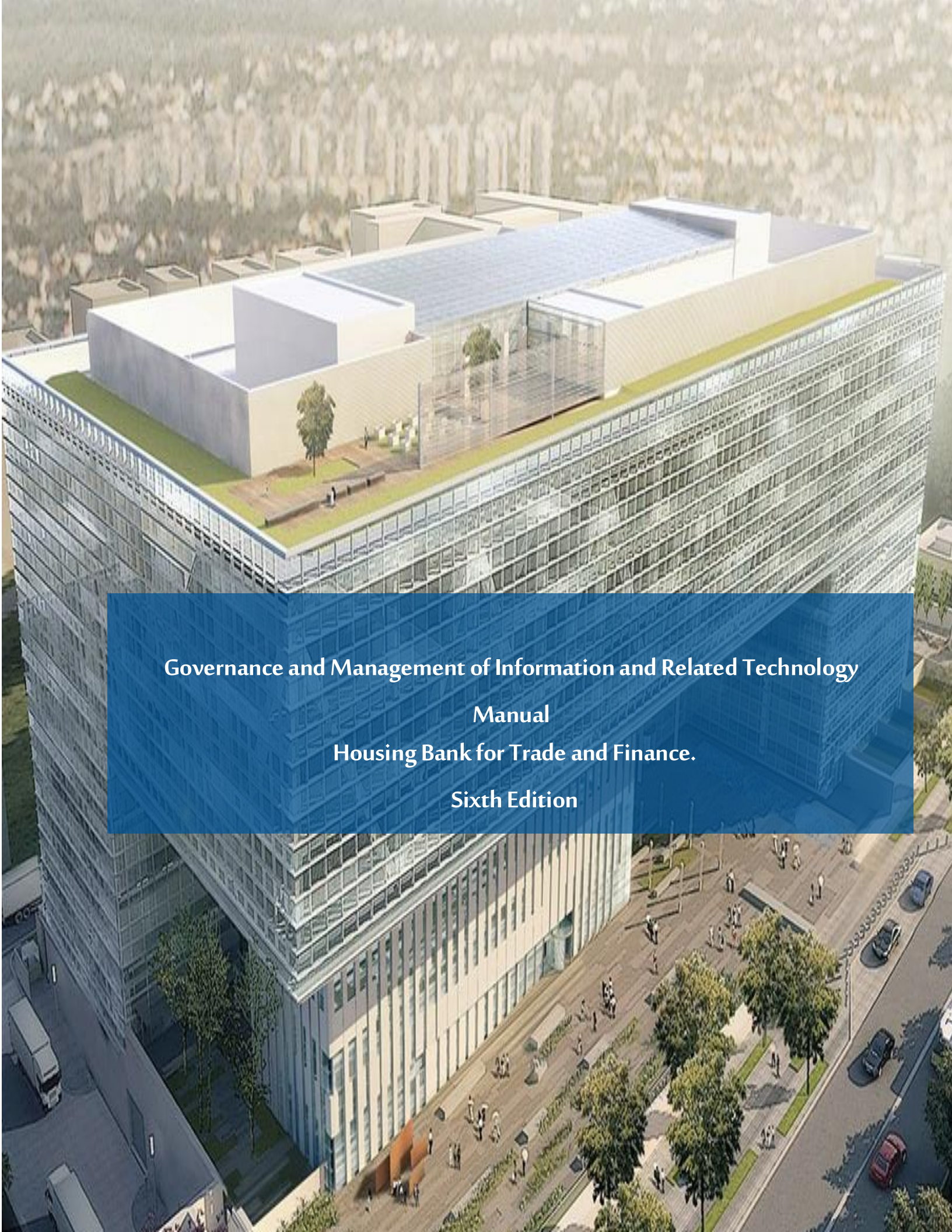


Governance and Management of Information and Related Technology

Manual

Housing Bank for Trade and Finance.

Sixth Edition

Table of Contents

First: Introduction

IT resources represent a fundamental component in terms of their relative size and their impact on an organization's ability to conduct its operations and, consequently, in achieving its objectives. They also play a crucial role in influencing both the competitiveness of the organization's products and services, and the processes of decision-making and risk management. This significance justifies the considerable investments made by banks in the information technology sector.

Accordingly, Housing Bank recognizes the necessity of adopting sound principles and standards for managing IT resources, in alignment with internationally accepted practices. This is essential to mitigate IT-related risks, avoid unproductive investments and unjustified expenditures that may result in substantial long-term losses, and prevent potential damage to the institution's reputation.

In light of the Bank's commitment to implementing corporate governance principles, it has developed a dedicated guide for the governance and management of information and related technology. This manual is consistent with and complements the Central Bank's Governance and Management of Information and Related Technology Instructions No. 65/2016 (issued on October 25, 2016), the Corporate Governance Instructions for Banks No. 63/2016 (dated September 1, 2016) and its subsequent amendments, as well as Circular No. 10/6/984 (dated January 21, 2019), which adopts the COBIT 2019 framework as a reference. This Governance and Management of Information and Related Technology manual is based on international standards and the key principles outlined in the Governance and Management of Information and Related Technology Instructions No. 65/2016 and Circular No. 10/6/984, as well as the COBIT framework and the IT Governance Framework issued by the Information Systems Audit and Control Association (ISACA) in the United States. The manual emphasizes several key pillars, most notably achieving strategic alignment by ensuring that IT objectives are aligned with the enterprise's strategic goals, optimizing the use of IT resources, ensuring value delivery, and maximizing added value—primarily measured by the contribution of IT to the achievement of strategic objectives. It also highlights the implementation of integrated IT risk management aligned with the organization's overall risk framework to support sound risk-based decision-making, the development and activation of performance measurement indicators, and the proper segregation and allocation of roles and responsibilities between the Board and Executive Management.

Second: Reference

The Manual for the Governance and Management of Information and Related Technology has been issued as a complementary document to the Corporate Governance Guide, in adherence to the Central Bank of Jordan's regulations, specifically the Governance and Management of Information and Related Technology Instructions No. 65/2016 dated October 25, 2016, and Circular No. 10/6/984 dated January 21, 2019.

Third: Definitions

The following words and expressions wherever mentioned in this manual shall have the meanings assigned to them hereunder, unless the context indicates otherwise. The Banking Law and the Instructions issued pursuant thereto shall be referred to regarding any other definitions contained in this manual that are not included in this article:

A. **Corporate Governance**: The system by which the Bank is directed and managed, which involves identifying the Bank's corporate objective and the framework for attaining them, the safe management of the Bank's operations, the protection of the interests of the depositors, fulfilment of the responsibilities towards the shareholders, and other Stakeholders, and compliance by the Bank with the legislations in force and the internal policies of the Bank.

B. **Governance of Information and Related Technology:** The distribution of roles and responsibilities, and the definition of relationships between various parties and stakeholders (e.g., the Board of Directors and Executive Management), with the aim of maximizing the added value to the institution by adopting an optimal approach that balances risks and expected returns. This is achieved through the application of governance rules, principles, and mechanisms for decision-making, setting strategic directions and objectives for the Bank, and establishing monitoring and compliance frameworks to ensure the Bank's sustainability and growth.

C. **Management of information and related technology:** A set of ongoing activities under the responsibility of executive management, including planning to achieve strategic objectives (such as alignment and organization), development and implementation (including procurement and execution), operations (including service delivery and support), and monitoring (including measurement and evaluation), in a manner that ensures the continued realization of the Bank's objectives and strategic direction.

D. **Objectives of Information Technology Governance and Management**: A set of goals that the institution seeks to achieve through practices and activities derived from its policies, necessary for realizing the objectives of information and related technology and aligning them with the enterprise's overall goals.

E. **Objectives of information and related technology - Alignment Goals**: A set of primary and secondary goals related to the governance and management of information and related technology, required to achieve the enterprise's strategic goals.

F. **Enterprise Goals**: The set of objectives related to institutional governance and management necessary to meet the needs of stakeholders and the objectives of the Central Bank's instructions in this regard.

G. **The Board**: The Board of Directors of the Bank.

H. **Senior Executive Management**: Includes the Chief Executive Officer, Sector Heads, Executive Vice President – Head of Risk Management, Executive Vice President – General Auditor, Executive Vice President – Head of Compliance, Heads of Departments and Divisions, or any employee at the Bank with executive authority equivalent to that of any of the aforementioned reporting directly to the Chief Executive Officer.

I. **Stakeholders**: Any party of interest in the Bank, such as shareholders, employees, creditors, customers, external suppliers or concerned regulatory bodies.

J. **Instructions**: The Central Bank's instructions regarding the Governance and Management of Information and Related Technology No. 65/2016, issued on October 25, 2016, and the subsequent Central Bank's circular No. 10/6/948 dated January 21, 2019.

K. **Auditor**: The person (natural or legal) or the entity authorized to examine the Bank's information technology-based operations in accordance with the requirements of the relevant instructions and approved by the Bank's management to fulfil those requirements for a period of no less than 3 consecutive years and no more than 6 consecutive years.

L. **Attachments / Annexes**: The attachments included in the Central Bank's Instructions on the Governance and Management of Information and Related Technology No. 65/2016, issued on October 25, 2016. These comprise eight annexes that are required to be implemented in alignment with the fifteen articles of the main instructions document, in addition to the COBIT 2019 reference framework, as adopted pursuant to the Central Bank Circular No. 10/6/948 dated January 21, 2019.

Fourth: Publication of the Manual for the Governance and Management of Information and Related Technology

The Bank shall publish this manual on its website and through any other appropriate means to ensure public access. The Bank shall also disclose, in its annual report, the existence of the manual for the Governance and Management of Information and Related Technology, as well as information of interest to stakeholders, including the manual itself, and the extent to which the Bank complies with its provisions.

Fifth: Committees

Two committees have been established: one at the Board of Directors level called the Information Technology Governance Committee, and another at the Senior Executive Management level called the Information Technology Steering Committee.

A. Information Technology Governance Committee:

- This committee shall consist of at least three members of the Board of Directors.
- Its members shall include individuals with expertise or strategic knowledge in information technology.
- The committee may, if necessary and at the Bank's expense, engage external experts—in coordination with the Chairman of the Board—to compensate for any shortage in this area and to promote objective perspectives.
- The committee may invite any of the Bank's executives to attend its meetings to seek their input, including internal audit representatives and members of the Senior Executive Management (e.g., EVP – Head of Information Technology), as well as external audit representatives.
- The Board shall define the committee's objectives and delegate authorities to it through a formal charter.
- The committee shall submit periodic reports to the Board, noting that delegating authorities to the committee does not absolve the Board from its overall responsibilities in this regard.
- The committee shall meet at least quarterly and shall maintain documented minutes of its meetings.
- The committee shall be responsible, at a minimum, for the following:

    1. Approving the strategic objectives of information technology and recommending to the Board of Directors the appropriate organizational structures, including the Senior Executive Management-level committees—particularly the Information Technology Steering Committee—to ensure the achievement of the Bank's strategic objectives, maximize the added value of IT resource investments and projects, and utilize appropriate tools and standards to monitor and verify progress.
    2. Approving the general framework for managing, controlling, and monitoring IT resources and projects in alignment with internationally accepted best practices—specifically COBIT 2019—to achieve the Bank's institutional and IT objectives, and ensure compliance with Central Bank regulations.
    3. Adopting the Enterprise Goals and Alignment Goals matrix.
    4. Adopting the prioritization and significance of enterprise goals and their alignment with Governance and Management Objectives, as well as their connection with other enabling components.

5. Ensuring the development of a RACI Chart for core IT governance objectives, identifying the parties who are: Responsible, Accountable, Consulted, and Informed across all governance and management activities for information and related technologies, and recommending its approval to the Board.

6. Ensuring the presence of a comprehensive IT risk management framework that aligns and integrates with the Bank's overall enterprise risk management framework in a way that takes into consideration and fulfills all IT Governance processes.

7. Reviewing the budget for IT resources and projects, including any amendments, to ensure alignment with the Bank's strategic objectives, and recommending its approval to the Board.

8. Supervising and reviewing IT operations and resources to ensure their adequacy and effective contribution to fulfilling the Bank's operational needs.

9. Reviewing the recommendations and meeting minutes of the Information Technology Steering Committee.

10. Reviewing IT audit reports, informing the Board accordingly, and taking necessary actions to address any identified deviations. Ensuring that **Central Bank of Jordan (CBJ)** is provided with the required reports-including internal and external audit reports- for assessing information and related technology (risks-controls) within the first quarter of each year.

11. Overseeing the preparation, review, and update of the Bank's manual for the Governance and Management of Information and Related Technology and recommending its approval to the Board of Directors.

12. Reviewing and evaluating IT-related policies and recommending their approval to the Board.

13. Ensuring the preparation, adoption, and periodic review of the Information Technology Steering Committee charter.

B. IT Steering Committee:

- The committee shall be formed under the chairmanship of the Chief Executive Officer (CEO), with membership including Senior Executive Management represented by: Chief Operations Officer, Chief Business Officer, Chief Financial Officer, Executive Vice President – Head of Risk Management, Executive Vice President – Head of Credit Management, Executive Vice President – Head of Information Technology , and Assistant Vice President – Head of Cybersecurity and Technology Risk. The Board shall elect one of its members as an observer to this Committee, in addition to the Executive Vice President - General Auditor.

- The committee may invite third parties to attend its meetings when necessary.
- The committee shall document its meetings through formal minutes.
- The committee shall convene periodically, at least once every three months.
- The committee shall, at a minimum, undertake the following responsibilities:

1. Developing annual plans aimed at achieving the Bank's information technology objectives in alignment with the strategic goals approved by the Board of Directors, overseeing their implementation to ensure successful execution, and continuously monitoring internal and external factors that may impact their achievement.
2. Linking the matrix of enterprise goals with the matrix of information and related technology alignment goals, adopting and continuously reviewing them to ensure consistency with the Bank's strategic objectives and regulatory instructions. This includes defining a set of benchmark indicators, reviewing them periodically, and assigning relevant executive management personnel to monitor and report on them regularly to the committee.
3. Supporting the realization of IT governance and management objectives, including alignment goals, by recommending the allocation of necessary financial and non-financial resources. This involves ensuring the deployment of competent and appropriate human resources within proposed organizational structures that cover all essential activities, ensure proper segregation of duties, and avoid conflicts of interest. It also includes adapting the technological infrastructure and associated services to serve these objectives and overseeing the execution of IT governance-related projects and operations.
4. Continuously reviewing IT projects and programs, assessing and prioritizing them based on risk and strategic importance.
5. Monitoring the status and progress of IT operations, resources, and projects to ensure their adequacy and effective contribution toward meeting the Bank's requirements and business needs. Monitoring the performance levels of technical and technological services and continuously working to enhance their efficiency and quality.
6. Evaluating and reviewing the annual IT systems budget (both capital and operational) and the IT strategy on a semi-annual basis to ensure continued alignment with the business strategy and regulatory requirements, assessing achievements within the period, and recommending appropriate corrective actions where necessary.

7. To make recommendations to the IT Governance Committee regarding the following matters:

   - Allocating the necessary resources and mechanisms to fulfill the functions of the IT Governance Committee.
   - Identifying any deviations that may adversely affect the achievement of strategic objectives.
   - Highlighting any unacceptable risks related to technology, security, and the protection of information.

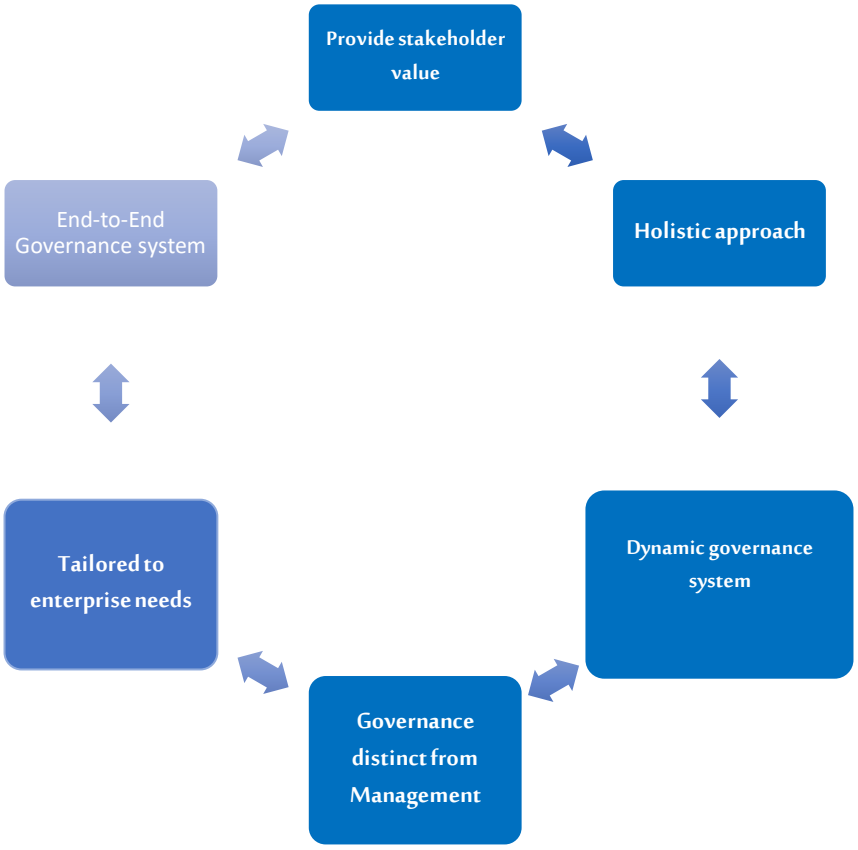
- Reviewing reports on performance and compliance with the requirements of the general framework for managing, controlling, and monitoring IT resources and projects.
- Approving RACI chart and practices for the core IT management objectives and their associated sub-processes.
- Internal and external audit reports for assessing information and related technology (risks-controls) within the first quarter of each year.

8. Provide the IT Governance Committee with the minutes of its meetings promptly and obtain confirmation of their review.
9. Approving the remaining components of the IT governance objectives documentation (excluding the authority and practice matrices).

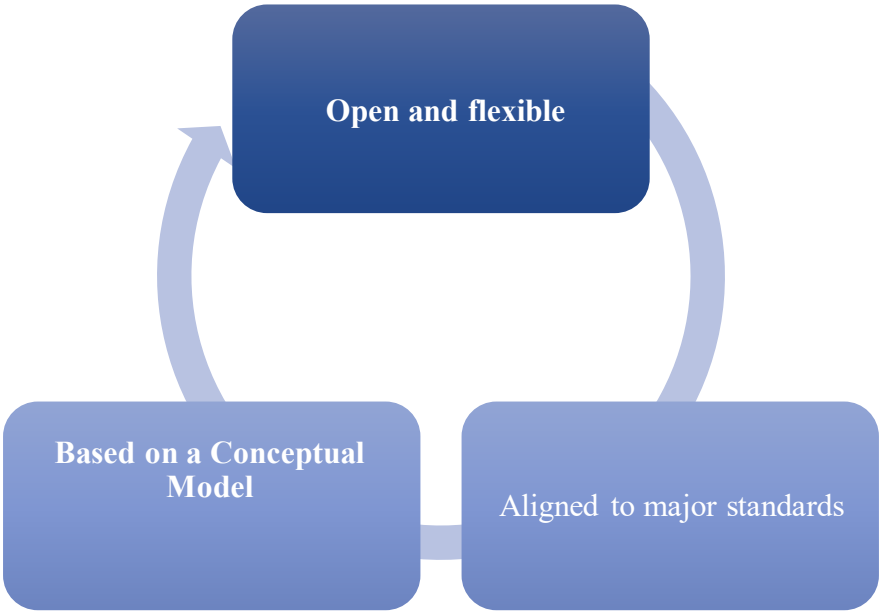
Sixth: Principles of the IT Governance Framework

The principles of information technology governance are divided into two groups:

First Group: The core and fundamental principles that constitute the Governance System.



Second Group: The principles associated with the Governance Framework necessary for establishing the governance system at the Bank level.



Seventh: Objectives of the Governance and Management of Information and Related Technologies

A. Meet stakeholders' needs and achieve the Bank's goals and objectives through the accomplishment of information and related technology objectives. This includes:

1. Providing high-quality information as a foundation to support the Bank's decision-making processes.
2. Prudent management of IT resources and projects to maximize their benefits and minimize waste.
3. Providing an excellent and supportive IT infrastructure that enables the Bank to achieve its objectives.
4. Enhancing the Bank's operations through the deployment of efficient and reliable technological systems.
5. Prudent management of IT risks to ensure the adequate protection of the Bank's assets.
6. Assisting in ensuring compliance with laws, regulations, instructions, as well as internal strategies, policies, and procedures.
7. Improving the internal control and oversight system.

8. Maximizing user satisfaction with Information Technology by meeting business needs efficiently and effectively.
9. Managing external service providers entrusted with the execution of operations, tasks, services, and products.

B. Achieving comprehensiveness in the governance and management of information and related technologies by considering not only the technology itself but also providing enabling components that accompany and complement IT services, including:

1. Principles, policies, and frameworks.
2. IT governance objectives.
3. Organizational structures.
4. Information and reports.
5. IT services, programs, and infrastructure.
6. Knowledge, skills, and expertise.
7. Code of Ethics, Values, and Conduct.

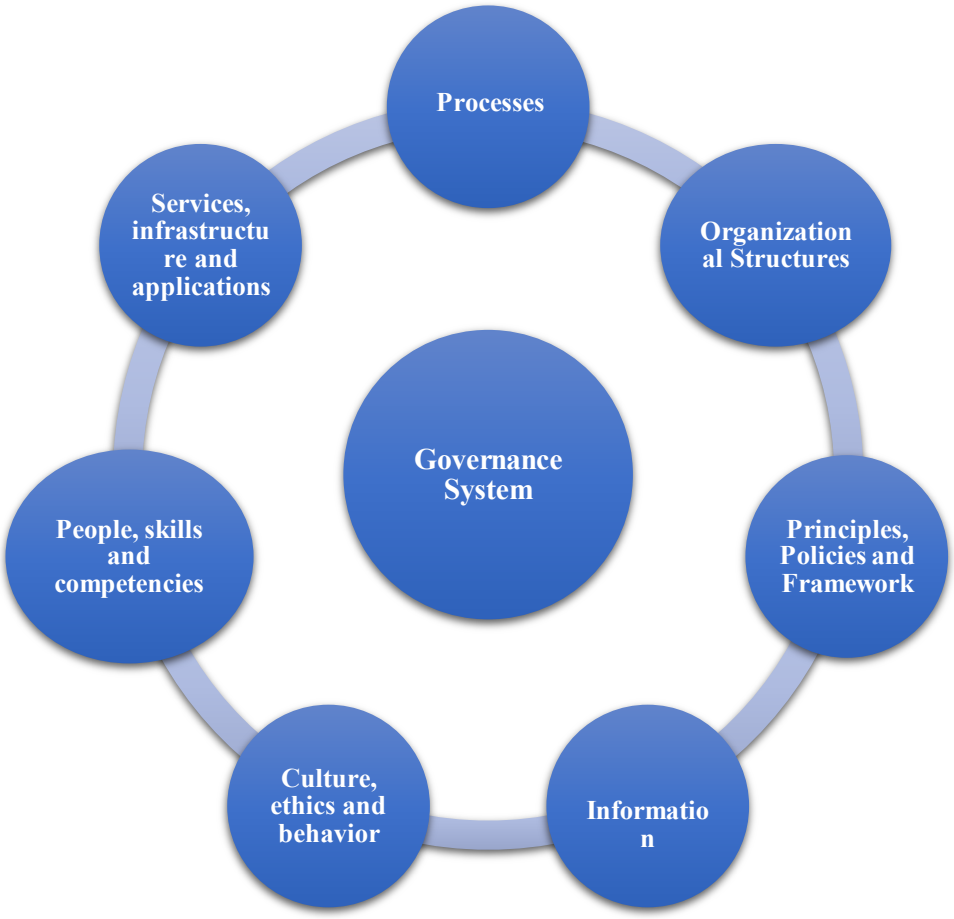
It is essential to provide these components with specific specifications and dimensions to meet and serve the requirements and objectives of information and related technologies, not only in IT operations and objectives but also in all Bank operations reliant on information and technology.

C. Adopting practices and organizational rules based on the best international standards as a starting point to be relied upon and built upon in the governance and management of IT operations, projects, and resources.

D. Separating the operations, tasks, and responsibilities of the board in the governance domain from those within the executive management's responsibilities concerning information and related technologies.

E. Enhancing mechanisms for self-regulation, independent oversight, and compliance examination in the governance and management of information and related technologies, contributing to continuous performance improvement and development.

Eighth: Governance System Components



1. Principles, Policies, and Frameworks

- The Board, or a delegated committee thereof, shall adopt the necessary set of principles, policies, and frameworks to achieve the general framework for the management, control, and monitoring of information technology resources and projects, in a manner that meets the requirements of the objectives of IT governance outlined in the COBIT 2019 reference framework.

- The Board, or a delegated committee thereof, shall adopt the principles, policies, and frameworks, particularly those related to IT risk management, information security management, and human resource [1] management, which meet the requirements, objectives of IT governance outlined in the COBIT 2019 reference framework.

- The Board, or a delegated committee thereof, shall adopt the necessary set of policies to manage the resources and operations of IT governance as detailed in Attachment No. 6 of the Instructions, considering this set of policies as a minimum with the possibility of combining and merging these policies as required by the nature of the work. Furthermore, other governing policies shall be developed in line with the evolution of the Bank's objectives and work mechanisms. Each policy shall specify the owning entity, scope , review and update frequency, access and distribution authorities, objectives, roles & responsibilities, related work procedures, penalties for non-compliance, and compliance review mechanisms.

- In establishing policies, the contribution of all internal and external stakeholders shall be taken into account, and the latest updates of international best practices shall be adopted as references for formulating these policies, such as COBIT 2019, COBIT 5, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL...etc.

2. IT Governance Objectives

- The Bank shall develop and formally approve a RACI Chart based on the objectives outlined in the COBIT 2019 framework. This Chart should clearly define the roles of the relevant entities in terms of being primarily Responsible, ultimately Accountable, Consulted, or Informed with regard to all objectives included in the referenced annex. The development of this Chart should be guided by the COBIT 2019 framework and must be approved by the committees specified in these instructions.

- The Bank shall develop a comprehensive IT Risk Management Framework that is fully aligned with and integrated into the Bank's Enterprise Risk Management (ERM) Framework, ensuring it fully addresses all IT governance objectives outlined in the COBIT 2019 framework.

- The Bank shall provide the required resources and mechanisms to effectively achieve both the Alignment Goals and IT Governance Objectives defined in the COBIT 2019 framework.

- The Alignment Goals and IT Governance Objectives specified in the COBIT 2019 framework, along with their associated requirements, constitute the minimum mandatory baseline that the Bank's senior management must continuously comply with and achieve. The Information Technology Steering Committee shall be primarily responsible for ensuring adherence to these requirements, while the IT Governance Committee and the Board of Directors shall hold ultimate accountability in this regard. All departments of the Bank, particularly the Information Systems, Information Security Management, and Project Management units—must define and restructure their processes to reflect and fulfill the requirements of all IT Governance Objectives stated in the COBIT 2019 framework.

- The Bank shall ensure alignment between the IT Governance Objectives outlined in the COBIT 2019 framework and the Alignment Goals, while actively contributing to their achievement. This alignment must further support the realization of the Enterprise Goals defined in the COBIT 2019 framework.

- The Board of Directors shall have direct responsibility for the Evaluate, Direct, and Monitor (EDM) governance objectives as defined in the COBIT 2019 framework.

- The Board of Directors and the Risk Management function shall assume direct responsibility for ensuring prudent management of IT risks, specifically for the governance objective EDM03 (Ensured Risk Optimization) and the management objective APO12 (Managed Risk), as defined in the COBIT 2019 framework.

3. Organizational Structures:

- The Board shall approve the organizational structures, both hierarchical and committee-based—particularly those related to the management of information technology resources, operations, and projects; IT risk management; information security; and human resource management. These structures must meet the IT governance objectives outlined in the COBIT 2019 reference framework and effectively support the achievement of the Bank's goals.

- When approving or amending the Bank's organizational structures, due consideration shall be given to the segregation of inherently conflicting duties, compliance with organizational safeguards such as dual control requirements (at a minimum), and the adequacy and periodic updating of job descriptions.

4. Information and Reports:

- The Board and Senior Executive Management shall develop the necessary infrastructure and information systems to provide information and reports to their users as a foundation for decision-making processes within the Bank. These reports and information must meet the Information Quality Criteria—namely, integrity, completeness, accuracy, and validity or currency—as well as confidentiality requirements in accordance with the data classification policy, availability requirements, and compliance standards. Additional requirements as outlined in COBIT 2019 shall also be observed.

- The Board, or a delegated committee thereof, shall adopt the information and reporting system detailed in Annex (7) of the Instructions and consider it as the minimum baseline. The ownership of each type of information and report shall be clearly assigned, with appropriate access and usage rights granted and delegated according to business needs and

relevant stakeholders. These systems and reports must be reviewed and updated continuously to align with the evolving objectives and operations of the Bank, and in accordance with accepted international best practices.

5. IT Services, Programs, and Infrastructure

- The Board, or a delegated committee thereof, along with Senior Executive Management, shall adopt the system of IT services, programs, and infrastructure that supports the implementation of IT governance objectives. This, in turn, contributes to achieving the objectives of information and related technology, and ultimately, the institutional goals of the Bank.

- The Board, or a delegated committee thereof, along with Senior Executive Management, shall adopt the IT services, programs, and infrastructure system as detailed in Annex (8) of the Instructions and consider it the minimum baseline. This system shall be continuously provided and developed to keep pace with the evolving objectives and operations of the Bank and shall align with internationally accepted best practices.

6. Knowledge, Skills, and Experience

- The Board, or a delegated committee thereof, shall adopt the HR Competency Matrix and human resources management policies necessary to meet the IT governance objectives requirements outlined in Annex (3) of the Instructions and the overall regulatory requirements, ensuring the placement of the right person in the right position.

- The Bank's management shall employ qualified and trained personnel with expertise in IT resource management, risk management, information security management, and IT audit management. This shall be based on standards of academic and professional knowledge, and practical experience, accredited by internationally recognized professional associations under international accreditation criteria for certifying bodies (ISO/IEC 17024), the Skills Framework for the Information Age (SFIA), and/or other equivalent standards, as applicable to each area of specialization. Current employees shall be continuously requalified and trained to meet both internal and external requirements.

- The Executive Management of the Bank shall continue to provide its staff with ongoing training and education programs to maintain a level of knowledge and skills that meets and supports the IT governance objectives outlined in the COBIT 2019 reference framework.

- The Executive Management of the Bank shall include objective measurement criteria in the annual performance evaluation mechanisms of its staff, considering the contribution of each role toward achieving the Bank's objectives.

7. Code of Ethics, Values, and Conduct

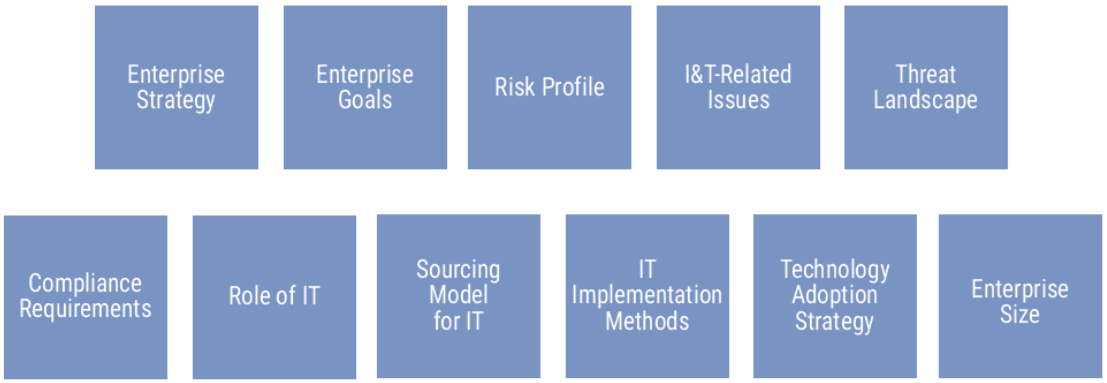
- The Board, or a delegated committee thereof, shall adopt an institutional code of professional ethics that reflects internationally accepted professional behavioral standards regarding the handling of information and related technology. This code shall clearly define acceptable and unacceptable behavioral standards and their consequences.
- Both the Internal and External Auditors shall comply with the Code of Ethics and professional practices approved by the Board, which shall include, at a minimum, the code of professional ethics set forth in the Information Technology Assurance Framework (ITAF), issued by the Information Systems Audit and Control Association (ISACA), and its subsequent updates.
- The Board and Senior Executive Management shall implement various mechanisms to promote the adoption of desirable behaviors and prevent undesirable ones, through the use of methods such as, but not limited to, incentives and disciplinary actions.

Ninth: High-Priority and Critical Objectives (Focus Areas)

The objectives of governance and the management of information and related technology, together with the governance components related to cybersecurity, risk management, data privacy and protection, compliance, monitoring, auditing, and strategic alignment, constitute a high-priority Focus Area.

Tenth: Governance System Design Factors

The governance and the management of information and related technology shall be designed in accordance with the recommended methodology outlined in the COBIT 2019 Design Guide. This process shall consider all or some of the design factors listed below, assigning appropriate weight to each characteristic or dimension as specified in the accompanying table, while aligning with the Bank's current strategic posture and assessment.



No.	Factor	Attributes / Dimensions of the Design Factor
1.	Enterprise Strategy	– Growth and Profitability Strategy – Innovation and Excellence Strategy – Cost Reduction and Operational Efficiency Strategy – Customer Service Strategy
2.	Enterprise Goals	A weight is assigned to each of the enterprise goals mentioned within the COBIT 2019 framework, in alignment with the Bank's strategic objectives.
3.	Risk Profile	Determine the probability and impact of the risks included within the COBIT 2019 framework, in alignment with the risk register of information and related technology.
4.	I&T Related Issues	The key challenges facing the Information and Technology Systems Department are determined through the list of challenges and difficulties outlined in the COBIT 2019 framework guide.
5.	Threat Landscape	– The threat landscape of the Bank (Medium) – The threat landscape of the Bank (High)
6.	Compliance Requirements	– low – Medium – High
7.	Role of IT	– Supports and serves the Bank but is not considered to directly impact business continuity. – Supports and serves the Bank and directly impacts business continuity. – An evolutionary and innovative role that does not impact the Bank's business continuity. – A strategic role that supports business plans and development and significantly impacts the Bank.
8.	Sourcing Model for IT	– Through outsourcing – Through internal resources – Through cloud computing

		– Through multiple models including local resources, external outsourcing, and cloud computing
9.	IT Implementation Methods	– Agile methodology – DevOps methodology – Traditional approach (Waterfall) – A hybrid of the above methodologies
10.	Technology Adoption Strategy	– A proactive and early adopter of leading technological standards – A proactive adopter of leading technological standards after they are fully developed and implemented in other banks. – Not proactive or an early adopter of leading technological standards and takes time to adopt them.
11.	Bank Size	– Large in terms of number of employees (more than 250) – Medium/Small (less than 250 employees)

– The Bank adopts the Goals Cascade methodology to achieve an enterprise governance framework based on the following:

Eleventh: Internal and External Audit

1. The Board shall allocate sufficient budgets and provide the necessary tools and resources, including qualified personnel, through specialized IT audit team, ensuring that both the Internal Audit Department in the Bank and the External Auditor are able to review and audit the recruitment and management of IT resources and projects and Bank operations based on specialized technical review (IT audit), in accordance with to item 4 hereunder, through qualified and internationally accredited professional staff in this field, who have valid professional accreditation certificates such as

CISA from qualified international associations under the International Accreditation Standards for Financial Institutions (ISO / IEC 17024) and / or any other parallel standards.

2. The Audit Committee of the Board, on the one hand, and the External Auditor on the other hand, shall provide the Central Bank of Jordan with an annual report of internal audit and another annual report of external audit respectively containing the response of the Executive Management and the Board's recommendations thereon, according to item 4.2 hereunder and according to audit report form (Risk - Controls) of information and related technology provided in Annex 4 of the Instructions, during the first quarter of each year. These reports shall replace its counterpart or these covered by reports required under previous instructions.

3. The Audit Committee shall include the responsibilities, authorities and scope of IT audit work within the Audit Charter on the one hand and within agreed procedures with the External Auditor on the other, in accordance with these instructions.

4. The Board shall ensure, through the Audit Committee, that the Internal Auditor and the External Auditor of the Bank upon implementation of processes of specialized information and its related technology audit, the commitment to the following:

   4.1 IT audit standards, according to the latest update of the international standard of Information Technology Assurance Framework (ITAF) issued by Information Systems Audit and Control Association (ISACA), including:

   - Perform audit tasks within the approved plan in this regard taking into account the relative importance of the processes, the level of risk and the degree of influence on the objectives and interests of the Bank.
   - Providing and complying with training and continuing education plans by specialized staff in this regard.
   - Compliance with the professional and organizational independency standards and ensure there is no current and future conflict of interests.
   - Commitment to the principles of objectivity, exercising due professional care, and continuously maintaining a high level of proficiency in the required knowledge and skills. This includes a deep understanding of the bank's various IT-driven mechanisms and processes, as well as familiarity with other audit reports (financial, operational, and legal). Additionally, the ability to provide appropriate evidence relevant to the case, along with sound judgment in detecting unacceptable practices or violations of applicable laws, regulations, and instructions, is essential.

   4.2 Examine, evaluate and review the processes of recruitment and management of IT resources and the Bank's operations based on them and provide a reasonable Overall audit assurance regarding the overall risk level of the information and related technology within an audit program that includes at least the axes set out in Annex (5),

provided that the audit repeat for all axes or portion of it as a minimum at least once a year in case of risk assessment at a degree of (5 or 4), according to risk assessment hierarchy described in annex (4), at least once every two years in case of risk assessment degree (3), and at least once every three years in case of the risk assessment degree (1 or 2), taking into account the continuous change in the level of risk, taking into account the significant changes on the environment of information and its related technology during the mentioned audit periods. The Central Bank shall be provided with audit reports for the first time regardless of the degree of risk assessment, and provided that the processes assessment of the mentioned axes include the bank procedures followed in terms of strategic planning, policy-making, written and adopted principles and procedures, procedures of employment of various resources, including information technology and human element resources, monitoring and improvement mechanisms and tools, and working on documenting the results of the audit and evaluation based on the importance of the imbalances and weaknesses (notes) as well as active controls and assessment of residual risks that are related to each of them using systematic standard to analyse and measure the level of risk, including corrective actions agreed upon and intended to be followed by the Bank's management with specific correction dates, with reference within a special agenda to the rank of the holder of responsibility in the Bank owner of each note.

4.3 Establish regular procedures to follow up on audit findings to ensure that the observations and deficiencies identified in the auditor's reports are addressed within the specified timelines. In cases of non-compliance, the level of importance and associated risks shall be escalated progressively, and the Board shall be kept informed whenever necessary.

4.4 Include the Performance evaluation mechanisms for the IT audit cadres with objective measurement criteria that take all the provisions of item (4) above into account. The evaluation processes should be carried out by the Board represented by the Audit Committee emanating from the Board.

5. The role of the Internal Auditor for Information and Related Technology (Internal IT Audit) may be outsourced to a specialized external party that is entirely independent from the approved external auditor. This is permissible provided that all the requirements of these instructions, as well as any other relevant regulatory guidelines, are fully met. The Audit Committee, established by the Board, and the Board itself shall retain their oversight roles in verifying compliance and ensuring that these requirements are met at a minimum.

6. The internal and external audit reports may be approved by the Information Technology Governance Committee or any committee acting on its behalf, provided that the Board is informed of these reports.

Twelfth: Scope and Mechanism of Application and Adoption of the Governance and Management System for Information and Related Technology and the Tasks of the Main Parties

First: Scope and Mechanism of Application and Adoption of the Governance and Management System for Information and Related Technology:

- The scope of implementing instructions shall include all the Bank's operations based on information technology in various branches and departments. All stakeholders' parties shall be considered concerned with applying the instructions, each in its respective role.

- The objectives outlined in the COBIT 2019 framework together with the other six enablers/ components related to cybersecurity, risk management, data privacy and protection, compliance, monitoring, auditing, and strategic alignment, constitute a high-priority Focus Area.

- The capability level of activities related to the objectives outlined in the COBIT 2019 framework and their associated enablers/ components shall be proportionate to their level of importance and priority, as determined by the assessment conducted by the IT Governance Committee referenced above. The capability level for activities associated with high-priority and high-importance objectives must not be less than Level 3 (Fully Achieved) according to the COBIT 2019 capability scale. It is permissible to classify no more than 26% of the COBIT 2019 objectives—equivalent to a maximum of 9 out of 35—as lower-priority and lower-importance objectives, based on the results of the information and technology governance and management system assessment approved by the Information Governance Committee.

- When the Bank signing Outsourcing Agreements with others to provide human resources, services, programs and information technology infrastructure to manage the Bank's operations, the Bank shall ensure that third parties comply with the provisions of these instructions in whole or in part to the extent that commensurate with the importance and nature of the Bank's operations, services, programs and infrastructure provided before and during the term of the contract, without releasing the Board and Senior Executive Management from final responsibility to achieve the instructions requirements including audit requirements set out in the Guide.

- The Bank must keep abreast of the future emerging versions and their updates regarding the COBIT general framework, and the international standards referenced within this framework.

- Banks shall tailor the enablers/ components, annexes, processes, and sub-objectives to align with their specific context, in line with the requirements of the COBIT 2019 framework and related instructions and shall implement the necessary changes to ensure a suitable environment for application.

- The Bank employs the Gap Analysis methodology to assess the disparity between its current state and the required regulatory and standards-based benchmarks, in preparation for implementation. This analysis takes into account both the Bank's current objectives and its future strategic goals.
- The Bank shall submit a Compliance Report to meet the requirements of the Central Bank of Jordan's instructions every six months from the date of instruction, indicating the level of completion of each item of instructions in accordance with the Central Bank's circulars and instructions, until full compliance with all requirements is achieved.

Second: Key Stakeholders and Their Responsibilities:

- **Chairman, Board Members, and Engaged External Experts:** responsible for providing overall guidance for the adoption and maintenance of information and related technology governance and management at the designated levels, approving assigned tasks and responsibilities, and providing the necessary support and funding.
- **The Chief Executive Officer (CEO), Deputy CEOs, CEO Assistants, Sector Heads, Operations Officers, and Branch Managers** are responsible for nominating qualified individuals with the necessary expertise to represent them in managing information and related technology projects and operations, and for clearly defining their roles and responsibilities.
- **IT Governance Committee and IT Steering Committee:** responsible for the assigned under the duties outlined in Article Five of this manual (page 5).
- **Internal Audit:** as directly assigned by the applicable regulations and participates in the adoption and implementation of the framework, representing the role of internal audit in operational matters as an independent advisor and monitor.
- **Risks, Compliance and Legal Departments:** participating in the adoption and ensuring the implementation of governance principles in a manner that reflects the role of these departments.
- **IT Governance Unit / IT Governance and Control Center:**
    - Managing compliance requirements with the approved governance standards and verifying the outputs of the governance framework within the Bank in alignment with the relevant instructions.
    - Assessing the mechanism of applying and adopting the IT governance objectives approved within the Bank's designed governance framework, overseeing the achievement of targeted maturity levels for these objectives to fulfil the Bank's objectives and strategies, ensuring compliance with regulatory authorities' instructions, and verifying adherence by all relevant stakeholders.

- Conducting an annual study to design the governance framework (or reviewing the existing study) to align with the Bank's objectives, the COBIT 2019 framework, and the Central Bank's IT governance instructions, and submitting this design for review and approval by the IT Governance Committee.
- Monitoring and overseeing the implementation of IT governance objectives in coordination with their respective owners, while periodically collecting, reviewing, and analysing performance indicators for each objective with relevant stakeholders - in compliance with IT governance and related technology instructions.
- Supervising and ensuring the development of the outputs of the approved IT governance system's objectives, in addition to verifying their review and maintenance according to their established periodicity.
- Preparing and updating Governance Objectives Processes Definition Documents (PDDs) and conducting periodic reviews with relevant stakeholders from various work units.
- Conducting a study to assess the significance and prioritization of governance and management objectives, including their correlation with Enterprise and Alignment goals
- Preparing reports, outputs, and materials to be presented to the IT Steering Committee and IT Governance Committee to ensure transparency and information quality, thereby supporting appropriate decision-making and recommendations to achieve benefits and maximize value-added for the Bank. Additionally, coordinating IT steering committee meetings and following up on the completion of assignments issued by this committee.
- Contributing to the dissemination of IT governance and control awareness Bank-wide, in accordance with the established plans for this purpose.
- Participating in the development and review of models, methodologies, and frameworks related to information systems, ensuring the inclusion of adequate IT controls in line with COBIT objectives, the Bank's approved frameworks, compliance requirements, risk observations, and IT governance audit findings.
- Participating in the development and review of information systems policies and procedures to ensure their alignment with the Bank's policies and instructions, as well as with the regulatory authorities' directives concerning information governance and related technologies
- Preparing the policies and procedures related to the IT governance framework in coordination with relevant stakeholders, in alignment with the Bank's policies and instructions, and the Central Bank's directives, including but not limited to the COBIT framework.
- Reviewing audit observations (internal and external) and the Central Bank's reports concerning the IT governance framework and related directives, while ensuring the development of corrective action plans for all outstanding observations and following up with the relevant parties to address them within the specified timeframe.

Thirteenth: Review and Amendments:

This manual shall be subject to review and updates as deemed necessary by the **IT Governance Unit / IT Governance and Control Center**. Any revisions shall be approved by the IT Governance Committee emanating from the Board.

Fourteenth: Articles and Annexes of the Instructions:

The annexes comprise a set of foundational pillars, enterprise goals, IT-related objectives and their associated processes, internal and external audit mechanisms, and the required forms, as outlined in the manual and in accordance with the fifteen articles and eight detailed annexes referenced and attached to these instructions, summarized as follows:

Instruction Articles:

1.1 Reference (Article1)

1.2 Definitions (Article2)

1.3 Publication of the manual for the Governance and Management of Information and Related Technology (Article 3)

1.4 Governance and Management of Information and Related Technology Manual (Article 4)

1.5 Publication of the Manual for the Governance and Management of Information and Related Technology (Article 5)

1.6 Objectives of the Governance and Management of Information and Related Technologies (Article 6)

1.7 Committees (Article 7)

1.8 IT governance objectives (Article 8)

1.9 Internal and External Audit (Article 9)

1.10 Principles, Policies, and Frameworks (Article 10)

1.11 Organizational Structures (Article 11)

1.12 Information and Reports (Article 12)

1.13 IT Services, Programs, and Infrastructure (Article 13)

1.14 Knowledge, Skills, and Experience (Article 14)

1.15 Code of Ethics, Values, and Conduct (Article 15)

Annexes to the Instructions

Annex 1: The Enterprise Goals (13 goals) and the associated performance indicators/measurement criteria required from banks to assess the achievement level of each goal shall replace the Enterprise Goals matrix in Annex (1) of the instructions.

Annex 2: The Alignment Goals matrix (13 goals) and the associated performance indicators/ measurement criteria required from banks shall replace the Enterprise Goals matrix in Annex (2) of the original instructions. This matrix aligns directly or indirectly with the Enterprise Goals.

Annex 3:

Governance and Management Objectives of Information Technology (40 objectives) under five key pillars that form the overall framework for the governance and management of IT systems and operations, as outlined on pages 33–35 of the COBIT 2019 Governance and Management Objectives publication.

- **Governance (Board of Directors):**

✓ Evaluate, Direct and Monitor (EDM) objectives, (5 objectives).

- **Executive Management (Planning, Building, Operation, Control):**

✓ Align, Plan and Organize (APO) objectives, (14 objectives).

✓ Build, Acquire and Implement (BAI) objectives, (11 objectives).

✓ Deliver, Service and Support (DSS) objectives, (6 objectives).

✓ Monitor, Evaluate and Assess (MEA) objectives, (4 objectives).

Annex 4: Form and Mechanisms of the Information and Associated Technology Audit Report, according to the following components:

I. Form of the Board's review and recommendations on the report.

II. Mechanisms**:** Composite Risk Rating, Assessment of Information and Related Technology (Risk-Control), Examination and Evaluation Methodology, Report Discussion, Audit Parameters, Qualifications and Experience of the Responsible Auditor and Audit Team Members.

III. Body of the audit report.

IV. Outstanding findings unresolved from previous years

Annex No. (5): Minimum Audit Areas for Information and Related Technology, including at least the following:

IT Governance, Application Software and Management, Database Management, Managing Main Computers, Networks Management, Management of Business Continuity Plans, Physical and Environmental Security

Annex No. (6): The Required Policies System with a Minimum of (26 main Policies):

Governance of Information Technology Organization, Information Security, Business Continuity Plans and Disaster Recovery Plan, IT Risk Management, IT Compliance, Data Privacy Outsourcing, Project Portfolio Management, Asset Management, Acceptable Use of Information Technology Resources, Change Management, Central Computers, Computer peripherals, Portable devices, User Access Management, System Development Life Cycle, Service Level Management, Backup & Restore,Data Retention, Systems and Equipment Purchasing, Remote Access, Networks, Wireless Networks, Vulnerability & Penetration Testing, Firewalls and Public Branch Exchange.

Annex No. (7) Information, Reports, and Working Principles with a Minimum of (20 Items):

Authority Matrix, IT Risk Factors Analysis, IT Risk Scenario Analysis, IT Risk Register, IT Risk scenario analysis, RACI Chart, IT Risk Profile, IT Risk Report, IT Risk Map, Risk Universe & Appetite & Tolerance, IT Key Risk Indicators, Risk Taxonomy, Risk and Control Activity Matrix (RCAM), Information Security Budget, MIS Report, IT Audit Strategy, IT Audit Procedures, HR Competencies, and The Best International Standards for The Management of Projects and Information Technology Resources, IT Risk Management, Security, Protection and Audit on Information Technology.

Annex No. (8): Services and Software Infrastructure for Information Technology with a Minimum of (8 Items):

Incident Management Services IT Assets Inventory Management, Information Security Best Practices Awareness, Access Management, Information management Systems, Monitoring of information Security, IT Environmental Systems Control & Management (Server Rooms, Communications, and Electricity) and IT Audit Software

References:

1. Instructions for the Governance and Management of Information and Related Technology No. 65/2016 dated 25/10/2016 issued by the Central Bank and Central Bank Circular No. 10/6/948 dated 21/1/2019, based on the COBIT 2019 reference framework and published on the Central Bank's website http://www.cbj.gov.jo

2. COBIT Instructions issued by the Information Systems Audit and Control Association (ISACA) in the United States of America and published on the Association's website https://www.isaca.org/COBIT/Pages/Product-Family.aspx

- COBIT 5 Framework
- COBIT 5 Implementation
- COBIT 5 Enabling Process
- COBIT 5 Enabling Information
- COBIT 2019 reference framework: Introduction and Methodology
- COBIT 2019 reference framework: Governance and Management Objectives
- COBIT 2019 Design Guide: Designing and Information and Technology Governance Solution
- COBIT 2019 Implementation Guide: Implementing and Optimizing and Information and Technology Governance Solution