

# THE INSTITUTE OF FINANCE MANAGEMENT



## FACULTY OF COMPUTING, INFORMATION SYSTEM & MATHEMATICS

### Tutorial Set 2

03/01/2026

**In a group of 6-7 members,**

**Read the below case study and answer the question below.**

You have been assigned to assess IFM computer labs Operational & Physical Security status. The second task you are required:

- i. As part of a IFM cyber security team audit, you are asked to assess weaknesses at IFM computer Laboratory's operational security (OPSEC). Draft a brief operational security protocol that addresses insider threats, secure information handling, and incident logging. Highlight three key risk mitigation strategies embedded in your design
- ii. Simulate a threat scenario where poor physical security compromises system integrity at IFM computer Labs (e.g., stolen hard drive, computer, broken monitor). What are five security failures that occurred and how could they have been prevented.
- iii. A malicious actor gains after-hours access to computer lab serve room due to a failed of physical security authentication system. Evaluate the chain of operational failures that contributed to the breach. Propose a revised access control strategy integrating physical and digital controls using current best practices.

**Deadline for submission: 09/01/2026 at 5:00pm via email: isaac.mutama@ifm.ac.tz**