WORLD BANK GROUP
Finance, Competitiveness & Innovation

Financial Sector Advisory Center (FinSAC) Conference on Fintech
May 22-23, 2019, Vienna, Austria

Session 5: Addressing Operational Risk in the Fintech Environment

Panelists:

- Silvia Senabre, Banco de España
- Komitas Stepanyan, Central Bank of Armenia
- Wiebe Ruttenberg, European Central Bank (ECB)
- David Papuashvili, National Bank of Georgia

Moderator: Mario Guadamillas, World Bank

Key Issues for Discussion

I. Cyber-risk: regulatory approach and ensuring information sharing

II. Accountability and coordination

III. Third party providers and outsourcing

IV. Financial Markets Infrastructures (FMIs) and cyber resilience oversight

Regulatory approach and ensuring information sharing

- **How is cyber risk different from other types of operational risk? Is there a need to issue specific laws, regulations or guidelines dealing with cyber risk? Should the principle of proportionality be applied to cyber risk regulations?**
- **How to ensure information sharing across different types of counterparts (IT experts, supervised institutions, supervisors,…) that may require different "lexikons"?**
- **How to properly define risk categories and impact of incidents through a taxonomy (e.g., EBA 2016)?**
- **Should information sharing be voluntary or mandatory? What incentives can be effective for information sharing?**
- **What can be learned from other sectors approach to cyber risk (e.g., ENIA's Cyber Exercise in 2018, aviation sector)?**

Accountability and coordination

- How to ensure that cyber security is not simply considered from a technical point of view but is central to corporate governance of financial institutions?
- What should be the responsibilities of the Board, Senior Management and Information Security Officer (ISO)?
- How to ensure that national cyber security strategies and nominated state agencies in charge of setting minimum standards and intervene in cyber incidents are effective?
- What should be the respective responsibilities of financial sector authorities and national security agencies?
- What should be the role of financial sector regulator vis-à-vis the network of Computer Security Incident Response Team (CSIRT) and Computer Emergency Readiness Team (CERT)?

Third party providers and outsourcing

- **Is it realistic to expect supervised financial institutions to be able to review the ICT controls of so many (including unknown) developers?**
- **What are the particular challenges related to particular services provided by leading technology players such as standard software applications, custom software applications, private cloud or public cloud?**
- **Who should be in charge of regulating and updating cloud providers?**
- **To what extent the reliance on the increasingly homogeneous services of cloud providers contributes to systemic risk?**

FMIs and cyber resilience oversight

- **How cyber resilient are Europe's FMIs? What are the key findings of the ECB's Cyber Survey among 76 FMIs active in Europe (2017 – 2018)?**
- **How do the ECB cyber tools - Cyber Survey, Cyber Resilience Oversight Expectations (CROE), European Red Team Testing Framework (TIBER-EU), crisis communication exercising (UNITAS) and Euro Cyber Resilience Board (ECRB) - interrelate with each other?**
- **What are the main elements of the CROE and how to ensure is not a compliance driven exercise?**
- **What are the main elements of the TIBER-EU Framework? Is ethical hacking of FMIs mandatory?**
- **Strategic dialogue between authorities and FMIs in the ECRB: "we are all victim"**
- **Are authorities and FMIs free to use the cyber tools as developed by the ECB/Eurosystem?**
- **Are the cyber tools as developed by the ECB/Eurosystem entity agnostic, i.e. can these tools be used by and for banks and even outside the financial sector?**