IT Risk Management: Information Security

This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

Agenda – Purpose of Presentation

- Recognize focus of information security programs
- Identify elements of an effective information security program.
- Describe what constitutes a security breach and recognize examples of breaches.

Information Security and Cyber Security

- Information security remains a significant input into the overall assessment of a firm’s IT environment.

- Cybersecurity, on the other hand, has close ties to information security and the technology infrastructure but has begun to be viewed as a systemic and far-reaching risk spurred on by near-daily headlines.

- Information security emphasis is on **information** availability, confidentiality, integrity, assurance, and accountability.

Information Security

- An effective information security program enables banks to meet business objectives by considering:

Objectives	Summary
Availability	The processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
Integrity	The procedures, policies, and controls that ensure information is not altered in an unauthorized manner, as well as systems, are free from unauthorized manipulation that compromises accuracy, completeness, and reliability
Confidentiality	The processes, policies, and controls employed to protect the information of customers and the institution against unauthorized access or use
Accountability	The processes, policies, and controls necessary to trace actions to their source
Assurance	The processes, policies, and controls used to develop confidence that technical and operational security measures work as intended

Elements of an Information Security Program

Element	Summary
Risk assessment	To identify the customer information assets, both physical and electronic, their location, and the controls in place to protect them and determine where there are exposures
Information security policy	To outline the practices and controls expected to protect the customer information identified in the risk assessment
Training	To ensure employees receive adequate training so they can uphold the controls outlined in the policy
Testing	To ensure that employees are following the practices as outlined and that the controls in place are effective
Board reporting	To inform the board annually on the program, including any major changes in the risk assessment or controls implemented by the policy

Access and Identity Management

- Access commensurate with job responsibility and business need
- Established process for granting, reviewing, and removing system access
- Monitoring of access levels and activity important to limiting:
  - fraud
  - Mishandling of customer information
  - Intentional or inadvertent viewing
  - Insider threats

Incident Response and Management

- Incident response plans:
  - should outline the protocol for notification, communication, and response if an incident occurs
  - are not unique to cybersecurity, as they have been used as part of the GLBA to ensure that financial institutions have a plan of action to address breaches of customer information
  - should address how to preserve forensic evidence, as well as how to ensure that the attack is over and the system or network has been secured
  - should ensure testing is conducted and that staff are aware of their roles and responsibilities
  - consider events occurring at third parties

Supervisory Considerations When Incident Occurs

- Is the incident contained? If not, ask to receive regular reporting until it is.

- Has the management team analyzed the situation? If contained, identify lessons learned and actions to address any known vulnerabilities.

- Have consumer compliance counterparts been alerted to incidents in which customer information was compromised or cards were reissued?