Con..Chapter 4

Analysis and Management of Banking Risks in Commercial Banks

Fourth: The Fundamental Principles of Banking Risk

The key principles essential for banking risk management are summarized as follows:

1. Responsibility of the Board of Directors and Senior Management: The responsibility for risk management primarily falls on the board of directors of each bank..

Fourth: The Fundamental Principles of Banking Risk

..which is accountable to shareholders for the bank's operations. The board must understand and be aware of the nature of the risks the bank faces and ensure they are managed effectively and efficiently.

Fourth: The Fundamental Principles of Banking Risk

2. Establishing the Risk Management Framework "Risk Management Strategy": The board of directors must approve the risk management strategy and encourage management to rationally handle risks within the bank's overall strategies and policies, working to avoid risks that are difficult to assess.

Fourth: The Fundamental Principles of Banking Risk

3. Integration of the Risk Management Process: Every bank should have an independent "Risk Management Committee," which includes some of the bank's executives and is responsible for identifying and implementing risk management policies without focusing solely on one type of risk.

Fourth: The Fundamental Principles of Banking Risk

4. Defining Responsibilities for Risks Associated with Banking Activities: Banks offer a variety of banking activities, including retail banking, corporate banking, and securities trading, each associated with numerous risks that affect the bank's performance and profitability.

Fourth: The Fundamental Principles of Banking Risk

5. Defining Methods for Measuring and Assessing Risks:

This principle emphasizes the need for a defined methodology and system for measuring and monitoring risks within the bank. The goal is to accurately measure and determine the impact of each type of risk on the bank's profitability and capital adequacy.

Fourth: The Fundamental Principles of Banking Risk

6. Audit Independence: The audit function must be independent and have full authority to carry out its duties. The goal is to ensure a clear separation between individuals and functions involved in making decisions related to identifying and measuring banking risks and those involved in monitoring and evaluating these risks.

Fourth: The Fundamental Principles of Banking Risk

7. Establishing Information System Security Controls:

Adequate controls must be in place to ensure the security of all information systems, preserving the accuracy, integrity, and confidentiality of information through reviews of all major systems by qualified external parties.

Fourth: The Fundamental Principles of Banking Risk

8. Establishing Contingency Plans: The bank's management must establish contingency plans that can be implemented in the event of changes in the bank's environment. These plans should cover all types of risks the bank may face in the future and should include preventive measures against crises, with approval from relevant authorities.

Activity No. (1)

- **Activity nature:** Discussion.
- **Activity Time:** 5 minutes.
- **Task:** Discuss The Principles of Banking Risk Managmet

5 minute break.....

Tea Break

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

The terms cyberattacked and cybersecurity have become widespread. With the growing discussions among information security experts, many questions have arisen about the nature of cyber risks, what cybersecurity is, whether information security is a part of cybersecurity, and the differences between the two.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

1. The Concept of Cyberattack Risks: Many terms describe the risks of cyberattacks, such as computer risks, electronic risks, information risks, IT risks, or internet risks. All these terms refer to the evolution of different patterns of information technology risks and the significant impact of technological advancements in information programming.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

A simple definition of cyberattack risks could be: "The risks targeting the disruption of computer systems or unauthorized access to recorded data and information for malicious purposes, such as theft, manipulation, espionage, fraud, hacking, or otherwise."

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

Below is a brief overview of the major cyberattacking risks considering applying digital transformation strategies in commercial banks:

- **Data and Information Security Risks:** Digital technology helps collect and store vast amounts of data, which can include private information related to individuals or institutions.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- **Privacy Breach Risks:** Maintaining personal privacy in the digital world has become more difficult, along with the growing risks of personal data theft or compromise.
- **Anonymity Risks:** Digital technology offers a broad space for users to conceal their identities, and many studies indicate that people are more likely to behave antisocially if they do not believe there will be consequences.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

2. The Concept and Areas of Cybersecurity: "all procedures, measures, technologies, and tools used to protect the integrity of networks, software, and data from attack, damage, or unauthorized access, including the protection of physical devices and databases." It is also defined as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

There are six general areas of cybersecurity:

- **Network Security:** The practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application Security:** A compromised application can provide access to the data it was designed to protect. Successful security begins in the design phase..

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- **Information Security:** Ensuring the integrity and privacy of data, both in storage and during transmission.
- **Operational Security:** The processes and decisions for handling and protecting data assets. Permissions that users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- **Enhancing Organizational Recovery from Cyberattacks:**

  Disaster recovery and business continuity determine how an organization responds to cybersecurity incidents or other events that cause the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operational capacity as before the event.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- **End-user Training (People):** The most unpredictable factor in cybersecurity. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, avoid plugging in unidentified USB drives, and many other essential lessons is vital to the security of any organization.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

3. Cybersecurity Objectives: The key objectives of cybersecurity can be summarized as follows:

- **Enhancing the protection of operational technology systems at all levels and components, including hardware, software, services, and data.**

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- Countering information security attacks and incidents targeting government agencies and public and private sector institutions.
- Providing a secure and reliable environment for interactions in the information society and the digital age.
- Ensuring the resilience of critical infrastructure to cyberattacks.

Fifth: Cybersecurity Risks (Concept and Objectives – Legislative)

- Providing the necessary requirements to reduce risks and cybercrimes targeting users.
- Eliminating vulnerabilities in computer systems and mobile devices of all types.
- Addressing and resolving gaps in information security systems.

Presentation activity……..

- **Activity nature:** Presentation.
- **Activity Time:** 10: 12 minutes.
- **Skills:** Professional financial analysis

The Next Lecture

Chapter 5

Models for evaluating the creditworthiness of banking institutions