No.: 10/1/13722

Date: 24/1/1438

Corresponding to: 25/10/2016

Governance and Management of Information and Related Technology instructions

No. (65/2016)

Contents

Introduction

IT resources are an important anchor in terms of the relative size and impact on the organization's ability to conduct its operations, thus achieve its objectives. IT resources also play crucial role in influencing the competitiveness of the organization's products and services on the one hand and on the procedures of decision-making and risk management on the other. This justifies the huge size of investments in information technology sector by banks.

Therefore, institutions in general and banks in particular have to follow the proper principles and standards in the management of IT resources in accordance with internationally accepted practices in this regard to reduce their risks and to avoid the entry into useless investments and unjustified expenses transferred into huge losses over the years and sometimes may undermine the institution reputation. Out of the Central Bank of Jordan's interest to apply the rules and pillars of corporate governance, it was necessary to issue instructions regarding the governance and management of information and related technology that is consistent with and complement our instructions no. (58/2014) dated 30/09/2014 and our instructions No. (61/2015) dated 12/05/2015. Information technology governance in the world has been a positive development that that has come out with general frameworks for a group of foundations and principles at a high level of maturity, especially the "Control Objectives for Information and Related Technology" (COBIT) framework issued by Information Systems Audit and Control Association (ISACA) in the United States.

The overall framework for the governance and management of information and related technology consists of a set of foundations and fundamental principles. The first is the strategic alignment that is required to be achieved through the strategic objectives of information technology and should lead to the achievement of the strategic goals of the institution,. The institution shall employ its information technology resources within available options that maximize value added, mainly measured by criterion of information technology contribution in achieving the organization's strategic objectives, and work on information technology risks management in an integrated manner that is consistent with the total risk management processes of the institution and according to proper procedures and practices that lead to proper risk-based decision-making mechanisms, and ensure the achievement of added value in the lowest cost with mitigation of expected loss and risks to reflect the bank's vision in this regard and within acceptable risk limits as much as possible. The senior management (the Board and Senior Executive Management) should undertake planning and institutional organization through the development of strategies, policies and action plans, build and adapt hierarchical and circular organizational structures (ie, in the form of committees) so as to achieve the strategic objectives, build procedures, tools and standards to measure the added value of information technology, to enable the Board and Senior Executive Management to control institutions operations to ensure the safety of planning, organization and recruitment mechanisms of information technology resources in order to take the feedback for continuous improvement and development, All this is

based on the principle of separating tasks and roles and distribute them properly between the Board on the one hand and the Senior Executive Management on the other hand.

Article (1): Reference

These instructions were issued pursuant to the provisions of Article (4/B/3) and Article (65/b) of the Central Bank of Jordan Law No. 23 of 1971 and its amendments, and Articles (21, 99/b, 92) of Banking Law No. 28 of 2000 and its amendments, and

Shall come into force after eighteen months of its issuance date, unless the context indicates otherwise.

Article (2): Definitions

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

a. **Governance of Information and Related Technology**:
   The distribution of roles, responsibilities and characterization of relations between parties and different actors and stakeholders (such as the Board of Directors and Senior Executive Management) in order to maximize the institution's added value by following the optimal approach which ensures a balance between risks and expected return, by adopting the rules, principles and mechanisms for decision-making and determining strategic trends, objectives in the bank and mechanisms of monitoring and checking compliance with the extent to achieve the sustainability and development of the bank
b. **Management of information and related technology:**
   A set of ongoing activities that are under the responsibility of the executive management and include planning in order to achieve the strategic objectives, including harmonization, regulation and construction and development activities including purchase and implementation, operation activities, including the delivery of services and support, monitoring activities including measurement and evaluation, Ensures the sustainability of the Bank's objectives and strategic direction.
c. **Processes of IT governance**: A set of practices and activities emanating from the institution's policies that are necessary to achieve the objectives of information and related technology.
d. **Objectives of information and related technology:** A set of main and subsidiary objectives related to the governance and management of information and its related technology that are necessary to achieve institutional objectives.
e. **Institutional Objectives**: A set of objectives related to institutional governance and management that are needed to achieve stakeholder needs and objectives of these instructions.
f. **The Board**: The Board of Directors of the Bank.

g. **Senior Executive Management**: Includes Bank's general manager/regional manager, or deputy general manager/ deputy regional manager, assistant general manager/assistant regional manager, Chief Financial Officer (CFO), Chief Operational Officer (COO), Chief Risk Officer (CRO), Head of Treasury (Investment), *Chief Compliance Officer "CCO"*, as well as any employee in the bank who has executive authority parallel to the *aforementioned* powers and is reporting to the general manager.
h. **Stakeholders**: Any party of interest in the bank, such as shareholders, employees, creditors, customers, external suppliers or concerned regulatory bodies.
i. **On-Site:** The location of operation in the same building of general (regional) administration of the bank in Jordan.
j. **Off-Site:** The location of operation in a building rather than general (regional) administration building of the bank in Jordan, but in the same governorate.
k. **Near-Site**: The location of the operation in is in a different governorate where the general (regional) administration of the Bank is located in Jordan.
l. **Off-Shore**: The location of operation in a country different from that of the bank's general (regional) administration.

Article 3: Scope and Procedure of Application and Concerned Parties

a. Subject to the provisions in paragraph (b) of this article, these instructions shall apply to all licensed banks without exception.
b. The foreign banks branches operating in the Hashemite Kingdom of Jordan shall abide by these instructions to the extent applied thereto, or by the policies of Corporate governance and fit and proper criteria issued by their headquarter (the mother bank) or regulatory authority in the home country, whichever is more stringent in terms of meeting the goals of corporate governance and fit and proper criteria. Should the latter be the more stringent, the branch must provide the CBJ with supporting documents to prove same, if there is no conflict with the regulations. In case of any conflict, the branch shall inform the CBJ and the mother company of such matter, and present the necessary clarification of such conflict, then obtain the Central Bank's approval.
c. When the banks signing Outsourcing agreements with others to provide human resources, services, programs and information technology infrastructure to manage the Bank's operations, they 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 Article 9 below. Instructions enforcement period or contract period shall be considered the duration in which the positions of the currently contracting companies shall be particularly adjusted, whichever is earlier.

d. 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 and location. To facilitate the application process, a project/program (group of related projects) shall be initiated and managed by the bank to find and provide necessary environment and achieve our instructions requirements, and we mention specifically the following parties and their key responsibilities in this regard:

   1. Chairman, members of the Board and external experts employed: To assume overall guidance responsibilities of the project / program, approve tasks and responsibilities within the project, and support and provide the necessary funding.
   2. The General Manager, his deputies, his assistants, the directors of operations and the branches: To assume the responsibilities of naming suitable persons with experience in the Bank's operations to represent them in the project and to describe their duties and responsibilities.
   3. IT Manager and Steering Committee and Project Managers: take over the responsibilities of project/program management, guidance and direct supervision of and recommendation to provide the necessary resources to complete, and to ensure proper understanding of all parties of the requirements and objectives of the instructions.
   4. Internal Audit: take over their responsibilities directly upon the instructions, and participate in the project/program, representing the role of internal audit in executive matters as a consultant and independent observer to facilitate the success and completion of the project/program.
   5. Risks, information security, compliance and legal departments: take over the responsibilities involved in the project/program, representing the role of those departments, and to ensure the representation of project/program by all concerned parties.
   6. Specialists, holders of technical and professional certificates of (COBIT 5 Foundation, COBIT 5 Assessor, COBIT 5 Implementation, CGEIT) standard, who are hired from inside and outside the bank: take over the role of mentor to disseminate knowledge of the standard and to facilitate the application process.

e. These instructions target access the Maturity Level 3.2: Established-Deployment, after a maximum of eighteen months from its date, and to reach Maturity Level 5.2: Optimization, after three years of its date, fully achieved for each of the two periods, according to maturity levels contained in (COBIT 5) standard.

f. The requirements of the instructions after their application are a first step and a starting point towards the continuous development and improvement of the governance and management information and its related technology. Accordingly, the banks' managements must keep abreast of the future emerging issues and their updates regarding the general framework

adopted in the formulation of these instructions (COBIT 5) and the contained criteria of other international document them within this framework.

g. When implementing and entering into the details of the seven pillars, attachments, processes and sub-objectives, the banks must tailor all of this in line with the data of each bank in order to serve the objectives and requirements of COBIT 5 and to find the change required to provide and create the necessary environment for application.
h. Follow gap analysis method between the current situation and the compare with the requirements of the instructions and the standard in preparation for the application process.
i. Banks should submit a Compliance Report to meet the requirements of our instructions every six months from the date of instruction, indicating the level of completion of each item of instructions

Article (4): Code of Governance and Management of Information and Related Technology

The bank shall develop a special code of governance and management of information and its related technology, which may be part of the Corporate Governance Code, so as the Code takes into consideration these instructions at a minimum and in line with its needs and policies. The Code shall be approved from the Board and to provide the Central Bank with it during a maximum period (150) days from the date of these instructions. This Code shall reflect the bank's vision of the governance and management of information and related technology in terms of its concept, importance, principles in compliance with international legislation and best practices in this regard. The bank, through the IT governance committee derived from its Board, shall review this code and update it whenever necessary.

Article (5): Publication of Code of Governance and Management of Information and Related Technology

Each bank shall publish the code on its website and through any other suitable means to make it available for public viewing. The bank shall include and disclose in its annual report the presence of a special code of governance and management of information and its related technology or incorporated within corporate governance code, disclose any Information related to the stakeholders including this code, and the bank's compliance with its contents.

Article (6): Objectives of Governance and Management of Information and Related Technology:

These instructions aim to achieve the following:

a. Meet the stakeholder's needs and achieve the trends and objectives of the bank through the achievement of the objectives of information and related technology, so as to guarantee the following:
    1. Provide high-quality information as an anchor to support decision-making procedures in the bank.

2. Strict management of resources and projects of information technology that maximizes the utilization of those resources and reduce their waste.
3. Providing a unique and supportive technological infrastructure enabling the Bank to achieve its objectives
4. Upgrade the various bank operations by employing efficient, reliable and distinct technological system.
5. Prudent risk management of information technology to ensure the necessary protection of the bank's assets.
6. Assist in achieving compliance with the requirements of laws, regulations and instructions as well as to comply with the policy, strategy and internal working procedures.
7. Improve internal control and supervision system.
8. Maximize the level of satisfaction of information technology by its users by meet the needs of work efficiently and effectively.
9. Management of external parties' services entrusted with the implementation of operations, functions, services and products.

b. To achieve Inclusiveness in governance and management of information and its related technology in terms of taking into account not only the technology itself, but the provision of seven enablers that accompany and complement the information technology services represented by: 1. Principles, policies and frameworks. 2. IT governance processes. 3. Organizational structures. 4. Information and reports. 5. Services, programs and infrastructure of information technology. 6. Knowledge, skills and experience. 7. System of values, morals and behaviors, and the necessity to provide specifications and dimensions to achieve specific service requirements and objectives of information and its related technology, not only in information technology and operations, but also in all the bank's operations based on information and technology.
c. Adopt practices, business rules and regulation, according to the best international standards as a starting point on which it is based and built in the areas of governance and management of operations, projects, and information technology resources.
d. Separate the operations, functions and responsibilities of the Board in the field of governance from those within the limits of the responsibility of executive management regarding the information and its related technology.
e. Strengthen the mechanisms of self-monitoring and independent control, and examine compliance in governance, information management and associated technology, thereby contributing to the continuous improvement and development of performance.

Article (7): Committees:

a. **Governance of Technology Information Committee**

The Board shall form a committee of governance of information technology from its members, and this committee shall be formed from three members at least, and preferably include people with experience or strategic knowledge in information technology. The committee may, if necessary and at the expense of the bank, hire external experts in coordination with the chairman of the Board in order to make up the shortfall in this field on the one hand and to promote the objective opinion on the other hand. The committee may invite any of the bank's administrators to attend meetings for the use of their opinion, including concerned persons in the internal audit and members of the executive management (such as director of information technology) or concerned in the external audit. The Board determines its objectives and delegate their powers, according to a charter that illustrates this, and may raise periodic reports to the Board, noting that the delegation of the Board powers to a committee or any other committee does not release it as a whole from taking over its responsibilities in this regard. The committee shall meet on a quarterly basis at least, maintains documented records of the meetings, and shall have the following tasks:

1. Adopting strategic information technology objectives and appropriate organizational structures, including Steering Committees at the Senior Executive Management level, in particular the Information Technology Steering Committee, to ensure that the Bank's strategic objectives are met and the best value added of IT resources projects and investments is achieved; Such as the use of the IT Balanced Scorecard system and the calculation of return on investment (ROI), and measuring the impact of the contribution to increase Financial and operational efficiency.
2. Adopting the general framework for the manage, control and monitor of IT resources and projects that complies with internationally accepted best practices in this regard, specifically Control Objectives for Information and Related Technology (COBIT), complies with the achievement of the objectives and requirements of our instructions by achieving the institutional objectives set forth in Annex (1) sustainably, and achieve the matrix of associated information and technology objectives contained in Annex (2), covering the governance of information technology processes contained in Annex (3).
3. Adopt the matrix of institutional objectives contained in Annex (1), and the objectives of information and its related technology contained in the Annex (2) and considering its requirements a minimum extent, and characterize necessary sub-objectives to achieve them.
4. Adopting a RACI Chart towards the core processes of the IT governance in Annex (3) and its sub-processes in terms of: the entity/entities, person/parties primarily responsible ,those definitively accountable, those consulted and those that are kept informed towards all the operations mentioned in the mentioned annex guided by (COBIT 5 Enabling Processes) standard in this regard.

5. Make sure there is a general framework for risk management and information technology that complies and integrates with the general framework of the overall risk management at the bank, and so that takes into account and meets all operations of governance of technology information contained in Annex (3).
6. Adoption of budget and resources of information technology projects in line with the strategic objectives of the bank.
7. General supervision and review the progress of operations, resources and information technology projects to ensure its adequacy and active contribution in achieving the requirements and business of bank.
8. Access to audit reports for information technology and take the necessary measures to deal with deviations.
9. Recommend to the Board to take the necessary action to correct any deviations.

b. **IT Steering Committee:**

The Senior Executive Management shall form the necessary steering committees to ensure a strategic alignment of information technology to achieve the strategic objectives of the bank in a sustainable manner. Therefore, a committee called the Information Technology Steering Committee shall be formed and headed by general manager and with the membership of Senior Executive Management managers, including the information technology manager, director of risk manager and information security manager. One of its members shall be elected to be an observer member in this committee as well as the internal audit manager, and can invite third parties to attend the meetings, when needed. The committee shall document its meetings in fundamental minutes, provided that periodic meetings shall be once every three months at least, and shall, in particular, carry out the following tasks:

1. Develop annual plans to ensure access to the strategic objectives approved by the Board, and supervise the implementation to ensure their achievement and control of internal and external factors affecting them continuously
2. Linking the matrix of Institutional objectives with the matrix of information and its related technology objectives as set forth in Annex 2, and adopting and reviewing them continuously to ensure the achievement of the Bank's strategic objectives and the objectives of the instructions, taking into account the definition of benchmarks set, review them and assign concerned persons of executive management to continuously monitor it inform the committee of it.

3. Recommend the allocation of financial and non-financial resources necessary to achieve the objectives and processes of IT governance contained in Annexes (2) and (3), respectively, at a minimum, and the use of efficient and appropriate human element in the right place through organizational structures that include all the necessary processes to support the objectives and takes into consideration separation of tasks and non-conflicts of interest, and adapt the technological infrastructure and other services related to the

objectives of the service, and take over operations of overseeing the progress of projects and processes of governance of information technology.

4. Arranging IT projects and programs by priority
5. Monitor the level of technical and technological services and work to raise their efficiency and improve them continuously
6. To make recommendations to the IT governance committee regarding the following matters:
    a. Allocate the necessary resources and mechanisms to fulfill the functions e of governance of information technology committee.
    b. Any deviations may adversely affect the achievement of strategic objectives.
    c. Any unacceptable risks related to technology, security and protection of information.
    d. Reports on performance and compliance requirements of the general framework for the management, control, and monitor of projects and resources information technology.
7. Provide the IT governance committee with minutes of its meetings and receive access to information

Article (8): Objectives and Operations of Information Technology governance

a. Objectives and operations of IT governance, according to the Annexes (2) and (3) respectively, and their data shall be considered a minimum that the bank's senior management shall comply with it and achieve it continuously. The Information Technology Steering Committee shall be the primarily responsible for ensuring compliance to achieve its requirements. The IT governance committee and the Board as a whole shall be finally responsible in this regard, and all the Bank's departments and, in particular, information technology department, Information security management and projects management shall determine their operations and re-draft them to stimulate and cover the requirements of all operations of information technology governance contained in annex 3.
b. The Board shall has direct responsibility for the five evaluations (Evaluate, Direct and Monitor) (EDM) in Annex (3).
c. The Board and Risk Management Department shall take over direct responsibility for the process of "ensuring prudent management of information technology risks" (EDM 03) and the process of "risk management" (APO 12) contained in Annex (3), respectively.

Article (9): Internal and External Audit

a. The Board should observe adequate budgets and allocate the necessary tools and resources, including qualified personnel, through specialized IT audit divisions, 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 section (d) of this Article,

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

b. 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 (d / 2) of this Article and according to audit report form (risk - controls) of information and its related technology in annex (4), during the first quarter of each year. These reports shall replace its counterpart or these covered by reports required under previous instructions.

c. The Audit Committee shall include the responsibilities, powers 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

d. 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:

    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:
        a. 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.
        b. Providing and complying with training and continuing education plans by specialized staff in this regard
        c. Compliance with the professional and organizational independency standards and ensure there is no current and future conflict of interests.
        d. Commitment to objective standards, due diligence, continuous maintenance of competency and proficiency of the knowledge and skills to be enjoyed, deep knowledge of the Bank's various IT-based mechanisms and processes, and other review and audit reports (financial, operational and legal) , The ability to provide evidence consistent with the situation, and the general sense of disclosure of unacceptable practices that are contrary to the provisions of laws, regulations and instructions
    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 e significant changes on the environment of information and its related technology during the mentioned audit periods. We 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 analyze 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.

3. Systematic procedures to follow up the audit results to ensure processing notes and imbalances included in the auditor reports in deadlines, and work to raise the level of importance and risk escalation gradually in the event of non-response and the Board put this in perspective whenever necessary
4. Include the Performance evaluation mechanisms for the IT audit cadres with objective measurement criteria that take all the provisions of item (d) above into account. The evaluation processes should be carried out by the Board represented by the Audit Committee and according to the organizational structure of the audit departments , or who replaces them in foreign banks.

e. It is possible to outsource the role of internal auditor of information and its related technology (Internal IT Audit) to a specialized external authority that's completely independent from external auditor approved in this regard, provided that it meets all the requirements of these instructions and any other relevant instructions, the audit committee emanating from the Board and the Board itself keep their role, in terms of checking compliance and ensuring to meet these requirements at a minimum.

Article (10): Principles, Policies and Frameworks:

a. The Board or delegate of committees shall adopt the necessary system of principles, policies and frameworks to achieve the general framework for manage, control and monitor the resources and projects of information technology to meet the objectives of the requirements of processes of IT governance contained in Annexes (2) and (3) respectively.
b. The Board or its delegate committees shall adopt principles, policies and frameworks, particularly those related to IT risk management, information security management and human resources management that meets the processes of IT governance requirements contained in Annex (3).

c. The Board or its delegate committees shall adopt the necessary policies system to manage the resources and operations of IT governance contained in Annex (6), and to consider these policy system a minimum with the possibility of the combination and integration of these policies as the work nature requires, and to develop other governing policies that keep up the development of the Bank's objectives and procedures of action, provided that each policy shall determine the owner, scope of application, periodicity of review and update, power of access, distribution, objectives, responsibilities, related working procedures and penalties in case of non-compliance and compliance inspection mechanisms
d. The establishment of policies takes into account the contribution of all internal and external partners and the adoption of international best practices and updates as references to the formulation of such policies as (COBIT5, ISO/IEC 27001/2, ISO3100, ISO/IEC 38500, ISO/UEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL... etc.).

Article (11): Organizational Structures:

a. The Board shall adopt organizational structures (hierarchical and committees), in particular those c related to the management of IT resources, processes and projects, IT risk management, information security management, and human resources management that meet the operations requirements of IT governance contained in Annex (3) and to efficiently and effectively achieve the Bank's objectives.

b. Ensure that the inherently conflicting tasks and regulatory protection requirements of bilateral control are separated as a minimum and the adequacy and updating of the job description when adopting and modifying the Bank's organizational structures.

Article (12): Information and Reports:

a. The Board and Senior Executive Management shall develop the infrastructure and systems necessary to provide information and reports to its users as an anchor for the decision-making processes in the bank. Therefore, Information Quality Criteria must be available, which are represented in (Integrity, Completeness, Accuracy and Validity or Currency) and the confidentiality requirements, according to data classification policy, availability requirements and compliance to such information and reports, as well as other requirements contained in the standard (COBIT 5 - Enabling Information) which are represented in (Objectivity, Believability, Reputation, Relevancy, Appropriate Amount Concise Representation, Consistent Representation, Interpretability Understandability, Ease of Manipulation, Restricted Access).
b. The Board or its delegate committees shall adopt information system and reports contained in Annex (7), and consider that system a minimum, taking into account determining the owners of such information and reports through which powers to review and use are determined and delegated as needed for the work and the relevant partners. Provided that

they are continuously reviewed and developed to keep up with the development of the bank's objectives and operations and in accordance with accepted best international practices in this regard.

Article (13): Services, Programs and Infrastructure of Information Technology:

a. The Board or its delegate committees and Senior Executive Management shall adopt system of services, programs and IT infrastructure supporting and assisting to achieve IT governance processes and therefore the objectives of information and related technology, and thus the institutional objectives.
b. The Board or its delegate committees and Senior Executive Management shall adopt system of services, programs and IT infrastructure contained in Annex (8), and considering that system as a minimum, provided that they are continuously provided and developed to keep up with the development of the bank's objectives and operations in accordance with accepted best international practices in this regard.

Article (14): Knowledge, Skills and Experiences:

a. The Board or its delegate committees shall adopt the HR Competencies and human resources management policies necessary to achieve the requirements of IT governance contained in Annex (3) and the requirements of these regulations in general, and to ensure that the right person in the right place.
b. The management of the bank shall employ the qualified and trained personnel from persons with expertise in information technology resources management, risk management, information security management and information technology audit management depending on the criteria of academic and professional knowledge and practical experience accredited by international associations that are eligible under the criteria for international accreditation institutions giving professional certificates of ISO/IEC 17024 and/or any other criteria parallel each according to its competence, provided that currently employed cadres shall be re-qualified and trained to meet the mentioned requirements within two years of these instructions.
c. 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 achieves IT governance processes contained in Annex (3).
d. The executive management of the Bank should include the performance evaluation mechanisms of the staff with objective measurement criteria that take into consideration the contribution through the career center to achieve the objectives of the bank.

Article (15): System of Values, Morals and Behavior:

a. The Board or its delegate committees shall adopt a moral professional institutional codes of conduct that reflects the professional international accepted rules of dealing with information and its related technology that clearly define the desired and undesirable behavioral rules and their consequences.
b. The internal and external auditors shall comply with the system of ethics and professional practices approved by the Board to include –at the minimum - the professional ethics in the Information Technology Assurance Framework (ITAF) issued by the Information Systems Audit and Control Association (ISACA) and its updates.
c. The Board and Senior Executive Management shall employ various mechanisms to encourage the application of desirable behaviors and to avoid undesirable behaviors through the use of incentive and sanctions methods, to name a few.

Governor

Dr. Ziad Fariz

- A number of 8 attachments.

Attachments
Annex No. (1)
Matrix of Enterprise Goals

Goal Code	Goals	Measurements Criteria of Goal Achievement (Examples)
01	Achieving Added Value of Bank Assets and Investments	• Percentage of assets and investments that have met stakeholders' expectations regarding the added value. • Percentage of products and services that have achieved their desired benefits of which. • Percentage of investments that have achieved the desired benefits.
02	Portfolio of Competitive Products and Services	• Percentage of products and services that met or exceeded the expected objectives, revenue and market share. • Percentage of products and services that have achieved customer satisfaction. • Percentage of products and services that have achieved competitive advantage in the market.
03	Overall Institutional Risk Management (Asset Protection)	• Percentage of main goals and services covered by the risk assessments. • The share of major non-identified accidents within risk assessments of total accidents. • Periodic update of risk profile.
04	Compliance with Laws and Regulations	• The cost of non-compliance with the laws and regulations, including fines and settlements. • Number of topics in violation of laws and regulations that have caused negative public opinion towards the bank or notoriety. • Number of topics in violation of terms of contract with third parties.
05	Financial Disclosure and Transparency	• Percentage of assets and investment that have been identified and approved for their budgets and expected returns Percentage of services costs that can be distributed to users. • Percentage of satisfaction surveys that have achieved expected goals by stakeholders regarding financial transparency, accuracy and understanding of the financial statements.
06	Culture of Institutional Customer Oriented Service	• Number of interruptions in banking and financial services due to IT-related incidents • Percent of satisfaction of stakeholders on the provided products and services. • Number of customer complaints. • Time trend of customer satisfaction surveys.
07	Continuity and Availability of Services	• Number of incidents of key and critical services stoppage. • Costs of interrupted operations and services. • Number of hours operation and services stoppage.

		• Percentage of complaints related to the cessation of services and operations
08	Speed of Change in Response to the Requirements of Work Environment	• The level of the Board's satisfaction to speed of response to the new requirements. • Number of services and products serviced by new created operations. • Average time to initiate achieving approved strategic objectives.
09	Decision-Making Methodology Based on Information	• The degree of Board's and senior management satisfaction to decision-making processes. • Number of incidents resulting from wrong decisions based on inaccurate information. • Time taken to provide the necessary information for decision-making.
10	Reducing Costs of Services and Products	• Time trend of costs compared with the level of service. • Periodical evaluation of provided services costs. • The level of satisfaction of the Board and senior executive management towards the costs of services provided.
11	Maximize the Functionality of the Services Provided	• Periodical evaluation of maturity level of the services provided. • The results and direction of the above evaluation. • Satisfaction of the Board and senior executive management on the Bank's operations capabilities.
12	Reducing the Cost of the Bank's Operations	• Periodic evaluation of cost reduction for operations. • Time trend of costs compared with the level of service. • Level of satisfaction of the board and senior executive management over the costs of operations.
13	Management of Change Programs of Business	• Number of programs completed with planned time and pre-estimated budgets • Percentage of stakeholders satisfied with completed programs Percentage of knowledge and awareness of business changes as a result of IT initiatives.
14	Operational and Labor Productivity	• Number of programs/projects completed by time and allocated budgets. • Levels of costs and operating labor compared to targets.
15	Compliance with Internal Policies	• Number of accidents resulting due to non-compliance with internal policies. • Percentage of stakeholders who are knowledgeable and aware of internal policies. • Percentage of the Bank's active policies.
16	Skilled and Motivated Staff	• Level of satisfaction of stakeholders with staff experience and skills • Percentage of jobs filled with less than the required skills, experience and knowledge. • Level of job satisfaction.
17	Culture of Excellence and	• The level of knowledge and awareness of the opportunities for

	Innovation	innovation and excellence. • Satisfaction of Stakeholders towards the level of excellence, creativity and ideas. • Number of products and services offered and approved resulting from the creative initiatives and proposals.

- Due to technical considerations, it is allowed to use English in writing the attachments.

Annex No. (2)

Matrix of Information and Related Technology Goals

Goal Code	Goals	Measurements Criteria for Goals Achievement (Examples)	Numbers of Directly Related Enterprise Goals *
01	The strategic plan for information technology is aligned with the strategic plan of the Bank through a methodology for strategic decision-making of information technology that is efficient and meets the requirements of the internal and external working environment	• Percentage of the bank's strategic objectives supported by strategic IT objectives. • satisfaction level of the bank units to portfolio of planned and implemented projects and services over the realizable requirements efficiently and effectively, and can be measured through a questionnaire method to name a few.	01, 03, 05, 07, 11, 13
02	IT practices compliance and their contribution to the Bank's compliance with laws, bylaws and instructions in force	• The cost of information technology non-compliance, including the required cost of correction, in addition to the impact on the Bank's reputation in this regard. • Number of observations of non-compliance with information technology requirements submitted to the Board of Directors or those that raise public opinion • Number of observations of non-compliance with contractual terms and conditions with third party information technology services providers. • Include the examination of processes for compliance requirements	01, 05, 07, 09, 12, 17
03	The commitment of the management to make informed decisions based on information technology	• Percentage of tasks and duties related to information technology from the total tasks and duties of the job description of the Bank's functions. • Number of times in which topics related to information technology are discussed in the meetings of the Board of Directors. • Periodic and regular meetings of the IT governance Committee, and the IT Steering Committee	04, 10, 16
04	Information Technology Risks Management for Bank's Operations	• Percentage of critical bank operations based on IT resources and infrastructure included in risk assessment processes • Number of major IT incidents not considered in risk assessment	02, 10

		• Proportion of operations with IT risk to total operations included in the risk assessment • Periodical update or risk profile.	
05	Ensure achieving benefit and added value of projects, resources, and information technology services portfolio	• Percentage of IT projects in which benefits and added value are monitored and measured during the life of the project. • Percentage of IT projects and services that have achieved targeted benefits and results and those that exceeded targets.	06
06	Transparency in disclosing costs, benefits and risks of information technology	• Percentage of projects in the Bank in which expenses and expected benefits of information technology are determined and approved. • Satisfaction surveys on the level of disclosure, understanding and accuracy of financial allocations for IT projects and services	01, 07
07	Provision of information technology services to meet the requirements of the Bank's operations	• Number of times the Bank's operations stopped due to incidents and disruption of information technology services. • The level of satisfaction by the departments of the Bank to the IT Department to meet the requirements of works at agreed time and specifications within the agreements of the level of external and internal services (SLA, OLA)	04, 10, 14
08	Appropriate use of the software and IT solutions	• Percentage of the Bank's operations officials who are satisfied with products and services of information technology. • Level of the Bank's operations officials understanding of software solutions and the characteristics of information technology to support their operations. • The level of satisfaction with the training provided to users of information technology, and the adequacy of the software manual and the various solutions	01, 07, 09, 17
09	Flexibility of operations and management of information technology resources	• Level of satisfaction of Bank officials in responding to their IT requirements • Number of Bank operations serviced by modern resources of information technology. • Average time taken to translate the Bank's strategic objective into an IT initiative	01, 14

10	Information security, software operation and IT infrastructure	• Number of incidents of information security that caused financial loss, interruption of operations or impact on reputation • Number of IT services in which security requirements of information technology are specified. • Period of time required for modifications required on the level of users access to privileges. • Periodic assessment of information security data, according to the latest accepted international standards.	04, 06, 11
11	Optimal Use of Information Technology Resources and Capabilities	• Periodical assessment of the maturity degree and costs of IT resources. • Results and direction of the above assessment. • Level of satisfaction of the bank's management as a whole on the capabilities of information technology and size of costs.	01, 07, 08, 09, 12
12	Supporting work mechanisms through the integration of applied software and technology resources within the Bank's operations	• Number of incidents resulting from software integration errors • The number of crashes in the Bank's operations due to the breakdown of software and information technology • Number of times of projects disruption or delay due to the infrastructure and information technology problems. • Number of non-integrated software and solutions which operate in isolation from other software and solutions.	05, 06, 11
13	The implementation of projects within the time and budgets set in advance within the framework of portfolio management of projects that comply with international rules and standards in this regard	• Number of projects implemented within the time limits and allocated budget. • Percentage of stakeholders' satisfaction for quality of project management. • Number of projects that require re-implementation because of poor quality in performance and achievement of goals • Ratio of maintenance costs to total IT costs	01, 03, 13
14	Availability of reliable and useful information that are based on in decision-making	• Level of the Bank departments' satisfaction on the quality and availability of information systems.	08, 16

		• Number of incidents of the Bank's operations due to lack of availability of information and technology. • Percentage and importance of the Bank's wrong decisions because of the limited availability of information and technology.	
15	Compliance of IT practices with the Bank's internal policies	• Number of IT incidents resulting from non-compliance with policies. • Percentage of individuals with correct understanding of the policies. • Percentage of policies that stimulate international best practices. • Periodic review and update of policies.	02, 10, 15
16	The level of skills and competitiveness of the bank's staff in general and IT cadres	• Percentage of employees with sufficient IT skills for work requirements • Satisfaction of employees with their IT tasks • Number of training and learning hours of employees.	16
17	Acquire knowledge and experience in technological innovations that can be provided to develop the bank's operations	• The level of knowledge in the bank's operations and the technological innovations that can be provided to support these operations • Level of satisfaction of operation owners for provided innovative technological ideas and creativity. • Number of completed operations and projects resulting from technological innovations.	09, 17

- Due to technical considerations, it is allowed to use English in writing the attachments.

* Enterprise Goals numbers from Annex 1 that directly relevant to the associated information and technology objectives

Annex No. (3)

IT Governance Processes

Process Code	Process Title	Process Description	Process Goal	Numbers of Goals of Directly Related Information and Related Technology Goals*
Evaluate, Direct and Monitor (EDM)				
EDM 01	Ensure Governance Framework Setting and Maintenance	Analyzing and clarifying IT governance requirements, developing and continuing to develop and update IT policies, principles and procedures, and related organizational structures, with a clear definition of responsibilities and competencies to achieve the Bank's objectives.	Establish an integrated methodology that complies with the general framework of corporate governance to ensure that IT decisions are in line with the Bank's strategic objectives and that information technology operations are efficiently and transparently monitored within the framework of compliance with the Bank's strategy and policies, regulations, bylaws and laws in this regard.	01,03,07
EDM 02	Ensure Benefits Delivery	Maximizing value added through the Bank's operations and IT resources at an acceptable cost.	Optimize and maximize the benefits of IT resources at the lowest possible cost to meet and achieve business requirements.	01,05,06,07,17
EDM 03	Ensure Risk Optimization	Appropriate understanding of risks in terms of risk appetite and risk tolerance and to justify the added value and benefits of accepting these risks, as well as to clarify, document and connect these rules to the concerned parties	Ensure that IT risks do not exceed the specific appetite and risk tolerance, ensure that information technology risks are identified and managed and that the likelihood of violating laws, regulations and instructions is minimized.	04,06,10,15

EDM 04	Ensure Resource Optimization	Ensuring the appropriateness and availability of operational and IT resources (human resources, business processes, and technology) to meet the Bank's objectives efficiently with minimal cost.	Ensure optimal utilization of resources, including information technology resources, and that there is a possible increase in realized benefits	09,11,16
EDM 05	Ensure Stakeholder Transparency	Ensure transparency in operations and reports on performance assessment of IT management, and ensure that the objectives and standards of corrective action are identified and approved	Ensure that benchmarking reports of relevant IT resources are communicated to the time needed to improve performance, identify who needs improvement and that IT objectives are aligned with the Bank's strategic objectives	03,06,07
Align, Plan and Organize (APO) Processes				
APO 01	Manage the IT Management Framework	Clarify and continue to update the vision and mission of IT governance, continue to employ mechanisms and delegate authority to manage information using technology to achieve Bank objectives within the framework of commitment to the principles and policies.	Use a consistent management methodology to achieve IT governance requirements that includes all the required organizational structures, roles, responsibilities, activities, processes, skills and experience.	01, 02, 09, 11, 15, 16, 17
APO 02	Manage Strategy	A comprehensive description of the Bank's current situation and the IT environment and a vision of the future direction includes the initiatives required to move to the future business environment, and to utilize the resources and capabilities of the Bank and the services provided and used by third parties effectively and reliably to achieve the Bank's strategic objectives.	Align the strategic objectives of information technology to meet the achievement of the Bank’s objectives, and to define responsibilities towards achieving the objectives clearly and to ensure that they are properly understood by the stakeholders	01,07,17
APO 03	Manage Enterprise Architecture	Establish the overall structure of IT management including the Bank's operations, information, data, software and IT infrastructure for the purpose of achieving the technology objectives and the Bank's strategic objectives efficiently and effectively through	Identify the different data needed to build IT management, define the principles and procedures used and describe the relationships between them to reach the Bank's operational	01,09,11

		the establishment of key business models and practices,, and determine the necessary requirements for a set of principles, procedures, and tools correlated with each other, and work to improve the level of compatibility between technology and the requirements of the Bank's work, and increase the agility of IT services, and improve the quality of information and technology used to manage the Bank's operations	and strategic objectives	
APO 04	Manage Innovation	Increasing awareness of what is being offered in the new information technology market to study the possibility of using it to support the Bank's current and innovative operations to achieve the strategic objectives of the bank.	Achieve the Bank's competitive advantage by developing and increasing the efficiency and effectiveness of the Bank's operations based on new IT	05,08,09,11,17
APO 05	Manage Portfolio	Implementing various information technology projects that meet the objectives and strategic direction of the Bank, taking into account the limited resources and therefore the optimal utilization of them, and work on assessing and prioritizing the projects based on their contribution to achieve the strategic objectives and the level of opportunities and risks corresponding thereto, and work on the recruitment of project products to mechanisms and tools serving the bank's operations, continue to monitor the benefits and value added level of the portfolio of projects and make timely adjustments based on feedback from such controls and on changes in the Bank's business plan.	Maximizing the benefits and optimal utilization of resources through a comprehensive management of the projects portfolio of the Bank	01,05,13
APO 06	Manage Budget and Cost	Managing the financial affairs of IT resources through the financial and IT management mechanisms of the Bank, including the preparation of budgets, the study of costs and benefits, and the prioritization of disbursement, through the use of unified objective	Consolidate the participatory relationship between the IT management and stakeholders in the Bank to ensure optimal utilization of technology resources and provide	05,06

		standards approved by the Bank in this regard, working in consultation with stakeholders To adjust the allocations allocated to serve the strategic and tactical objectives of the Bank	information in this regard with high transparency that facilitates accountability, quantification of benefits and value added, and facilitates decision-making mechanisms in the recruitment of IT resources	
APO 07	Manage Human Resources	Employ a methodology that ensures the creation of organizational structures and horizontal and vertical institutional lines of communication, the recruitment of skilled and efficient human beings, the distribution of powers, functions, roles and responsibilities, the creation of training and continuous learning plans, and the continuous motivation of staff to achieve the required performance.	Optimize human resources to serve the Bank's objectives.	01,11,13,16,17
APO 08	Manage Relationships	Managing the relationship between the IT Department and the rest of the Bank's departments to ensure a permanent and transparent institutional connection that supports the common interest in achieving the Bank's objectives within acceptable and approved budgets and risks, and extending trust through a language of mutual understanding that promotes a positive spirit of decision-making and responsibility.	Improve results, increase confidence, and efficient reliance on IT resources.	01,07,12,17
APO 09	Manage Service Agreements	The level of quality of information technology services is consistent with the Bank's expectations and needs, including mechanisms for identifying, defining, designing and requesting such services, documenting third party contracts and setting standards for continuous monitoring of the quality and level of such services	Make sure that IT services are provided to a level of quality and meet the Bank's current and future needs	07,14
APO 10	Manage Suppliers	Management of third-party IT services to support the Bank's operations and objectives, including suppliers selection and communication mechanisms, contract	Reduce the level of risk as much as possible by the use of the services provided by third parties and to	04,07,09

		management, monitoring and evaluation of their performance to check efficiency, effectiveness and compliance with contractual terms with them	ensure access to these services at the lowest possible prices	
APO 11	Manage Quality	Define quality requirements in all processes, mechanisms and procedures of the Bank, including controls and continuous monitoring processes and use the practices and standards required for continuous development	Ensure the provision of technology solutions and services that meet business needs and receive the satisfaction of its users	05,07,13
APO 12	Manage Risk	Continue to identify, evaluate, adjust and control the risks of information technology to keep it within the target levels of risk accepted and approved by the Bank	The integration of IT risk management with the overall management of the risks in the bank, and to maintain the desired balance between benefits and costs	02,04,06,10,13
APO 13	Manage Security	Definition, operation and control of information security management system	Maintain the magnitude of the impact and probability of the occurrence of IT incidents within acceptable levels of risk appetite	02,04,06,10,14
Build, Acquire and Implement (BAI) Processes				
BAI 01	Manage Programs and Projects	Manage all the Bank's projects to achieve strategic objectives in a cooperative manner between the IT department and the other concerned departments through the planning, control and implementation mechanisms of the projects and the continuation of project evaluation in the post-implementation stages	Ensure the benefits of project management and reduce the level of risk and delay costs through proper communication between users and IT management.	01,04,05,13
BAI 02	Manage Requirements Definition	Analysis of the needs and requirements of IT solutions prior to the acquisition and development of such solutions including work mechanisms, programs, data / information, infrastructure and services, to ensure consistency with strategic objectives of the Bank, and coordination when considering options with technology users including feasibility study, risk analysis, costs, benefits and approvals Required	Providing cost effective solutions that meet business needs.	01,07,12
BAI 03	Manage	Selection and development of IT solutions that meet	Providing IT solutions with the	07

	Solutions Identification and Build	the requirements and needs of the work including the mechanisms of design, development, procurement and outsourcing. Including configuration management, solution screening mechanisms, needs management and identification, maintenance and continuous development of software, work mechanisms, data / information, infrastructure and services	required time and at the lowest cost to serve the Bank's objectives	
BAI 04	Manage Availability and Capacity	To balance the required IT services between the present and the future, taking into account the costs and performance level, including the identification of current and future capabilities based on the needs and plans of the bank, through business impact analysis and risk assessment.	Availability of IT services, efficient resource management, maximizing systems performance by anticipating future capacity.	07,11,14
BAI 05	Manage Organizational Change Enablement	Maximize the probability of successful corporate change processes quickly with minimal risk including change mechanisms, bank operations, IT and individuals	Prepare and ensure individuals' commitment to institutional change successfully and with minimal risk	08,13,17
BAI 06	Manage changes	Management of all amendments through the provision of necessary controls and amendment policies including emergency and urgent adjustments and modifications to the Bank's operations, software and technology infrastructure, as well as the provision of standards and procedures for the amendment, include measuring the impact of the amendment to the processes, and priorities in the amendment, and approvals required for the amendment and procedures for emergency modifications, and extract reports tracking adjustments, closure and documentation	Make the required adjustments as soon as possible and with the least possible risks of any adverse effects that affect the credibility of the amendments	04,07,10
BAI 07	Manage Change Acceptance and Transition	Operating IT solutions after taking formal acceptance approvals from user management, including pre-implementation planning, data migration, and acceptance of successful use testing.	Run technology solutions safely in line with expectations.	08,12

BAI 08	Manage Knowledge	Provide and maintain an up-to-date and reliable knowledge system to support the bank's operations and to help make sound decisions. Knowledge Lifecycle Management: Planning, gather knowledge, classify, regulate, update, use and delete.	Provide knowledge for staff to enable them to perform their duties, and raise the level of productivity	09,17
BAI 09	Manage Assets	Management of IT assets throughout their lifecycle to ensure that they achieve the desired benefits at the lowest possible cost, that they are suitable for the operations under them, that they are numbered and protected, that important assets to support sensitive banking operations are continuously available and reliable, and to manage the software licenses to ensure that they are sufficient to support the operations of the bank and that their use is within the limits of applicable laws.	Accounting and optimization of IT assets	06,11
BAI 10	Manage Configuration	Describe each of the bank's main resources on the one hand and the IT capabilities required to provide technology services on the other, and define the relationship between them, including the collection of different definitions information and the establishment of the standard basis for the definitions and subject them to periodic reviews and ongoing audits.	Provide adequate information on the services and characteristics of the assets of information technology to efficiently manage these assets, and the impact of changing those characteristics on business in terms of information security and technology	02,11,14
Delivery, Service and Support (DSS)				
DSS 01	Manage IT Operations	Coordinate and implement internal and third-party IT activities and processes, including the development of operational and control standards and policies	IT Operations as planned in this regard.	04,07,11
DSS 02	Manage Service Requests and Incidents	Responding in a timely manner to user requests and all types of IT events, restarting technology processes after interruptions, documenting user requests, investigating and diagnosing technology breakthroughs, and informing and addressing the relevant administration	Increase productivity and reduce interruptions by responding quickly to user requests and handling IT incidents.	04,07

DSS 03	Manage Problems	Identify and classify information technology failures, including their main causes, to prevent accidents, and make recommendations and improvements required	Increase the availability rate and the level of information technology services and reduce costs and improve the level of satisfaction by users of technology by reducing the number of failures	04,07,11,14
DSS 04	Manage Continuity	Create and develop a plan to manage the continuity of the Bank's operations and information technology to serve the Bank's sensitive and critical operations to address the causes and incidents of interruptions within the limits targeted in this regard	Ensuring the continuity of critical bank operations and supporting IT operations to meet breakout incidents within targeted limits	04,07,14
DSS 05	Manage Security Services	Protect the Bank's information and maintain it at an acceptable risk level within the framework of the Bank's information security and protection policies, and to establish and continue to update the roles and responsibilities of the Information Security Department, access and use privileges and use and monitor the use of the resources of technology	Reduce the negative impact on the Bank's operations due to incidents and weaknesses of information security	02,04,10
DSS 06	Manage Business Process Controls	Identify, define and continue to employ the operational controls of the bank to achieve the specific security requirements of the information and technology associated with them, whether executed internally or relying on third parties.	Maintain the integrity, credibility and security of information processed by the bank's operations or processes by third parties helper.	04,07
Monitor, Evaluate and Assess (MEA) Processes				
MEA 01	Monitor, Evaluate and Assess Performance and Conformance	Collecting, verifying and evaluating the objectives and criteria for measuring the performance of the bank's operations, including the operations of information technology and work procedures, monitoring these operations to ensure that the objectives are achieved and to report on this matter periodically.	Transparency regarding the performance level towards achieving the goals.	04,07,11,15
MEA 02	Monitor, Evaluate and	Continuous monitoring and evaluation of the environment of internal controls by both the self-	Provide transparent information to stakeholders regarding the safety and	02,04,15

	Assess the System of Internal Control	assessment and independent evaluation, and enable management to identify imbalances in the effective controls to take needed improvements and corrections, planning, organizing and updating the evaluation principles and rules of the Bank's internal control system	proper of the bank's internal control system in contributing to the bank's objectives by properly understanding the bank's residual risk levels.	
MEA 03	Monitor, Evaluate and Assess Compliance with External Requirements	Assess the level of compliance with the practices of each of the Bank's IT-based operations and laws, regulations and instructions and the terms of contracting with third parties, obtain assurance of the identification of legal and contractual requirements and the level of compliance with them; and consider compliance with technology requirements as part of overall compliance with the Bank's practices and operations	Making sure that the Bank complies with the laws, regulations and instructions.	02,04

- Due to technical considerations, it is allowed to use English in writing the attachments.

* Number of objectives of information and its related technology of the annex No. (2) directly related to governance operations of information technology.

Annex No. (4)

Governance and Management of Information and its Related Technology report Form

(Auditor's Name or Audit Company)

Assessment Report (Risk - Controls) of Information and its Related Technology Of Bank ..... Public (or Regional) Administration - Amman/Jordan (or home country of the branch)	
Audit period From - To Number of work days ( ) Day/Days	
Name of Responsible Auditor	With an attached supplement on qualifications, experience and copies of professional certificates and fellowships
Audit Team Members Names	With an attached supplement on qualifications, experience and copies of professional certificates and fellowships

First: <u>Form of the Board's review and recommendations on the report:</u>

Name	Position	Revision Signature and Date	Recommendations/Notes

Second: <u>Introduction</u>: (Due to technical considerations, it is permitted to use English in writing the report)

1. **Composite Risk Rating: Rating (risks - controls) of information and its related technology:**

   (Risks - controls) of information and its related technology have been rated at the bank with ( ) degree. **Based on the following rating axes**, knowing that rating degrees are divided in descent order to five levels (Composite Risk Rating): (Strong Performance, Rate 1), (Satisfactory Performance, Rate 2), (Fair Performance, Rate 3), (Marginal Performance, Rate 4) and (Unsatisfactory Performance, Rate 5):

   a. IT governance and its related technology has been rated by ( ) degree.
   b. Applications has been rated by ( ) degree.
   c. Data management has been rated by ( ) degree.
   d. Main computers and managing them has been rated by ( ) degree.

e. Networks has been rated by ( ) degree.
f. Emergency plans, work continuity and physical and environmental protection has been rated by ( ) degree.

2. Examination and Evaluation Methodology:

The following evaluation methodology was followed for the weaknesses mentioned in the above-mentioned axes:

a. Quantity of Risk:

Has been calculated and rated based on the following function:

Quantity of current Risk = [Weakness * Threat] (Note) * Importance – Activated Controls

In other words, the assessment of current risk is based on the importance of the weakness and threat of the (note), taking into account buffers represented in activated controls, Where risk levels were divided down to three levels (high, medium, low) (it is possible to choose a more detailed rating system). The importance (i.e. inherent risk) is divided in descent order into four levels (critical, essential, medium, low), and controls were divided in descent order into four levels (excellent, good, suitable, weak). Knowing that the risk-based approach has been followed in terms of assessing the risk aspects and the negative impact on the Bank's operations.

b. Quality of Risk Management:

It has been estimated based on quality of bank's operational risk management in terms of availability of a risk strategy or risk policy approved by the Board that represents the bank's vision and Risk Appetite. In addition to reliance on an administrative institutional structure for the implementation of the strategy and a mechanism to determine, measure, control and monitor the risk, taking into account response and cooperation degree, existence of future correction plans, quality of risk management in terms of mitigate, transfer, accept, avoid and reject the risks. Quality of risk management has been divided in descent order into three levels (strong, acceptable, weak) (it is possible to choose a more detailed rating system).

The following is a table summarizing the evaluation of the observations contained in the report and determines responsibility:

Note Code	Note	Responsibility	Risk Quantity	Risk Management Quality
Axis serial number: sequence in the same axis	Note title	position of the responsible person or authority / authorities	Choosing color of risk rate	Choosing color of risk rate

3. **Report Discussion:**

On / / the report was sent to the bank's management in preparation for a meeting with concerned parties to discuss its contents. On / / the meeting was held with the management of the bank represented by ……, and the meeting achieved its goals in terms of:

a. Confirming the credibility of audit report contents.
b. Confirming the bank management's right understanding of audit report content.
c. Agree on dates in which bank management shall be committed to in order to correct gaps and weaknesses contained in the audit report.

4. Report Determinants:

Any determinants that negatively affects the course or result of auditing job shall be mentioned, for example but not limited to not providing required data or information in the proper way or at the required date, the extent of cooperation of the Bank's management with the auditor and facilitate his task, and any other barriers or determinants.

5. Qualifications and Experiences of the Responsible Auditor members of the audit team:

(Shall be mentioned).

Third: <u>Body of the Report</u>: The details of the above evaluation are shown below**:**

(Contains six evaluation pillars that should cover minimum requirements for governance and management of information and its related technology instructions)

1. Information Governance and management and its related technology:

It shall be rated by above mentioned component risk rating as follows:

Note (1:1): information Governance and its related technology: (it is mentioned as an example, other notes shall be described in the axis)

Evaluation of Note (1:1)								
Importance	Critical	X	Essential		Medium		Low	
Controls Evaluation	Excellent		Good		Suitable		Weak	X
Amount of risk	High	X	Medium		Low			
Quality Risk Management	Strong		Acceptable		Weak	X		

Vulnerabilities that forms weaknesses in controls, systems and procedures are characterized, in addition to characterization of possible threats. In effect, the impact, either financial, operational, legal or reputation…. etc. is characterized.

Recommendation:

The actions to be taken by the Bank's management are described in order to reach the acceptable risk.

Bank Management's Response:

Bank management's response shall be mentioned.

2. **Applications:-**

   Are rated as ( ) degree, as follows:

3. **Data Management:-**

   Are rated as ( ) degree, as follows:

4. **Main Computers, Including Operating Systems and Other Software (Servers):-**

   Are rated as ( ) degree, as follows:

5. **Local Computer Networks, WANs, Internet, Intranet and Support Systems:-**

   Are rated as ( ) degree, as follows:

6. **Business Continuity and disaster recovery plans, physical and environmental security:-**

   Are rated as ( ) degree, as follows:

Fourth: <u>Table of notes that have been suspended and not processed several years ago:</u>

Note	Description of the Note	Amount of risk	Risk Management Quality	Action taken by the Bank's management and history	recommendation

Annex No. (5)

Auditing Information and its Related Technology items

IT Governance
The sufficiency and efficiency of achieving IT governance processes contained in Annex no. 3 and the instructions of Central Bank of Jordan in this regard through applying monitoring, evaluation and measurement (MEA) processes in the mentioned Annex.
The level of strategic alignment between IT objectives and the organization's objectives
The efficiency and effectiveness of security and information protection policies
Level of user satisfaction with IT management, services, products and technical support provided
The efficiency of the committees of information technology in terms of tasks, scope of work and activity
The efficiency of organizational structures, ensuring non-conflict of interests and segregation of conflicting tasks by their nature
The sufficiency and efficiency of the skills and qualifications of respective internal audit, external audit and IT consultants
Sufficiency and comprehensiveness of job description for the IT staff and internal audit of information technology and information security
The sufficiency of the IT risk management, operational risk and operational practices in risk-based decision-making mechanisms, including IT risks and strategic risks
The sufficiency and the organization of information security management in terms of organizational structures and employing various resources including the human element
Is there project portfolio management? What is its sufficiency and regulation?
Compliance with instructions, laws, legislation and related regulations of the Central Bank of Jordan
The compliance of the Board of Directors and Executive Management with IT governance instructions
The extent of the use of tools and programs to detect fraud (CAATS) like (ACL, IDEA) by audit
The existence and sufficiency of outsourcing policies.
Sufficiency of the documentation of external and internal contracts and their appendices, such as the presence of service level agreements, operational level agreements, etc. in terms of detail of the services provided and responsibilities
The sufficiency and organization of training programs to increase the level of awareness and dissemination of good practice for the security and protection of information for each of the bank's employees and customers, and the availability of standards in this regard in the form of rules of professional conduct
Application Software and Management
The sufficiency and efficiency of applicable and applied procedures dealing with mechanisms of development, purchase, testing and operating programs
The sufficiency and integrity of the definition of procedures for the definition of staff privileges

on programs based on the nature of the work (Role based access privileges
The extent of information security management engages in granting and prior consent to access and use of sensitive programs
Checking controls of sensitive data entry programs (such as the presence of Maker, Checker)
Checking outputs controls and custody of sensitive documents extracted from different programs
Examine the integrity of programs in Data Processing and reliability of input and output
Check the operation controls for electronic channels and electronic payment systems
The extent of using Computer Aided System Engineering (CASE) program in documentation and follow-up processes
The extent to which major programs have received qualification certificates from recognized international rating institutions (Accreditation)
Compliance with the instructions of Central Bank of Jordan regarding the automated classification of facilities
Database Management
Efficiency and activation of data displacement policies, and database management
Efficiency and sufficiency of specialized staff in Database Administrators (DBA)
Efficiency and sufficiency of applied procedures to monitor and improve the performance of databases and data in general
Checking protection controls concerning the separation of databases management powers from data itself to protect from risk of penetration and unauthorized modification by databases officer
Efficiency and activation of backup procedures
Efficiency and activation operation of monitoring use of (DBA) by separate management such as information security
Efficiency, activation and reliance on mechanisms such as the Error Dictionary to address the mistakes and problems of data management
Managing Main Computers
Efficiency and activation of backup procedures of systems configurations
Efficiency and activation of devices performance monitoring procedures
Efficiency and activation of systems examination procedures at every change (upgrade, development)
Efficiency and activation of audit reports to track usage of systems managers (Administrators Logs), and are they reviewed by a separate party like (Security Administrator)
Efficiency and activation of documented procedures to address operating errors
Efficiency and activation of procedures of changing passwords for system administrators access and users with high privileges
Efficiency and sufficiency of Vulnerability Assessment and Penetration Tests
Checking the level of availability of main computers (Clustering, Fault Tolerant ... etc.)
Sufficiency of operations of separating development and testing environment for operating environment
Networks Management
The existence, efficiency and activation of definition and network management policies
The extent of using networks to disseminate and raise awareness of the practices of security and protection of information to the Bank’s employees and customers
Existence and efficiency of Help Desk

Sufficiency and efficiency of specialized staff in the Network Administrators
Sufficiency and efficiency of strict procedures for change management
Compliance with licensing of software and intellectual property rights
Adequacy and effectiveness of procedures for monitoring the performance of networks and tools used for monitoring
Checking the level of availability of network elements and their suitability for business continuity plans
Sufficiency and efficiency of network usage control procedures (supervisory control by the network administrator or his / her authorized representative, and independent monitor by the information security management
Encryption power used by data transmission via WAN and those open with others
Examine Firewalls and specifying the level of OSI/ISO that works on it (example of the third-level Network Layer, or seventh-level Application Layer) and sufficiency of security standards, confidentiality protection, privacy and credibility of data in particular.
Sufficiency and effectiveness of separate management procedures such as information security to review and monitor amendments on Firewall security policy (ACL) and to track usage by Network Administrator.
The extent of using IDS/IPS devices on networks, and the sufficiency and effectiveness of the procedures regarding audits in this regard.
Sufficiency of activated protection controls for remote access processes (On-line Access and Use)
Management of Business Continuity Plans, Physical and Environmental Security
Sufficiency and efficiency of business continuity plans, including high availability of IT resources, human element and Procedures and organization of plans Within the framework of compliance with the instructions of the Central Bank of Jordan in this regard
Sufficiency and efficiency of assets inventory procedures, such as hardware, software, and information systems
Sufficiency and effectiveness of protection of different devices from unauthorized access procedures and viruses, such as access across networks through computers equipped with outlets (CD Rom, USB ... etc.)
Sufficiency of physical protection procedures of elements and components of networks from unauthorized access, such as the existence of Open Ports for ineffective network elements
Sufficiency of physical protection procedures of network elements (Switches, Routers, ... etc.) from unauthorized access
Examination of the physical and environmental security requirements of the operating rooms of the original and alternative data centers and communications, based on the evaluation criteria, such as suitability of the site, suitable temperature and humidity, raised ground, the location of the room in the building, and existence of automatic fire extinguishers and their type (type of used gas if it is allowed to use under Jordanian and international standard), fire alarms and water leak detectors, surveillance and recording cameras,, visitor log, and restricting access to authorized persons only and controls used in that
Sufficiency of the procedures for the periodic review of the visitors' file for the Bank and for the data center and communication

- Due to technical considerations, it is allowed to use English in writing the attachments.

Annex No. (6)

Policies System (Minimum)

Policy Name	Purpose	Scope
Governance of information technology organization	Setting necessary rules and standards for the management of information technology resources, including administrative form (centralized or decentralized), and organizational structures, including the activities, functions and responsibilities of the management of these resources, including financial resources.	Operations, services and projects of information technology.
Information Security	Setting rules and standards to ensure the requirements of protection, confidentiality, reliability, availability and compliance with the management of IT resources according to accepted international standards such as ISO-IEC 27001/2.	All information and technology associated with it.
Business continuity plans and disaster recovery plan	Establish rules and standards needed to build disaster recovery and human protection plans, business continuity plans, including building, operating, testing, training and updating mechanisms to ensure availability of critical bank operations	Critical bank operations, and human protection
IT Risk Management	Setting rules and standards for IT risk management as part of the Bank's overall risk, including governance of those risks, responsibilities and functions of different parties, and risk assessment and control mechanisms, in order to enhance risk-based decision-making processes and achieve the objectives of the Bank.	All bank operations and information technology inputs.
IT Compliance	Setting the rules and standards necessary to ensure compliance with the instructions of the Central Bank and other regulatory bodies and the applicable laws and regulations and policies of the bank.	All IT operations of the Bank
Data Privacy	Setting rules and standards necessary to protect private data relating to natural or legal persons from unauthorized disclosure and use	All data.
Outsourcing	Adopting a general policy for the use of resources in general and IT resources in particular, those resources, whether in-sourcing or outsourced, take into consideration the instructions, bylaws and laws and reflect the accepted international best practices in this regard and take into account the (on- site, Off-site, Near-site, Off-shore), taking into account the requirements of Service Level control and activation Audit Right by reliable third parties, and ensuring business continuity and security controls to meet the requirements of Confidentiality and credibility in addition to the requirements of Efficiency and effectiveness in resource utilization.	All the bank's operations.

Project Portfolio Management	Setting rules and standards for the projects management, including project phases and governance, to meet quality requirements and those related to Confidentiality Requirements and those related to compliance to achieve the objectives and operations of the bank.	All Bank projects related to information technology.
Asset management	Setting rules and standards necessary to classify the degree of risks of different data and systems, and to identify the owners and controls of their protection during the stages of their different life cycle.	Data, hardware, software and tools associated with it.
Acceptable use of information technology resources	Setting rules and standards necessary to determine acceptable and unacceptable behavior of IT resources	Hardware, software, applications and networks, including the Internet and e-mail.
Change Management	Setting rules and standards necessary to ensure the credibility of change in terms of documenting necessary approvals from owners of assets subject to change.	All information technology operations.
Central computers	Setting rules and standards to reduce illegal access and use of devices, including access controls for IT staff and those with higher privileges to operating environments, as well as day-to-day management standards for various hardware and software, including protection controls and periodic monitoring and maintenance mechanisms	All central devices owned or managed by the Bank for all development, testing and operating environments, including operating systems and other associated tools
Computer peripherals	Setting behavioral and technical rules and standards to ensure protection of sensitive data stored on devices	All network-related or stand-alone peripherals
Portable devices	Setting behavioral and technical rules and standards to ensure protection of sensitive data stored on devices	All portable devices such as Laptop, PDA, Smartphone, USB Memory Cards, ... etc.
User access management	Setting rules and standards to ensure that the powers and privileges of access to data, programs and devices are provided to users as necessary and minimized to ensure the confidentiality, reliability and availability of information technology resources	All software, hardware, databases, etc.
System Development Life Cycle	Setting the rules and standards necessary to implement the stages of development / acquisition of various software to ensure that it meets the requirements of work through different development methodologies commensurate with the requirements and objectives of the work.	New and old software developed locally and acquired from external sources.

Service Level Management	Setting rules and standards to identify, accept, document, measure, monitor and improve the level of services provided by both internal and external parties to ensure optimum utilization of resources and support the Bank's various operations.	All agreements, contracts and obligations with external parties and parties within the bank.
Back-up and Restore	Setting rules and standards for backup and retrieval mechanisms to ensure data availability, reliability and confidentiality.	Data in operating environments where needed.
Data Retention	Setting the rules and standards for the size of data to be met, whether paper or on-line data, the length of time to keep and the differentiation between the size of available data and the speed and performance of data access	All the hardware and software tools, means and data retention.
systems and equipment Purchasing	Setting rules and standards for differentiation between external suppliers	All the technical equipment and related programs.
Remote Access	Setting rules and standards for the remote network of the Bank's computer networks, to reduce the risk of access to and use of sensitive data and sources of the Bank and of internal control systems for the protection of the Bank's assets and to protect against reputation risks	Parties, internal and external partners such as service providers, and all development, testing and operating environments for devices and networks, including but not limited to Internet networks, encrypted networks, and various communication lines such as Frame relay, ISDN, VPN, DSL, MPLS
Networks	Setting rules and standards to ensure the efficiency and effectiveness requirements in exploiting elements of networks and communications on the one hand and to achieve the requirements of security and protection on the other hand support to achieve the objectives of the Bank.	All network elements in all environments.
Wireless networks	Setting rules and standards in order to protect sensitive data transmitted over wireless networks from interception and illegal use.	Including all the physical and virtual wireless networks.
Firewalls	Setting the minimum rules and standards governing the mechanism of work and protection devices of Firewalls in order to activate them in the required manner to protect and ensure the confidentiality and credibility of the Bank's data and operations and its availability	All the Firewalls operating in all environments such as (DMZ, Proxy, External DNS, VPN, Routers, Switches, Servers, …. etc.)

Penetration Testing and Vulnerability Assessment	Setting rules and standards for testing devices and network elements to ensure that there are no security holes that enable penetration of sensitive data, systems and processes of the bank	All the technical assets of the Bank of centralized computers and peripherals and protection devices and components of networks and software.
Public Branch Exchange	Setting minimum protection rules and standards for the Public Branch Exchange systems to ensure protection and confidentiality of the Bank's data and operations against illegal use	All divider devices owned and not owned by the bank

- Due to technical considerations, it is allowed to use English in writing the attachments.

Annex No. (7)

Information and Reports (Minimum)

Report Title	Content
Authority Matrix	Matrix defines the powers and privileges granted to all programs, databases and network elements, detailing the user name, function and powers or privileges.
IT Risk Factor Analysis	1. Internal threats. 2. External threats. 3. Weaknesses in the management of information technology resources. 4. Weaknesses in the ability of information technology to enable the Bank's operations. 5. Weaknesses in IT risk management.
IT Risk Scenario Analysis	1. Source of the threat (Actor): either internal or external. 2. Threat Type: error, penetration, virus, failure, normal, external events. 3. Event: Disclosure of confidential information, disruption, illegal modification, theft, destruction, ineffective Design, laws and regulations, unacceptable use. 4. Asset or Resource Affected: human, organizational structures, operations, infrastructure, information technology, information, programs. 5. Time: Time of occurrence, the duration of the incident, the age of the accident before it was discovered
IT Risk Register	1. Introduction: asset owner, evaluation team, the valuation date, the subsequent valuation date, Risk Assessment Summary and Risk Management Option. 2. The above IT risk analysis scenario. 3. IT risk assessment in terms of the pivotal calculated risk represented by the probability of the accident (Potentiality) and the size of the impact or Severity. It is preferable to use a double standard for evaluation axes and to show the impact on the Bank's IT objectives and operations using the evaluation axes of one of the global models For example: a. COBIT Information Criteria b. Balanced Scorecard (BSC) c. Extended BSC d. Westerman e. COSO ERM f. FAIR (Factor Analysis of Information Risk) 4. Risk Appetite. 5. Risk management Option Acceptance (if the amount of risk calculated is less than the risk appetite) mitigation, avoidance, conversion). 6. Risk management plan items and follow-up (implemented, or are in progress according to the plan). 7. Key Risk Indicators to ensure that risk appetite and risk tolerance are

	not exceeded (Positive deviation of risk appetite).
RACI Chart	Lists identifying the responsible entity or entities or person or parties, and those Accountable, and the Consulted, and those that are informed, for all IT resource management processes, risk management and information security Supervision and auditing
IT Risk Profile	1. The risk register. 2. Analysis of risk factors. 3. Losses and Near-Misses 4. Audit independent entities.
IT Risk Report	It describes the amount of current IT risks involved in the Bank's operations, and the actions taken or to be taken to manage those risks. The format and presentation of these reports is designed to serve the decision-maker owner of the process/operations under his / her responsibility
IT Risk Map or Heat Map	A graph showing the risk Axes (probability and impact) and risk areas that are acceptable and not acceptable based on risk appetite under colors that help to clarify this and indicate the calculated IT risk inherent in the Bank's operations
Risk Universe, Appetite and Tolerance	A report showing all the risks involved in the process, including IT risk, showing the amount of risk appetite and the risk tolerance ratio
Key Risk Indicators	A measurement standards to be determined and compared to Benchmark to monitor the current risk to make sure they do not exceed the risk appetite, and is determined to be the major benchmarks based on the following criteria: a. Impact: The share and size of the indicator in measuring the impact of risk. b. Measurability. c. Reliability. d. Sensitivity.
Risk Taxonomy	It explains the meanings of terms used in the identification, measurement, management and control of risks, in addition to the measurement standards and expression of risk, so the use of those terms in the same meaning and understanding of all partners in accordance with our instructions in this regard.
Risk and Control Activity Matrix (RCAM)	A matrix showing the amount of calculated risks and the corresponding procedures and controls taken to manage and control these risks and their adequacy
Information Security budget	The planned expenditure on information security for the next year is determined within the general budget of the Bank and in line with the planned projects, including the analysis of the current deviation of the current year's expenses compared with the corresponding budget for the same year
MIS Report	A matrix showing all types of reports produced to show the name and function of the owner of the report, the periodicity of production and action taken
Audit Strategy	The objectives of the IT audit, the scope of audit and the audit programs

	used in the audits are defined
IT Audit Charter and Engagement Letter	An independent charter or within the General Charter of Internal Audit, specifying the powers, responsibilities, nature and scope of IT audit work in accordance with our instructions in this regard. The Engagement Letter signed with the External Auditor shall also be included
IT Audit Plan	A forward-looking, risk-based audit plan is drawn up
HR Competencies	It includes academic, professional and technical certificates and the total experience and skills needed for IT management personnel, IT risk management and operation, IT audit, information security and protection
Assurance Findings Register	Contains all audit points and observations, procedures and follow-up.
Assurance Report Repository	It contains all IT audit reports.
The best international standards for the management of projects and information technology resources, and IT risk management, security, protection and audit on information technology	A library is created with the required references according to international best practices and provided to the Bank staff according to the nature of the work, in addition to the system of laws, regulations and instructions.

- Due to technical considerations, it is allowed to use English in writing the attachments.

Annex No. (8)

Services and Software Infrastructure for Information Technology

Service, Program and Tool Name	Description
Incident Management Services	The total number of individuals, procedures, programs and tools used in the detection and assessment of risks and containment, treatment and responding to accidents and writing and reporting them, close them and to draw lessons from the critical review mechanisms through them.
IT Assets Inventory	Total individuals, procedures, programs and tools used in the inventories of IT assets using solutions such as: • Configuration management database (CMDB) • Asset management systems • Simple Network Management Protocol (SNMP) • Reporting agents
Awareness of information security good practices	The total number of individuals, procedures, programs and tools used to design periodic messages for both internal partners of the bank's staff, and external partners, such as the bank's clients, how to properly handle the minimum requirements for information security, and the use of tools such as: • Training courses (internal and external) • News feeds • Knowledge bases (KBs) • Training tools • Social media • Email • Collaboration tools • Vendor and industry advisories • CERT advisories
	The total number of individuals, procedures, programs and tools used in the Documentation (identification and confirmation) of the identity, use of tools such as: • Biometrics • Certificates • Dongles • Smart cards • Embedded device IDs • One-time passwords (OTPs), fobs, cellular telephones • Username/passwords • Identity as a Service (IDaaS), barcodes, Universal • Product code (UPC) • Certificate revocation list (CRL), ID federation • Root certificates • Key management services • Location services

	• Reputation services • Public key infrastructure (PKI)
Security and protection of logical data and information	The total number of individuals, procedures, programs and tools used in maintaining the confidentiality and reliability and high availability of data and information, and the use of tools such as: • PKI, sniffers, DPI • Encryption services • Firewalls • Packet analyser, sensors • IPS / IDS • Data loss prevention (DLP) • System and device management solutions • Software distribution solutions • Remote management systems • Virtualization and cloud management solutions • Document management • Data classification systems • Application-centric data management solutions • Data obfuscation solutions • Vendor information security advisories and KBs, • Honeypots, tarpits • Antimalware, antirootkit, antispyware, antiphishing
Monitoring of information Security	The total number of individuals, procedures, programs and tools used to ensure the provision of means of continuous monitoring to achieve the goals of security and protection of information, such as: • Logs • SNMP • Alerting systems • SIEM (Security Information and Event Management) • Management dashboards • Network operations centers (NOCs)
IT Audit Software	Software to assist in auditing information technology and fraud detection, and software used in the planning and risk assessment, writing and documentation and access to audit reports, such as: • CAATs (Computer Assisted Audit Techniques) • Document management systems • Planning tool • Tracking issues system • Data analytics/sampling techniques • Workflow systems
Hosting and controls of physical and environmental security for the	Provide minimum physical and environmental security controls as follows: • Take into account that the rooms are in place and that the infrastructure design of the building is protected distant threats floods and potential water leaks and sewage, either below or at the end of the building, near the roofs or any other exposed

servers main rooms and rooms of communications and electricity supply	location. The room space should be adequate to meet the Bank's current needs and take into consideration possible future expansion. • The location of the rooms and the building should be generally unlimited access (either by nature of the location or under exclusive contractual agreements) by all telecommunications companies and from various suppliers • The main server rooms and communication rooms (e.g. Routers, Switches, ..etc) and power supply rooms should be protected by physical and environmental protection so that they are surrounded by armed walls without windows and are isolated in terms of electromagnetic influences that adversely affect computer data and serviced by an adequate, back-up reserve for use by individuals in emergencies, the room must be designed in terms of design with access to electricity and firefighting equipment (e.g., FM 200) according to international and local standards in this regard. It should also be on Raised Floor, They must contain smoke, water, heat and humidity reagents with high sensitivity. Recorded TV and cooling should be provided throughout the room in a fair manner to protect the equipment from high temperature and humidity, with dust extraction devices from the room ,and to be entering an airtight observer so as to prevent unauthorized persons from that, taking into account not to put any signs of third parties on the whereabouts of those sensitive rooms in the bank without escorts authorized. • Server rooms and communication rooms must be equipped with multi-source power outlets and automatic switching, i.e., UPS batteries as well as generators with sufficient power to operate the bank's devices and operations (at least sensitive) in case of main power failure. • Must take into account the requirements of the Civil Defense and the Department of Standards and Metrology (where this is required). • All of the above applies also on servers, telecommunications and electricity alternative rooms (Disaster Recovery Sites).

- Due to technical considerations, it is allowed to use English in writing the attachments.