بنك القاهرة عمّان
CairoAmmanBank

Board of Directors Resolution Adopted on 19/12/2023

Subject: Governance and Management of Information and Accompatnying Technology Guide

The Board of Directors, in its meeting held on 19/12/2023, approves the Governance and Management of Information and Accompanying Technology Guide, attached herewith as a copy.

Yazeed Al Mufti
Chairman of the Board of Directors

SCANWAVE

ISACA®

Governance and Management of Information and Accompanying Technology Guide

بنك القاهرة عمّان
CairoAmmanBank

Revision History

Event	Date	Approving Body	Name	Version No.
Author				
Reviewer				

This guide has been developed based on the instructions of the Central Bank of Jordan No. 2016/65, Circular 10-6-984, and the COBIT 2019 framework issued by the Information Systems Audit and Control Association (ISACA).

Contents

1. Introduction

Cairo Amman Bank, represented by its board of directors and executive management, recognizes the importance of information technology as with all banking units operating in the bank. The bank, represented by its board of directors, executive management, and all business units, whether banking or IT, have worked together to integrate information technology under the umbrella of governance and its management style.

In response to the instructions of the Central Bank of Jordan Circular No. 2016/65 and Circular No. 10-6-984, which align and complement Circular No. 85/2014 dated 30/09/2014 and Circular No. 16/2015 dated 21/5/2015, the bank has taken the initiative to adopt the COBIT 2019 framework for governance and management of information technology in compliance with the instructions issued in this regard.

COBIT 2019 provides a comprehensive framework that helps the bank achieve its goals related to obtaining the highest benefits from information technology by maintaining a balance between highest IT benefits and the lowest risks and resources. The COBIT framework enables the full application of governance and management for all business units in the bank, thus covering all IT functions and responsibilities in the bank.

2. Overview of Cairo Amman Bank

Cairo Amman Bank, established as a Jordanian public company in June 1960, has been committed to utilizing its strong capital base and extensive experience spanning over sixty years to play a leading role in serving the national economy by providing a comprehensive and distinguished range of successful banking services and solutions that meet the diverse needs of its customers.

The bank has also added a new dimension to many projects in society by financing development projects, providing financing for small, medium, and micro projects that contribute to the Jordanian economy. It also meets the immediate needs of its customers by providing personal loans through salary transfers and offering investment services, credit cards, and bank transfers through a distinguished and integrated network of bank branches in Jordan, Palestine, and Bahrain.

Cairo Amman Bank offers its customers a variety of innovative banking services that cater to all customer segments and meet all their banking, financial, and investment needs. The bank also provides electronic banking services through its website www.cab.jo, which allows customers to perform banking transactions wherever they are. These exceptional services reflect the bank's new corporate identity, which embodies the spirit of modernity, openness, and communication to serve all its stakeholders and achieve maximum benefits beyond traditional boundaries. In this regard, the bank has made every effort to cover all areas of the Kingdom by being present in Jordan Post centers.

With its commitment to facilitating customer service, Cairo Amman Bank places in the hands of its customers a wide network of ATMs spread across various regions in Jordan and Palestine. The bank takes pride in being the first bank in the world to use iris scan technology as a means for customers to access their bank accounts, eliminating the need for ATM cards and PIN numbers. The system recognizes the customer's identity and enables them to access their account, whether through the service barrier in the branches or through the ATM, to perform their banking transactions. This aims to facilitate customer experience, provide sufficient protection and safety, and establish the bank as a pioneer in the use of modern technology in the banking sector.

With banking, investment, and financial efficiency, and distinguished expertise, we continue to contribute to the national economy and provide leading banking services that elevate the individual's level in Jordan.

3. Scope

This guide applies to all operations of Cairo Amman Bank that rely on information technology in all departments and branches of the bank. All stakeholders must comply with these instructions, each according to their role and position.

This guide also applies when signing outsourcing agreements with third parties to provide human resources, services, programs, and IT infrastructure to manage the bank's operations and the services, programs, and infrastructure provided before and during the contracting period. This does not exempt the board and the senior executive management from the final responsibility for meeting the requirements of these instructions.

The list below represents the main parties and their responsibilities in this regard:

- Board President and Members: Responsible for overall project/program direction, approving tasks and responsibilities within the project, and providing support and necessary financing.
- External experts and consultants.
- CEO, Group Heads, Executive Operations Managers, and Branch Managers: Responsible for identifying suitable individuals with banking operations expertise to represent them in the project and defining their tasks and responsibilities.
- IT Steering Committee and Project Managers: Responsible for project/program management, providing direct guidance and supervision, recommending necessary resources to complete it, and ensuring all parties understand the requirements and objectives.
- Internal Audit: Directly responsible for their assigned responsibilities according to instructions, participating in the project/program as an advisory and independent monitoring role to facilitate its successful completion.
- Risk Management, Information Security, Compliance, and Legal: Participate in the project/program in their respective roles, ensuring representation of the project/program by all relevant parties.
- Specialists and certified technical and professional framers from within and outside the bank: Act as guides to disseminate knowledge of the framework and facilitate the implementation process.
- According to the instructions of the Central Bank of Jordan, the Board of Directors assumes direct responsibility for the five governance processes (evaluation, direction, monitoring).
- The Board of Directors and Risk Management assume direct responsibility for the risk reduction process (EDM03) and risk management process (APO12).

4. Objectives

The objectives set by Cairo Amman Bank for the institutional governance and accompanying information technology management framework are as follows:

4.1 Meeting the needs of stakeholders and achieving the bank's objectives through the effective management of information and accompanying technology, ensuring:

- Provision of high-quality information as a basis for decision-making mechanisms within the bank.
- Efficient management of IT resources and projects, maximizing their utilization and minimizing waste.
- Provision of the necessary technological infrastructure to enable the bank to achieve its objectives.
- Enhancement of various bank processes through the utilization of an efficient and reliable technological system.
- Effective management of IT risks, ensuring necessary protection for the bank's assets.
- Assisting in compliance with laws, regulations, and instructions, in addition to complying with internal strategies, policies, and procedures.
- Improvement of internal control and audit systems.
- Maximizing user satisfaction with IT services by efficiently meeting their needs.
- Managing external service providers responsible for executing operations, tasks, services, and products.

4.2 Separate the operations, tasks, and responsibilities of the board related to governance from those within the executive management's responsibility regarding information and its accompanying technology.

4.3 Achieve comprehensiveness in the governance and management of information and its accompanying technology by considering not only the technology itself, but also providing enabling elements (foundations) that complement IT services. These elements include: 1) principles, policies, and frameworks, 2) IT governance processes, 3) organizational structures, 4) information and reporting, 5) IT services, programs, and infrastructure, 6) knowledge, skills, and experiences, 7) values, ethics, and behaviors.

4.4 Adopt international best practices and rules in work and organizational structure as a starting point to build upon in the areas of governance, operations, projects, and IT resources management.

4.5 Enhance self-regulation, independent control, and compliance examination in the domains of governance and the management of information and its accompanying technology, contributing to continuous improvement and development of performance.

5. General Policies

5.1 This guide is based on the instructions of the Central Bank of Jordan No. 2016/65 and Circular 10-6-984, which were based on the COBIT framework. This guide should be reviewed and updated regularly to align with updates to this framework.

5.2 The guide is adopted by the board of directors. The bank, through the IT governance committee established by the board of directors, reviews and updates this guide as needed. This guide reflects the bank's perspective on information and technology governance and management, including its concept, importance, and basic principles.

5.3 The bank publishes this guide on its website and through any appropriate means. The bank also discloses in its annual report the existence of a special guide for information and technology governance and management or an included guide to its institutional governance, as well as the information that concerns stakeholders, including the guide, and its level of compliance with its contents.

5.4 5.4 Cairo Amman Bank adopts a comprehensive cybersecurity program and a set of policies and procedures related to cybersecurity, in line with the instructions of the Central Bank of Jordan. This program is part of the bank's framework for information and technology governance and management.

5.5 The objectives and processes of information technology governance in appendices (2) and (3) and their data are considered a minimum requirement for the bank's top management to comply with and continuously achieve. The IT steering committee is primarily responsible for ensuring compliance with its requirements, while the IT governance committee and the board of directors are ultimately responsible. All bank departments, particularly the IT department, information security management, and project management, must identify and rephrase their processes to align and cover all requirements of information technology governance operations stipulated in appendix (3).

5.6 Committees

- **IT Governance Committee:**
  In accordance with the instructions of the Central Bank of Jordan, the Board of Directors has formed a committee consisting of board members to oversee IT governance. This committee is composed of at least three members, including individuals with expertise and knowledge in information technology.

- The committee may seek the assistance, at the bank's expense, of external experts when necessary. This is done in coordination with the chairman of the board to compensate for any deficiencies in this area and to enhance an objective opinion. The committee may invite any bank administrators to attend its meetings for their opinions, including those involved in internal auditing, senior executive management

members such as the Executive Director of IT and Project Management, or those involved in external auditing. The board defines the committee's objectives and delegates authority to it through a charter that outlines its responsibilities. The committee is required to submit regular reports to the board. It should be noted that delegating authority to the committee or any other committee does not exempt the board from its overall responsibilities in this regard.

- This committee meets at least quarterly, and records and minutes of the meetings are kept and documented according to proper procedures. The committee is responsible for the following tasks:
  - Approving the strategic objectives of information technology and the appropriate organizational structures, including the executive management-level steering committees, particularly the IT Steering Committee. This ensures the achievement of the bank's strategic objectives and the realization of the best added value from IT projects and investments, as well as the use of necessary tools and standards for monitoring and ensuring the achievement of these objectives. Examples of these tools include using IT Balanced Scorecards to calculate the Return on Investment (ROI) and measuring the impact of contributions in increasing financial and operational efficiency.
  - Adopting the general framework for managing, controlling, and monitoring IT resources and projects that follow the best international practices accepted in this regard, specifically COBIT. This will help achieve the goals and requirements of governance and IT management instructions, through sustainable achievement of institutional objectives mentioned in the instructions, and ensuring achievement of the information and technology matrix associated with it, covering IT governance operations.
  - Adopting the institutional objectives matrix mentioned in Appendix (1) of the Governance and Information Technology Management instructions and its updates mentioned in Central Bank Circular 10-6-984, and information and technology objectives mentioned in Appendix (2) and its updates mentioned in the same circular, and considering them as minimum data. Sub-objectives necessary to achieve these goals should be described.
  - Adopting a RACI Chart towards the main IT governance processes in Appendix (3) and its update mentioned in Central Bank Circular 10-6-984 and the sub-processes arising from them, in terms of the entity/entities/person/parties primarily responsible (Responsible), those ultimately responsible (Accountable), those Advisory (Consulted), and those to be Informed (Informed) regarding all processes in the mentioned appendix, guided by COBIT 2019 standard in this regard.
  - Adopting the importance of prioritizing enterprise goals and their relationship to alignment goals and governance and governance and management objectives, in addition to their connection to other enablers or components.

This is based on a qualitative and/or quantitative study conducted annually, taking into consideration the factors that shape the IT governance framework (COBIT 2019 - Design Factors). This study should be aligned with the bank's privacy and overall strategies, as well as the IT management strategy developed by the IT management and the strategy department. Cybersecurity, risk management, data privacy and protection, compliance, monitoring and audit, and strategic alignment should be included as focus areas of high importance and priority.

The maturity level of activities related to governance and management objectives and other seven enablers should be directly proportional to their importance and priority based on the above-mentioned study results. The maturity level of objectives with high importance and priority should be at least "Fully Achieved 3" on the maturity scale defined in the COBIT 2019 framework. Additionally, no more than 26% of the management objectives (up to a maximum of 9 out of 35 objectives) should be considered of lower importance and priority based on the study results.

- Ensure the existence of a general framework for IT risk management that aligns with the overall risk management framework of the bank and meets all the IT governance processes mentioned in Appendix (3).
- Adopt a budget for IT resources and projects that aligns with the bank's strategic objectives.
- Supervise and monitor the work processes and resources of IT to ensure their efficiency and effective contribution to the bank's requirements and operations.
- Review IT audit reports and take necessary actions to address any deviations.
- Recommend to the board the necessary actions to correct any deviations.
- Adopt a cybersecurity policy.
- Adopt a cybersecurity program.
- Review compliance with the cybersecurity policy and program.
- Review the committee charter every 3 years or as needed and make any necessary amendments for approval by the board of directors.
- Study any matter presented to the committee by the board of directors or any matter deemed necessary by the committee to discuss, provide opinions, and make recommendations to the board of directors.
- **The IT Steering Committee:**
  - The executive management has formed this committee to ensure the strategic alignment between the objectives of IT and the strategic objectives of the bank, in a sustainable manner, through the implementation of the IT management strategy formulated in collaboration between the IT department and the strategy department. Therefore, a committee called the IT Steering Committee was formed, chaired by the CEO and including members of the executive management, including the Executive Director of IT, the Project Management Director, the Executive Director of Risk Management, the Information Security and Financial Crimes Control Department Director. The board appoints one of its members to be an observer in this committee, in addition to the Executive Director of Internal Audit. The committee has the authority to invite external parties to attend its meetings as needed.

- This committee meets at least quarterly and keeps records and minutes of meetings in accordance with standard documentation practices. It has been ensured that the following matters are included within the committee's scope of responsibilities:
  - Developing annual plans related to information and technology and ensuring they align with the strategic goals approved by the board.
  - Supervising the implementation of annual plans to ensure their achievement, monitoring internal and external factors that may impact them continuously.
  - Aligning the bank's objectives with the accompanying information and technology objectives, continuously reviewing and approving them, including achieving the bank's strategic objectives.
  - Defining a set of Key Performance Indicators (KPIs), reviewing them, and assigning relevant executive management to monitor them continuously and report to the committee.
  - Recommending the allocation of necessary financial and non-financial resources to achieve the objectives and establish IT governance processes.
  - Recruiting competent and suitable human resources through organizational structures that include all necessary processes to support the goals while ensuring task separation and avoiding conflicts of interest.
  - Overseeing the implementation of projects and IT governance processes.
  - Prioritizing IT projects and programs according to importance.
  - Monitoring the level of technical and technological services and continuously working on improving their efficiency.
  - Providing necessary recommendations to the IT governance committee regarding the following matters:
    - Allocating resources and mechanisms necessary to fulfill the IT governance committee's tasks.
    - Any deviations that may negatively affect the achievement of strategic goals.
    - Unacceptable risks related to technology and information security.
    - Performance and compliance reports with the general framework for managing and controlling IT resources and projects.
  - Keeping the IT governance committee informed by providing meeting minutes in a timely manner.
  - Approving and implementing recommendations to the IT governance committee regarding the importance and prioritization of enterprise goals and their alignment with alignment goals, governance objectives, and management objectives, as well as their connection to other enablers/components.

This is based on a qualitative and/or quantitative study conducted annually, taking into consideration the factors that shape the IT governance framework (COBIT 2019 - Design Factors). This study should be aligned with the bank's privacy and overall strategies, as well as the IT management strategy developed by the IT management and the strategy department. Cybersecurity, risk management, data

privacy and protection, compliance, monitoring and audit, and strategic alignment should be included as focus areas of high importance and priority.

The maturity level of activities related to governance and management objectives and other seven enablers should be directly proportional to their importance and priority based on the above-mentioned study results. The maturity level of objectives with high importance and priority should be at least "Fully Achieved 3" on the maturity scale defined in the COBIT 2019 framework. Additionally, no more than 26% of the management objectives (up to a maximum of 9 out of 35 objectives) should be considered of lower importance and priority based on the study results.

5.7 Policy System:

- The board or its authorized committees are responsible for approving the principles, policies, and necessary frameworks for achieving the overall framework for managing, controlling, and monitoring information technology resources and projects in line with the requirements of IT governance objectives and processes.
- The board or its authorized committees are responsible for approving the principles, policies, and frameworks, especially those related to IT risk management, information security management, and human resource management that meet the requirements of IT governance processes outlined in Appendix (A).
- The board or its authorized committees are responsible for approving the policy system necessary for managing information technology resources and processes outlined in Appendix (A), considering it as a minimum threshold with the possibility of integrating these policies as required by the nature of the work. Other policies should be developed to align with the bank's objectives and work mechanisms.
- When developing policies, the contribution of all internal and external stakeholders should be considered, and international best practices and updates should be adopted as references in formulating these policies, such as COBIT 2019, ISO/IEC 27001/2, ISO 31000, ISO 22301, PCI, ISO/IEC 15504, ISO/IEC 9126, ISO/IEC 38500, DXX, ITIL, etc.

5.8 Information, Data, and Reports:

- The board of directors and senior management are responsible for ensuring the development of the necessary infrastructure and systems to provide information and reports to users with the aim of contributing to sound decision-making in the bank.
- The board of directors or authorized entities adopt the information and reporting systems outlined in Appendix (B), which serve as the minimum requirements. The owners of this information and the reports determine the authority for review, usage, and delegation as needed for operations.
- Policies and reports are regularly reviewed and updated to align with the bank's objectives and operations based on best practices and standards.

5.9 Organizational Structure:

- The board is responsible for approving the organizational structures (hierarchical and committees), specifically those related to the management of IT resources and operations, IT risk management, information security management, and human resource management that meet the requirements of IT governance processes and achieve the bank's objectives efficiently and effectively.
- The separation of conflicting tasks and the regulatory protection requirements related to dual control should be considered as a minimum. Additionally, job descriptions should be reviewed and updated when approving and modifying the bank's organizational structures.

5.10 Services, Infrastructure, and Applications:

- The board, or those delegated by its committees and the executive management, should approve the system of services, programs, and infrastructure mentioned in Appendix (C) for information technology that supports the achievement of IT governance processes and, therefore, the objectives of information and accompanying technology and corporate objectives.
- The board, or those delegated by its committees and the executive management, should approve the system of services, programs, and infrastructure for information technology, considering it as a minimum requirement. The provision and continuous development of this system should be ensured to keep up with the evolving objectives and operations of the bank, in line with best international practices accepted in this regard.

5.11 Knowledge, Skills, and Experiences:

- The board, or those delegated by its committees, should approve the qualification matrix and human resource management policies necessary to achieve the requirements of IT governance processes and ensure the right person is in the right place.
- The bank's management should employ qualified and trained individuals with experience in the fields of IT resource management, risk management, and IT audit management. This should be based on academic and professional knowledge standards and practical experience recognized by qualified international associations according to international accreditation standards for certification-granting institutions, each according to their specialization. The current workforce should undergo re-qualification and training to meet the requirements of this guideline.
- The bank's executive management should continue to provide its employees with training and continuing education programs to maintain a level of knowledge and skills that meet and achieve IT governance processes.
- The bank's executive management should include mechanisms to evaluate employees based on objective standards, taking into account their contribution through the functional center in achieving the bank's objectives.

5.12 Culture, Ethics, and Behavior:

- The bank's board of directors or its authorized committees should adopt a code of conduct that reflects the professional behavior related to information and technology management. This code should clearly define the applicable rules and ethics.
- The internal and external auditors should comply with the ethics and professional practices system approved by the board, which includes, at a minimum, the professional ethics system outlined in the ISACA ITAF: Information Technology Assurance Framework and its updates.
- The board and executive management should employ different mechanisms to promote the desired behaviors and avoid undesirable behaviors. This can be achieved through methods such as using incentives and sanctions, among others.

5.13 Internal and External Audit:

- The board is responsible for monitoring sufficient budgets and allocating necessary resources, including qualified human resources, through specialized audit departments in the field of information technology. They also need to ensure that both the internal audit department of the bank and the external auditor are capable of reviewing and auditing the bank's recruitment processes, resource management, and information technology projects and operations. This should be done by employing professional and internationally certified personnel in this field, who hold valid professional accreditation certificates such as CISA.
- The audit committee, which is formed by the board, along with the external auditor, must provide the Central Bank of Jordan with an annual report for internal audit and another for external audit. These reports should include the executive management's response, the board's observations and recommendations regarding the audits. These reports should be submitted during the first quarter of each year.
- The audit committee should outline the responsibilities, authorities, and scope of work for auditing information technology within the audit charter, as well as through agreed-upon procedures with the external auditor.
- The board, through the audit committee, must ensure that both the internal auditor and the external auditor of the bank, when conducting specialized audits related to information technology, commit to the following:
  - Adhering to information technology audit standards according to the latest update of the international ITAF standard issued by the ISACA Audit and Control Association. These standards include:
    a) Executing audit tasks within an approved plan that takes into account the relative importance of processes, risk levels, and the impact on the bank's objectives and interests.
    b) Providing and complying with continuous training and education plans for the specialized staff in this regard.

c) Complying with professional independence standards and ensuring no conflict of interests.
d) Adhering to objectivity standards, exercising care, and continuously maintaining competitiveness and professionalism.

- Examining, evaluating, and reviewing recruitment and management processes related to information technology and the bank's operations relying on it, and providing a general opinion on the overall risk level of the information and the accompanying technology within the auditing program.
- Implementing regular procedures to monitor the results of the audit in order to ensure the resolution of observations and imbalances mentioned in the auditor's reports within the specified timelines. The importance and risks should be escalated gradually in case of non-compliance, and the board should be informed accordingly whenever necessary.
- It is possible to assign the role of the internal auditor for information and accompanying technology to an entirely independent external specialized entity, different from the external auditor appointed in this regard, provided that all the requirements of these instructions and any other relevant instructions are met, and the audit committee formed by the board and the board itself retain their functions in terms of compliance review and ensuring that these requirements are met at a minimum level.

6. Goal Setting and Monitoring

Each institution operates in a different context, which is determined by both external and internal factors. External factors include the market, industry, geographical policies, etc., while internal factors include culture, organization, risk tolerance, etc. This institutional context requires a governance and management system that is aligned with it.

The needs of stakeholders should be translated into an executable institutional strategy that forms integrated goals. These goals serve as a mechanism to translate stakeholder needs into meaningful and achievable institutional objectives that are allocated and derived from them. This translation allows for the establishment of specific goals at each level and in each area of the institution to support overall objectives and stakeholder requirements, thus aligning the needs of the bank with effective IT solutions and services.

The bank has adopted a cascading goals mechanism to translate stakeholder needs into specific and actionable goals, dedicated to activities and objectives related to alignment and enabling. This translation enables the establishment of specific goals at each level and in each area of the bank to support overall goals and stakeholder requirements, effectively supporting the alignment between the bank's needs and IT solutions and services.

Appendix A: Policy System (Minimum Requirements)

* *The table below is based on the Central Bank of Jordan's Appendix No. (6) instructions.*

The bank adopts the following list of minimum policies to regulate and manage operations within the bank.

Policy	Purpose	Scope
IT Governance	Establishing the necessary regulations and standards for managing IT resources, including the administrative structure (centralized or decentralized) and organizational frameworks, including activities, tasks, and responsibilities for managing those resources, including financial resources.	IT operations, services, and projects
Information Security and Protection	Developing the necessary regulations and standards to ensure the requirements of protection, confidentiality, integrity, availability, and compliance in managing IT resources, according to internationally accepted standards such as ISO-IEC 27001/2.	All associated information and technology
Business Continuity and Disaster Recovery Plans	Establishing the necessary regulations and standards for building disaster recovery plans and protecting humans, as well as business continuity plans, including mechanisms for building, operating, testing, training, and updating those plans to ensure the availability of critical bank operations.	Critical bank operations and human protection
IT Risk Management	Developing the necessary regulations and standards for managing IT risks as part of the overall bank's risks, including governance of those risks, responsibilities, and tasks associated with different parties, as well as mechanisms for assessing, controlling, and monitoring risks, with the aim of enhancing risk-based decision-making processes and achieving the bank's objectives.	All bank operations and their IT inputs
IT Compliance	Establishing the necessary regulations and standards to ensure compliance with the bank's policies, the instructions of the Central Bank, other regulatory bodies, as well as current laws and regulations.	All bank operations related to information technology
Data Privacy	Establishing the necessary regulations and standards to protect data of persons and individuals from unauthorized disclosure and use.	All private data

Policy	Purpose	Scope
Outsourcing	Adopting a general policy for resource utilization, including information technology resources, whether owned by the bank or outsourced to third-party providers, while adhering to applicable instructions, regulations, and laws, and following international best practices. The policy should consider the location of the production process and comply with monitoring requirements and the use of reliable third-party services to ensure service levels and audit rights.	All bank operations
Project Portfolio Management	Developing regulations and standards for project management, including project phases and necessary governance to achieve quality requirements, protection, confidentiality, and compliance with the bank's objectives and operations.	All bank projects related to information technology
Asset Management	Establishing regulations and standards to classify the risk level of data and different systems and determining ownership and protection controls throughout their various life cycles.	Associated data, devices, software, and tools
Acceptable Use of IT Resources	Establishing the necessary regulations and standards to determine acceptable and unacceptable behavior for information technology resources.	Devices, software, applications, and networks, including the internet and email
Change Management	Establishing regulations and standards to ensure the credibility of changes, including documenting the necessary approvals from the change-mandating assets.	All information technology operations
Mainframe Computers	Developing regulations and standards to reduce unauthorized access and use of devices, including access controls for IT department employees and privileged users in operating environments, as well as standards for managing daily operations of different devices and software, including protection controls, monitoring mechanisms, and regular maintenance.	All central devices owned or managed by the bank for all development, testing, and operations data, including operating systems and other associated tools
Terminal Computers	Establishing regulations and standards for behavior and technical measures to ensure the protection of sensitive data stored on devices.	All terminal devices connected to networks or operating independently
Mobile Devices	Establishing regulations and standards for behavior and technical measures to ensure the protection of sensitive data stored on devices.	All portable devices such as laptops, PDAs, smartphones, USB memory cards, etc.

Policy	Purpose	Scope
User Access Management	Establishing regulations and standards to ensure the granting of access privileges for data, software, and devices to users based on their work needs, while guaranteeing confidentiality, integrity, and availability of information technology resources.	All software, devices, and data processing equipment and similar items
System Development Life Cycle	Developing the necessary regulations and standards to implement different software development life cycle stages, ensuring that they meet the business requirements through suitable development methodologies aligned with the business objectives.	Both new and old software, advanced locally, and acquired from external sources
Service Level Management	Establishing regulations and standards to define, accept, document, measure, monitor, and improve the level of services provided, whether by internal or external parties, to ensure optimal utilization of resources and support various banking operations.	All contracts, agreements, and commitments with external parties and parties within the bank
Backup and Restoration	Developing regulations and standards for backup and recovery mechanisms to ensure the availability, integrity, and confidentiality of data.	Data in operating environments and wherever necessary
Data Retention	Establishing regulations and standards for the required data size, whether in physical or digital form, and the retention period for online data, considering the trade-off between data size, speed, and performance in accessing the data.	All devices, software, and tools for data retention
System and Equipment Purchasing	Developing regulations and standards for evaluating and selecting external providers.	All related technical equipment and software
Remote Access	Establishing regulations and standards for remote network connectivity to the bank's computer networks, aiming to minimize the risk of unauthorized access and usage of sensitive data and bank assets, as well as protection of internal control and monitoring systems, to mitigate reputation risks.	Internal and external parties, such as service providers, for all development, testing, and operation data for devices and networks, including, but not limited to, internet networks, encrypted networks, and various communication lines such as VPN, ISDN, Frame Relay, MPLS, DSL, etc.
Networks	Developing regulations and standards to ensure the efficiency and effectiveness of network and communication elements, while meeting security and protection requirements, in support of the bank's objectives.	All network components with all their data
Wireless Networks	Establishing regulations and standards for protecting sensitive data transmitted over wireless networks from interception and unauthorized use.	Actual and virtual wireless networks

Policy	Purpose	Scope
Firewalls	Establishing minimum regulations and standards for activating and configuring firewalls to ensure the proper functioning and protection of devices, safeguarding the confidentiality and integrity of the bank's data and operations.	All firewall devices working with all data such as DMZ, Proxy, External, DNS, VPN, Routers, Switches, Servers, etc.
Penetration Testing and Vulnerability Assessment	Developing regulations and standards for regularly scanning devices and network elements to identify and address any security vulnerabilities that could potentially be exploited to gain unauthorized access to the bank's data, systems, and sensitive operations.	All technical assets of the bank, including central computers, peripheral devices, security devices, network elements, and software
Public Branch Exchange	Defining the minimum regulations and standards for the protection of partitioned systems to ensure protection, confidentiality, and integrity of the bank's data and operations from unauthorized use or access.	Owned and non-owned partition devices of the bank

Appendix (B): Minimum Reports and Information

* ***The following table is based on the instructions of the Central Bank of Jordan's Appendix No. 7.***

The bank will adopt the minimum list of reports below to ensure the integrity of reports within the bank, as reports serve as an anchor for decision-making processes.

1. Authorization and Privileges Matrix
2. Risk Factors Analysis
3. Information Technology Risk Scenarios Analysis
4. Information Technology Risk Register
5. RACI Chart (Responsibility Assignment Matrix) for each service provided
6. Information Technology Risk File
7. Information Technology Risk Report
8. Information Technology Risk Map
9. Risk Universe, Appetite, and Tolerance
10. Key Risk Indicators
11. Risk Taxonomy
12. Risk and Control Activity Matrix (RCAM)
13. Information Security and Protection Budget
14. MIS (Management Information Systems) Report
15. Information Technology Audit Strategy or Methodology
16. Audit Charter
17. Information Technology Audit Plan

18. Qualification Matrix
19. Information Technology Audit Register
20. Information Technology Audit File
21. Best International Standards for IT Resource and Project Management, IT Risk Management, IT Security and Protection, and IT Audit.

Appendix (C): Information Technology Services, Programs, and Infrastructure

The bank will adopt a list of information technology systems, services, and infrastructure that support the following information to achieve governance and management of information and associated technology.

1. Incident Management Services.
2. Information Technology Asset Inventory.
3. Awareness of Good Information Security Practices.
4. Logical Data and Information Security and Protection.
5. Information Security Monitoring.
6. Information Technology Audit Software.
7. Physical and Environmental Security Monitoring for Data Centers, Communication Rooms, and Power Supplies.

Definitions

- Governance: Ensures evaluating the needs, conditions, and options of stakeholders to define balanced and agreed-upon goals at the enterprise level that are achieved; and monitoring performance and compliance towards the agreed-upon goals.
- COBIT: Formerly known as Control Objectives for Information and Related Technology (COBIT); now used only as a name.
- COBIT framework: A globally accepted and comprehensive framework for enterprise information and technology governance and management that supports executive management in defining and achieving business goals and related compliance objectives. COBIT supports enterprises in developing, implementing, improving, and monitoring good governance and management practices related to information technology.
- Enterprise goal: The business objective.
- Information and technology governance in the enterprise: A vision of governance that ensures information and related technology support and contributes to achieving enterprise goals.
- Board of Directors: The bank's board of directors.
- Senior executive management: Includes the bank's CEO or regional manager, deputy CEO or deputy regional manager, assistant CEO or assistant regional manager, CFO, operations manager, risk manager, treasurer (investment), compliance manager, as well as any bank employee with executive authority parallel to any of the aforementioned authorities and is functionally and directly linked to the general manager.
- Stakeholders: Any interested party in the bank, such as shareholders, employees, creditors, customers, suppliers, or relevant external regulatory bodies.
- Auditor: The individual (natural or legal) or entity responsible for examining the bank's IT-based operations and meeting the requirements and agreements specified by the bank's management to achieve those requirements for a period not less than 3 consecutive years and not more than 6 consecutive years.