



MEFMI
Macroeconomic and Financial Management
Institute of Eastern and Southern Africa



Joint Bank of Tanzania / MEFMI Cyber Security in the Financial Services Sector Workshop

Duration 5 days

Dates 26 – 30 August 2024

Venue Arusha, Tanzania

Language English

Fee USD750 per participant

Early bird USD700 per participant

Registration deadline 12 August 2024

Course fees include training materials, lunch and refreshments on training days and a certificate of completion

Please note that the course fees **exclude** accommodation, airport transfers and transport to and from the venue.

BACKGROUND

The growth of cyber-related threats has increased the level of risk to the ICT infrastructure and services used by organisations to offer services to various stakeholders. The volume and velocity of data traversing and stored in the various ICT networks is of undoubtably immense value and potentially malicious users recognise this. Malicious users' attraction to the data for purposes of financial gain, hacktivism, data exfiltration and for egoistic reasons requires that organisations put in place effective protection mechanisms for the data. IBM and the Ponemon Institute reported that the average cost of a data breach reached a record high of US\$4.45 million, with the financial services sector having the second highest costs for data breaches. The global nature of cybercrime requires concerted approach towards cybersecurity and building resilient cybersecurity frameworks.

COURSE OBJECTIVE

To raise participants' awareness on the motives and methods driving cyber financial crimes and equip them with tools for detection, reporting and prevention techniques as well as necessary internal and external controls management.

EARLY
BIRD FEE
US\$700
PER DELEGATE

Register & pay
by **29 July**
2024 to qualify
for the discount

Discounted rates for group
registration (5 persons and above)

COURSE CONTENT

- Current and emerging cyber financial crime threat landscape and fraud topologies
- Impact of cyber financial crimes on firms and the financial services sector
- Relevant legislation
- Key security methods used to prevent cyber financial crime
- Warning signs of cyber financial crime
- Ethical considerations in financial fraud prevention
- Anti-fraud measures
- Investigating suspected fraudsters
- Investigations into social media, malware, viruses, and ransomware

TARGET GROUP

Senior and middle level professionals in the following departments/units: ICT, ICT security, internal audit, risk management, security, legal, regulatory compliance, operations and finance.

FOR FURTHER DETAILS AND REGISTRATION CONTACT

Email: Sharon.Wallett@mefmi.org / bdu@mefmi.org

Landline: +263-242-745988-94

Mobile: +263-772-216-515

