing of backup procedures for operational processing, the retrieval of outstanding operations, their prioritisation and manual handling of transactions that are otherwise settling automatically.

B. New technologies for wholesale central bank money settlement

ECB OMG members shared their opinions on implications stemming from DLT and wholesale central bank money:

- DLT can bring significant benefits for the financial market, by enabling secure real time transactions, mitigating counterparty risk, and potentially enhancing financial stability, but it is still difficult to assess the scale of final implementation and operating costs and the actual market demand and benefit compared to existing solutions.
- DLT solutions should be carefully assessed to ensure that they are cheaper, more resilient, more efficient than existing solutions.
- Significant challenges in the widespread use of DLT based solutions are seen in interoperability with legacy systems, multiple, simultaneous investments made to address existing market infrastructure and regulation related requirements.
- Many members are monitoring the discussion around DLT since a long time, but only few currently actively participate in experiments and/or trials.

6. AOB

Janusz Ryzner (ECB OMG Secretariat) informed the members about the upcoming review of the FX Global Code and announced that at a later stage, members may be asked to provide their view on the work conducted by the work stream on FX settlement risk.

The next online meeting will take place on 20 June 2024 (guest speaker Pavel Harvanek from the EIB on modern back-office architecture), and a physical meeting on 26 September.