



INTERNATIONAL MONETARY FUND

Middle East Regional Technical Assistance Center

DONORS: | EUROPEAN UNION | FRANCE | GERMANY | SWITZERLAND | THE NETHERLANDS

BENEFICIARIES / CONTRIBUTORS: | AFGHANISTAN | ALGERIA | DJIBOUTI | EGYPT | IRAQ | JORDAN |
LEBANON | LIBYA | MOROCCO | SUDAN | SYRIA | TUNISIA | WEST BANK AND GAZA | YEMEN



The IMF’s Middle East Regional Technical Assistance Center and Monetary and Capital Markets Department conclude Workshop on “Regulatory and Supervisory Approaches to Managing Cyber Risks in the Financial System”

The International Monetary Fund (IMF)’s Middle East Regional Technical Assistance Center (METAC) and the IMF Monetary and Capital Markets Department organized a joint regional workshop on “Regulatory and Supervisory Approaches to Managing Cyber Risks in the Financial System” during October 23-25, 2018 in Amman, Jordan. Eighteen senior bank supervisors from 9 METAC member countries (Afghanistan, Djibouti, Egypt, Iraq, Jordan, Libya, Morocco, Tunisia, and West Bank and Gaza) attended the workshop.

The workshop reported on emerging cyber security trends and measures to handle them. It also provided hands-on capacity building to financial sector supervisors of METAC constituent jurisdictions on preparing quality regulation and efficiently supervising cyber risk.

The workshop provided a forum to exchange views and share country, regional, and international experience on cyber security management. Discussions covered a number of related topics such as the systemic dimension of cyber risk and its potential impact on financial stability, the cyber regulatory frameworks internationally, cyber and third-party risk management, cyber security and the cloud, role of security reviews in building cyber resilience, strategies to promote domestic and cross-border information-sharing, supervision techniques for IT risk and cyber, on-site cyber and IT examinations, including practical experience on inspection in FinTech companies, and the IMF approach to provide technical assistance in that field. The practical case studies provided during the workshop provided an opportunity to build hands-on expertise in understanding and managing cyber-attacks and their management.