
# Information and Technology Management Governance Manual

# Introduction

Following Jordan Commercial Bank's commitment to the security of its operating environment and utilizing best international practices in the management of information technology resources, projects, and services in a manner that enables it to conduct business and achieve its strategic objectives effectively and efficiently. This, in turn, reflects positively on the bank's product and service quality on the one hand, and on the decision-making and risk management mechanisms on the other. Apart from upholding the banking system's integrity and adhering to international standards for sound banking practices, the bank recognizes the importance of adhering to the highest standards in the field of information and related technology.

The Board of Directors and the Executive Management have realized the need to adopt successful products that require the application of information technology in an efficient and effective manner along with the various practices and work procedures of the Bank in a manner that calls for a framework and principles of governance and management of information and related technology. Separating the operations, tasks and responsibilities of the Council in the field of governance from those that fall within the limits of the executive management’s responsibility regarding information and accompanying technology and following the sound foundations and standards in managing information technology resources according to international best practices, especially the COBIT framework to control risks and reach the aspirations of stakeholders by applying the rules of governance sound. In order to avoid entering into useless investments and unjustified expenses that translate into huge losses, which may in some cases affect the bank’s reputation and performance.

This guide has been prepared and attached to the Corporate Governance Guide in order to confirm the identity of the Jordan Commercial Bank, and it expresses the bank's view of the governance and management of information and related technology in terms of its concept, importance, and basic principles in a manner that takes into account legislation and international best practices, and it emphasizes the bank's commitment to all laws and regulations issued in this regard.

The provisions of this guide apply to Jordan Commercial Bank branches in Jordan. The bank publishes the information technology governance guide on its website and is committed to disclosing the guide and the extent of its commitment to implementing what is stated in it in its annual report.

# Chapter One: Information Technology Governance, Scope and Objectives

First: Governance:

Planning for the purpose of achieving strategic objectives, including alignment and regulation, construction and development activities, including procurement and implementation, operating activities, service delivery and support, and monitoring activities, such as measurement and evaluation, are all part of the management of information and related technology. Considering this, information governance and the technology that supports it defines the process of assigning roles and responsibilities and describing relationships between parties, entities, and stakeholders with the goal of maximizing the bank's added value by taking the best approach that ensures a balance of risks and expected returns. And by adopting the rules, foundations, and mechanisms required for decision-making, defining the bank's strategic directions and objectives, and mechanisms for monitoring and examining the extent of compliance to achieve them in the pursuit of continuous progress and development, through the governance of operations, which is linked to the set of practices and activities emanating from the bank's policies and required to achieve the information and accountability objectives, These goals, which are derived from institutional goals, are broken down into main goals and sub-goals in order to meet the needs of stakeholders.

Any person with an interest in the bank, such as shareholders, employees, creditors, customers, external suppliers, or regulatory authorities involved in the bank's activities, is referred to as a stakeholder.

Second: Scope of Information Technology Governance and the Concerned Parties:

The information technology governance instructions apply to all of the bank's information technology-based operations in its various branches and departments, and all stakeholders are considered to be affected by the application. The Bank has launched a project to create the necessary environment and meet the requirements of the Information Technology Governance Instructions in accordance with the (COBIT) framework, and there are roles for each of the following:

- The president, board members, and external experts are in charge of the project's overall direction, assigning tasks and responsibilities, providing support, and approving the necessary funding.
- The general manager, his deputies, assistants, and operations managers must identify and define competent people with experience in the bank's operations to represent them in the project.
- Executive management and managers in charge of information technology operations and procedures. The Information Technology Steering Committee directs and submits the necessary reports to the Information Technology and Cyber Security Governance Committee of the Board of Directors, project managers are followed up on, taking into account the availability of sufficient resources and a thorough understanding of the institutional objectives of information technology governance.
- The internal audit committee is also tasked with providing independent advice and monitoring for the success of the implementation in executive matters as an independent consultant and observer to facilitate and succeed in completing the institutional control framework by reviewing information technology audit reports, taking the necessary steps to address deviations, monitoring the level of technical and technological services, and working to raise their efficiency. The Audit Committee of the Board of Directors, on the one hand, and the external auditor, on the other, submit annual reports to the Central Bank of Jordan for internal and external audits, respectively. During the first quarter of each year, the Executive Management responds to the briefing and recommendations of the Council in this regard.
- The project's risk, information security, compliance, and legal departments are committed to representing their departments' roles, implementing the framework, following up on requirements, adhering to objectives and policies, and maintaining an appropriate control environment.
- The bank relies on experts and holders of technical and professional certificates related to the standard (COBIT Foundation, COBIT Assessor, COBIT Implementation, CGEIT) from both inside and outside the bank to act as guides and assessors during the application process, as well as to spread knowledge of the standards and make the compliance process easier.
- When signing outsourcing agreements with third parties to provide human resources, services, programs, and infrastructure for information technology with the goal of running the bank's operations, the bank must ensure that third parties follow the IT governance instructions in whole or in part to the extent that is proportionate to the importance and nature of the bank's operations, services, programs, and infrastructure. The ultimate responsibility for achieving the

requirements of the instructions under consideration, including the audit requirements referred to in this guide, remains with the Board and Senior Executive Management.

Third: Objectives of Governance and Information Management and Related Technology:

The primary objective of IT governance is to "create added value" for the bank by maximizing the use of information technology, preserving, and increasing the value provided by current investments, and eliminating IT initiatives and assets that do not contribute to the creation of sufficient added value for the bank. This means maximizing resource utilization while minimizing risk, in addition to addressing the business risks associated with the use of information technology, its ownership, operation, adoption, and inclusion in the bank. This is to ensure the existence of appropriate capabilities to implement the strategic plan, providing sufficient, appropriate, and effective resources, and reconciling in the decision-making process between stakeholders' interests towards added value on the one hand, and comparing risks with returns through optimal utilization on the other.

Accordingly, the objectives that the Bank seeks to achieve by adopting an IT governance framework are:

1. Meeting the Stakeholder’s needs by achieving the objectives of information and related technology, ensuring:
• Providing high-quality information that serves as a foundation for the bank's decision-making processes.
• Prudent management of information technology resources and projects, with an emphasis on maximizing resource utilization and minimizing waste.
• Establishing a distinct and supportive technological infrastructure that enables the bank to accomplish its objectives.
• Improving the bank's various operations using an efficient technological system with a high credit rating.
• Prudent management of information technology risks to ensure the bank's assets are adequately protected.
• By strengthening the bank's internal control and control systems, it will be easier to comply with the requirements of laws, legislation, and instructions, as well as the internal strategy, policies, and procedures.
• Improving the system of control and internal monitoring.
• Increasing users' satisfaction with information technology by efficiently and effectively meeting business needs.
• Managing third-party services entrusted with the execution of operations, tasks, services, and products.
2. Providing the necessary components to achieve comprehensiveness in the governance and management of information and related technology.
3. Adopting business and organizational practices and rules based on the best international standards as a foundation for future development in the areas of governance and management of information technology operations, projects, and resources.
4. Separate the board's operations, tasks, and responsibilities in the field of governance from those that fall under the executive management's responsibility for the information and technology that goes with it.
5. Strengthening self-monitoring, independent oversight, and compliance examination mechanisms in the areas of governance, information management, and related technology, which contribute to continuous performance improvement and development.

Governance and management objectives, as well as the other six components related to cybersecurity, risk management, privacy and data protection, compliance, monitoring, auditing, and strategic alignment, are (Focus Areas) of high importance and priority.

## Chapter Two: The Bank's Governance and Information Management Framework and Related Technology (COBIT) and Components

### First: Principles of Information Technology Governance:

The main principles of information technology governance enable the bank to create an effective governance and management framework that maximizes the use of data and technology investments. According to the COBIT framework, the following are the main principles of information governance and management, as well as related technology:

#### 1. Meeting Stakeholder Needs (Provide Stakeholder Value):

The bank's primary objective is to add value to stakeholders and thus achieve benefits at the lowest possible cost of resources.

2. Holistic Approach:
A comprehensive system of corporate governance and IT management system is implemented.

1. Dynamic Governance System:
The Bank's governance system is dynamic and subject to change.

4. Tailored to the enterprise needs:
The Bank's governance system is designed to meet the needs of the organization by setting priorities.

#### 5. Separating Governance from Management:

The board of directors is responsible for ensuring that the bank follows good corporate governance practices and that the roles of the board and executive management are clearly defined. The general manager's and other executive management cadres' responsibilities include planning, construction, operation, and monitoring activities, as well as aligning them with the board of directors' directions in order to achieve the bank's strategy objectives.

6. Covering the Enterprise End-to-End:
Technology governance works to create an integration between information technology governance and corporate governance, covering all functions and operations within the bank.

### Second: Components:

In terms of information governance and management, comprehensiveness is achieved by considering not only the technology itself, but also the provision of 7 Components that accompany and complement the information technology services represented by the following:

1. Principles, Policies, and Frameworks are tools for translating desired behaviors into daily management guidelines.
2. Processes are an organized set of practices and activities used to achieve specific goals.
3. Organizational Structures.
4. Culture, Ethics and Behavior, through the Bank's system of values, ethics, and behaviors.
5. Information, which includes all information generated and used by the Bank and is required for the Bank's proper operation and governance.
6. Services, programs, infrastructure, and applications that support information technology processing and facilitate the provision of services.
7. People, Skills, and Competencies are required for all activities to be completed successfully and for the right decisions and actions to be taken.

The Bank is committed to activating the 7 Components in order to achieve the existing comprehensiveness of the general framework for information technology governance.

When implementing and entering the details of the 7 Components, attachments, operations, and sub-goals, the Bank adapts (tailors) all of this in accordance with the Bank's data in order to serve the objectives and requirements of the Information Technology and (COBIT) Governance Instructions and work to find the required change to provide and create the necessary environment for the application by using the Gap Analysis method between the current situation and the application's requirements. The bank has committed to sending the Central Bank of Jordan a semi-annual achievement report detailing compliance with COBIT requirements and describing the level of achievement.

Third: Information Technology Governance Operations:

The general framework for the application of information technology governance (COBIT) consists of two main areas of operations:

1. The scope of the Board of Directors' operations is as follows: It can be broken down into five steps. Each process defines evaluation, direct, and monitor practices, abbreviated (EDM5), which ensures the development and maintenance of an IT governance framework, the realization of benefits, risk management, ensuring optimal resource utilization, and dealing transparently with stakeholders.

2. The scope of the executive management process is as follows: It has four axes that correspond to the areas of responsibility: Planning, Build, Operate, and Monitor, abbreviated as PBRM. These axes provide a thorough examination of the scope of information technology governance. The names of the axes have been chosen in corresponds with their initial meaning:

- Alignment, Planning, and Organizing (APO): is responsible for developing the bank's information technology policy, IT strategy, organizational structure development, financial management, and investment portfolio management.
- Build, Acquisition, and Implementation (BAI) is the process of conducting business analysis, project management, evaluating usage scenarios, defining, and managing requirements, programming, systems engineering, decommissioning systems, and capability management.
- Delivery, Service and Support (DSS): It manages availability, problem management, service desk and incident management, security, IT operations, and database management.
- Monitoring, Evaluation and Assessment (MEA): It stands for compliance review (conformance), efficiency control, and control auditing.

The Bank is committed to ensuring the successful implementation of the axes and processes described to ensure the proper application of information technology governance.

Fourth: Levels of Maturity and Capacity of Actions:

There are six levels through which procedures can be classified for the purposes of improving procedures, assessing process maturity, determining the target level, and identifying deviations:

- Level (0) Incomplete process: There are no clear processes in place, so the bank is unaware that there is a problem that needs to be addressed.

- Level (1) Performed process: The bank recognizes that there is a problem that needs to be addressed, but there are no standard procedures; rather, there are approaches tied to a specific purpose that are used on an individual or case-by-case basis. The bank's management approach is disorganized in general.

- Level (2) Managed process: Processes develop to the stage where similar procedures are followed by different individuals performing the same task, there is no formal training or dissemination of standard procedures. Responsibility is left to the individual, and there is a high degree of reliance on people’s know-how; as a result, mistakes are possible.

- Level (3) Established process: The procedures are documented and identified as standard procedures, then published in the bank through training, with the documentation stating that they must be followed, but deviations are unlikely to be detected.

- Level (4) Predictable Action: Management monitors and measures policy compliance and intervenes when processes appear to be failing; actions are subject to continuous improvement and provide a mature experience to others; and automation and tools are used in a limited or fragmented manner.

- Level (5) Improved Procedure: At this level, procedures have been revised to achieve best practices status, based on the results of continuous improvement and the development of maturity models in collaboration with other institutions, as well as the Bank's ability to adapt quickly.

According to the quantitative and qualitative study results, the level of maturity of the activities related to the objectives of information technology governance and the rest of the six Components associated with them is directly proportional to the degree of importance and priority. The bank also strives to ensure that the maturity level of important and priority activities is at least level (3) (Fully Achieved) according to the maturity scale contained in the framework (Cobit)*, and the bank always strives to achieve higher levels than the required maturity level.

---

* It is possible to consider no more than (26%) of the goals of governance and management within the administration's goals (with no more than 9 goals and a maximum of 35 goals) as being of lower or neglected

## Chapter Three: The board of directors' role in information and technology management

The roles, activities, and relationships define the stakeholders in governance and how they are involved in the implementation process. One of the most critical principles underlying information technology governance is the separation of the board of directors' and executive management's responsibilities. By determining how to communicate between the owners' interests and executive management, a distinction is made between the board of directors' role and the executive management's activities. The following are the tasks and responsibilities of the research entities:

1. Duties and Responsibilities of the Board of Directors:

- Monitoring senior executive management's work to ensure the effectiveness and efficiency of operations, the accuracy of financial reports, and the extent of compliance with current laws, legislation, and instructions, as well as the "risk management" process.
- Budgets are monitored and necessary tools and resources, including qualified human resources, are allocated through departments specializing in information technology auditing. Assuring that both the internal audit department of the bank and the external auditor are capable of reviewing and auditing the processes for hiring and managing information technology resources and projects, as well as the bank's operations based on them. Additionally, the presence of a specialized technical audit (IT Audit) conducted by qualified and internationally accredited professional cadres in this field who hold valid professional accreditation certificates such as (CISA) issued by qualified international associations in accordance with the international accreditation standards for certification institutions (ISO/IEC 17024) and / or any other equivalent criteria.
- The Council adopts the system of principles, policies, and frameworks required to achieve the general framework for managing, monitoring, and controlling information technology and cyber security resources and projects in a way that meets the requirements of information technology governance objectives and processes related to information technology risk management and information technology security and protection management through the Information Technology Governance Committee. They also adopt human resource management that meets the requirements of information technology governance processes, as well as the policies required to manage information technology governance resources and processes, and to work with these policies in conjunction with the bank's other policies that regulate its work and align goals, work mechanisms, and related work procedures, penalties for noncompliance, and compliance mechanisms. All internal and external partners' input is considered when developing policies, as is the adoption of international best practices and their updates.

- Adopting organizational structures (hierarchies and committees) for managing information technology resources, processes, and projects, managing information technology risks, information security, and human resources that comply with information technology governance processes and efficiently and effectively accomplish the bank's goals, while ensuring task separation and bilateral control are kept to a minimum, adequacy, and up to date.
- Develop the infrastructure and information systems necessary to provide information and reports to its users as a basis for the bank's decision-making processes. The information quality requirements of integrity, accuracy, and currency, as well as the confidentiality requirements of the data classification policy, as well as the requirements for availability and compliance with that information and reports, must be met, in addition to other requirements contained in COBIT and Information Enabling.
- The Board, through the Information Technology and Cyber Security Governance Committee, adopts and considers the information and reports system as a minimum, considering those responsible for developing the information and reports, as well as the powers of access and use that are delegated according to the need for work and the relevant partners. The information and reports are reviewed and updated on a regular basis to ensure that they keep up with the Bank's goals and operations, and that they adhere to accepted international best practices.
- The Board, through the Information Technology and Cyber Security Governance Committee, adopts a system of information technology services, programs, and infrastructure that support and assist in achieving information technology governance processes and, as a result, the information and technology objectives that accompany it as well as institutional objectives. The Board considers that system to be a minimum, and it is continuously developed to keep pace with the evolution of the goals and operations of the Bank, in accordance with the best accepted international practices. technology.
- The Council adopts the qualifications matrix (HR Competencies) and human resources management policies necessary to achieve the requirements of information technology governance processes based on merit through the Information Technology and Cyber Security Governance Committee and the Nominations and Remunerations Committee by adhering to the methods of incentives and penalties.
- The Council, through the Information Technology and Cyber Security Governance Committee and the Audit Committee, adopts a professional and institutional ethical system that reflects the widely accepted international professional code of conduct for dealing with information and the technology that supports it, and that clearly defines desirable and undesirable behavioral rules, as well as their consequences.

2. <u>IT and Cyber Security Governance Committee:</u>

An Information Technology and Cyber Security Governance Committee, consisting of four members of the Board of Directors with experience and strategic knowledge in IT, was formed by decision of the Board of Directors to meet the tasks required of the aforementioned Board. A Chairman of the Committee was chosen from among the four members, it meets quarterly at the least, keeps records of minutes of meetings, and submits periodic reports to the Board. The Committee's responsibilities are summarized as follows:

- Ensuring alignment and compatibility between the Jordan Commercial Bank's general strategic plan and the Information Technology Department's strategic plan to achieve the bank's strategic objectives.
- Assuring that information technology services are used in a way that helps to reduce risks.
- Following up on performance indicators and monitoring the general strategy's implementation and realization, project progress, resource utilization, service delivery quality indicators, and balanced goal cards that reflect strategic goal achievement.
- Assuring that available resources are best utilized, whether they are sensitive systems, information, IT infrastructure, or employees.
- Relying on the strategic goals of information technology and cybersecurity governance, and appropriate organizational structures including steering committees at the senior executive management level, especially the IT and Cybersecurity Steering Committee, to ensure the achievement and fulfillment of the bank's strategic objectives and to achieve the best added value from information technology projects and investments, and using the necessary tools and standards to monitor and ensure its achievement, such as using IT Balanced Scorecards and calculating Return On Investment (ROI), and measuring the impact of contribution to increasing financial and operational efficiency.
- Adopting a general framework for managing, controlling, and monitoring information technology resources and projects that is modeled after best international practices, in particular (COBIT 2019), which aligns with and meets the achievement of the instructional objectives and requirements by achieving sustainable institutional goals, and achieving a matrix of compliance objectives covering governance and management objectives.
- Adopting the matrix of institutional objectives, compliance objectives, considering them as a minimum threshold, and describing the necessary sub-goals to achieve them.
- Adopting a Responsibilities Matrix (RACI Chart) towards the key operations of governance and management objectives and their resulting sub-operations in terms of the entity, entities, person, or parties primarily responsible, those ultimately accountable, those to be consulted, and those to be informed regarding all operations in the facility, guided by the COBIT 2019 standard in particular.
- Ensuring the existence of a general framework for managing information technology risks that aligns and integrates with the overall general framework for risk management in the bank, taking into consideration and fulfilling all governance and management objectives.
- Approving the information technology budget and projects in accordance with the Bank's strategic objectives.
- General oversight and review of information technology operations, resources, and projects to ensure their adequacy and effectiveness in meeting the bank's requirements and business objectives.
- Reviewing the audit reports for information technology and taking the necessary measures to address the deviations.
- Recommending to the Council that any deviations be corrected as soon as possible.
- Reviewing and adopting the cybersecurity policy and program by the board of directors, supervising, and ensuring its compliance and identifying the roles and responsibilities related to cybersecurity.
- Ensure the establishment of a system and mechanism for managing third-party services to support the bank's service delivery process.
- The IT and Cybersecurity Governance Committee ensures the independence of the Information Security Unit, which administratively reports to the Risk Department. The Steering Committee reviews the minutes of the meetings, which include periodic reports prepared by the Information Security Unit and submitted to the IT and Cybersecurity Governance Steering Committee. These reports cover cybersecurity in the bank, deviations related to the application of the cybersecurity policy and its procedures, the results of cybersecurity risk assessments, the results of assessments of the adequacy and effectiveness of the cybersecurity program and policy, and

recommendations, actions, and requirements for implementation. A summary of the most important cybersecurity threats and breaches during the reporting period is also included.
- Prioritize the objectives of governance and management and assess their alignment with institutional and compliance objectives, as well as their relationship with the other six components. This should be based on a qualitative and/or quantitative study conducted for this purpose at least annually, considering the design factors included in COBIT 2019 - Design Guide.
- Approve the annual audit report assessing the information and technology risks and controls associated with them for the bank.
- Continuously monitor and approve the level of cybersecurity risks and the bank's ability to tolerate them, ensuring that overall cybersecurity risks are within an acceptable range.
- Ensure that the bank has a cybersecurity awareness program and that it is aware of the legal and regulatory implications of cybersecurity risks.
- Allocate sufficient budget and resources to meet cybersecurity requirements.
- Support and participate in cybersecurity risk resilience assessments and any cybersecurity initiatives.

3. Audit Committee:

- Included are the responsibilities, powers, and scope of information technology audit work within the Audit Charter on the one hand, and procedures agreed upon with the external auditor on the other, as well as regulatory requirements.
- Confirming to the Board that the bank's internal auditor and external auditor are committed to the following when conducting specialized audits of information and related technology:

1. Information technology auditing standards according to the latest update of the international standard) Information Technology Assurance Framework (ITAF) issued by the Audit Association and Information Systems Control (ISACA), including:

● Conducting audit tasks in accordance with an approved plan that considers the relative importance of operations, the level of risk, and the degree of influence on the bank's objectives and interests.
● Providing and adhering to training and continuing education plans by the specialized staff in this regard.
● Adhering to professional and organizational standards of independence, as well as ensuring that current and future interests do not conflict.
● Commitment to objectivity standards, due professional care, and continuous improvement of the competitiveness and professionalism of the knowledge and skills to be enjoyed, as well as a thorough understanding of the bank's various mechanisms and processes based on information technology and other audit reports (financial, operational, and legal). Capacity to provide evidence that is appropriate for the situation, as well as common sense in identifying unacceptable practices that violate applicable laws, regulations, and instructions.

2. Examining, evaluating and reviewing the processes of hiring and managing information technology resources as well as the bank’s operations based on them, and providing a public opinion (Reasonable Overall Audit Assurance) on the overall level of risks to the information and related technology within an audit program that includes at least the required axes, bearing in mind that the risk assessment degrees are divided in descending order into five Levels (which are the Composite Risk Rating Scale): Rate 1) Strong Performance Rate; Rate 2) Satisfactory Performance Rate; Rate 3) Fair Performance Rate; Rate 4) Marginal Performance Rate; Rate5) Unsatisfactory Performance Rate.
And the audit should be repeated for all or part of the axes at least once a year if the risks were rated at (5 or 4) on the risk assessment scale, at least once every two years if the risks were rated at (3), and at least once every three years if the risk was rated at (2 or 1).
Considering the continuous change in the risk level and the fundamental changes that occur in the information environment and related technology over the audit periods specified, provided that the Central Bank receives audit reports. The audit reports include assessments of the axes mentioned above, as well as the mechanisms used for strategic planning and developing policies, principles, and procedures, and for utilizing various resources, including information technology and human resources, mechanisms and tools for monitoring, improvement, and development. As well as work on documenting and evaluating audit results based on the significance of imbalances and weaknesses due to observations. In addition to active controls and assessing the level of residual risks using a systematic standard for analyzing and measuring risks, the corrective measures agreed upon and intended to be followed by the bank's management with specific dates for correction are included, along with a reference table that ranks the responsible person in the bank concerned with the observation. During the first quarter of each year, the Central Bank of Jordan

must be provided with an annual report for internal audit and another for external audit, which includes the response of executive management, the briefing, and recommendations of the Board in this regard, and according to an audit report form (risks - controls) of the information and accompanying technology.
3. Regular procedures to follow up on audit results to ensure that the observations and imbalances contained in the auditor's reports are addressed within the specified timeframes, as well as work to gradually raise the level of importance and risks in the event.
4. Include annual performance evaluation mechanisms for IT audit cadres with objective measurement criteria, if evaluations are conducted by the Council, represented by the audit committee that emanates from it, and in accordance with the administrative and organizational hierarchy of the audit departments of non-response, as determined by the Board.
5. The internal auditor and the external auditor must follow the system of ethics and professional practices outlined in the International Standard (Information Technology Assurance Framework) (ITAF) issued by the Information Systems Audit and Control Association (ISACA) and its updates.

The bank may delegate the Internal IT Auditor role for information and related technology to a specialized third party (outsource) independent of the accredited external auditor, provided that all requirements of the IT governance instructions and any other applicable instructions are met, and the Board of Directors and its Audit Committee retain their role in ensuring compliance and meeting minimum requirements.

## Chapter Four: Executive management's role in managing information and related technology.

1. Responsibilities and tasks of the executive management:
- Hiring qualified and trained personnel with experience in information technology resource management, risk management, information security management, and information technology audit management, based on academic and professional knowledge and practical experience recognized by qualified international associations under the international accreditation standards for professional certification institutions (ISO/IEC 17024) and/or any other standards, each according to its competence and in accordance with the bank's policies. As well as to provide continuous training and education to employees to maintain a level of knowledge and skills that complies with and supports information technology governance processes.
- Adopting a system of information technology services, programs, and infrastructure that supports and assists in the achievement of information technology governance processes and, as a result, the associated information and technology objectives, institutional goals, and providing and developing them on an ongoing basis to keep pace with the bank's goals and operations in accordance with internationally accepted best practices.
- Include annual performance evaluation mechanisms for cadres with objective measurement criteria that consider the contribution of the job position to the achievement of the bank's goals.
- Develop the infrastructure and information systems necessary to provide information and reports to its users as a basis for decision-making processes within the bank, and in doing so, the information quality requirements such as integrity, accuracy, and currency, as well as the confidentiality requirements, must be met in accordance with the data classification policy, as well as the availability and compliance requirements for such information and reports (COBIT - Enabling Information).
- Using incentives and penalties, various mechanisms are used to encourage the application of desirable behaviors and to avoid undesirable behaviors.

2. IT and Cyber Security Steering Committee:
To achieve the Bank's strategic objectives in a sustainable manner, an Information Technology and Cyber Security Steering Committee was formed to oversee the process of strategic information technology compatibility. The Chairman of the Committee, the General Manager, and members of the executive management, including the Director of Information Technology, the Director of Risk Management, and the Director of Information Security, are all members of the committee. A member of the Board was also elected to be an observer member of this committee in addition to the General Auditor in an observer capacity, who can invite others when needed to attend the meetings. The

committee keeps minutes of its meetings, which are held at least once every three months. The committee's responsibilities are summarized as follows:

1. Develop annual plans to ensure that the Board's approved strategic goals are met, supervise their implementation to ensure that they are met, and continuously monitor internal and external factors that affect them.
2. Connecting the institutional objectives matrix to the accompanying compatibility objectives matrix, approving, and reviewing it on an ongoing basis to ensure the bank's strategic objectives are met, as well as the objectives of governance instructions and information and related technology management, while considering the definition of a set of measurement and review criteria and assigning those responsible from the executive management to monitor the results.
3. Recommending the allocation of financial and non-financial resources required to achieve the goals and information technology governance processes, as well as the use of competent and appropriate human resources through organizational structures that include all processes required to support the goals, taking into account task separation and the absence of conflict of interests, and the adaptation of technological infrastructure and other services related to it to serve goals, as well as oversee the implementation of IT projects and governance processes.
4. Arranging IT projects and programs in order of priority.
5. Monitoring the level of technical and technological services and working to raise their efficiency and improve them continuously.
6. Submitting the necessary recommendations to the IT Governance Committee regarding the following matters:
- Allocating the resources and mechanisms required to achieve the tasks of the IT and Cyber Security Governance Committee.
- Any deviations that may negatively affect the achievement of strategic objectives.
- Any unacceptable risks related to technology, security, and information protection.
- Performance reports and adherence to the general framework for managing, controlling, and monitoring IT resources and projects.
7. Providing the IT and Cyber Security Governance Committee with the minutes of its meetings and obtaining information that indicates access to them. The Director of the Operations Engineering Department will be the representative of the Committee.

Resources:

1. Institutional Governance Instructions No. (2/2023) dated 14/02/2023 issued by the Central Bank of Jordan.
2. Instructions for Governance and Information Management and Related Technology No. (65/2016) dated 25/10/2016 issued by the Central Bank of Jordan and circular No. (984/6/10) dated 21/1/2019 issued by the Central Bank of Jordan.
3. COBIT 2019 Framework – Introduction and Methodology issued by the Information Systems Audit and Control Association (ISACA) in the United States of America.