Governance and Management of Information and Related Technologies Guide

Table of Contents

Introduction

The information technology resources are considered a key cornerstone in terms of relative volume and impact on the bank's ability to facilitate its operation and, consequently, achieve its objectives. In addition, they play a sensitive role in impacting the competitiveness of the bank's products and services, from one side, and on the mechanisms of decision-making and risk management, from the other. This justifies the large investments in the information technology sector by the banking institutions.

The entrepreneurship institutions in all sectors and businesses have faced significant challenges requiring them to essentially use the modern and advanced technologies. This has become an important issue and standard for the development of such organizations and an impetus to deal with them and for competitiveness in their working fields. This required such organizations to invest in information technologies and their systems.

On the other hand, these huge investments and contemporary technologies faced many risks, threats and challenges as the new environment caused changes that did not exist before in view of the use of traditional methods which depend on manual systems. New forms of risks emerged with the use of technology and electronics which marked this era and organizations started to compete among themselves on using them . Therefore, our Bank had to follow the proper standards and acceptable international practices in the management of information technology resources to minimize their risks and avoid unfeasible investments or unjustified expenses.

IT Governance concept is the subject of significant attention at all the governmental and legislative levels and from the supervisory bodies and business institutions on equal terms due to the benefits and advantages revealed by the studies and researches at the macroeconomic level and at the level of economic units as a result of implementation of good governance standards and principles. The in-sight attempts to establish the corporate governance led to the emergence of a pressing need of one of the governance elements which is the IT governance that is considered the good implementation of the principles and rules of which is an introduction for the protection of information security and privacy in the economic establishments.

First: Guide Reference

This Guide is issued based on the requirements of the Governance and Management of Information and Related Technologies by the Central Bank of Jordan No. (65/2016) on 25/10/2016 and its related instructions applicable in this regard. COBIT 5 and COBIT 2019 international standards were adopted in the issuance of this Guide.

Second: Definitions

Unless otherwise required by the context, the following words and expressions shall have the meanings assigned thereto.

1	The Bank	Jordan Islamic Bank
2	The Central Bank	The Central Bank of Jordan
3	Guide	Governance and Management of Information and Related Technologies Guide
4	Governance of Information and Related Technologies	Distribution of roles and responsibilities and description of relation between different parties and entities and stakeholders (like the Board and the Executive Management) to maximize the added value for the establishment through the adoption of optimum approach which guarantees the balance between expected risks and revenues through the adoption of necessary rules, principles, and mechanisms for decision-making and identify the strategic approaches and objectives in the Bank and the mechanisms of audit and control of the compliance with their achievement to ensure the Bank's sustainability and development.
5	Information Management and Related Technologies	A set of ongoing activities that fall within the responsibility of executive management and includes the planning for achievement of the strategic objectives. This includes the compatibility, organization, building and development activities, procurement and implementation, operation activities, the supply of services and support, control activities including measurement and assessment and to ensure the sustainability of achievement of the Bank's objectives and strategic approaches.
6	Information Technology Governance Operations	A number of practices and activities emerging from the organization policies and which are necessary to achieve the objectives of the information and related technology.
7	Objectives of Information and Related Technology	A number of primary and secondary objectives related to the governance and management activities of information and related technology necessary for the achievement of the organization objectives.
8	Corporate Objectives	A number of objectives related to the corporate governance and management which are necessary for meeting the stakeholders' needs and the objectives of these instructions.
9	The Board	Board of Directors of Jordan Islamic Bank
10	Senior Executive Management	Includes the CEO / General Manager of the Bank, the Deputy General Manager, Assistant General Manager, Head of Finance, Head of External Operations, Head of Central (Local) Operations, Head of Risk Department, Head of Treasury, Head of Compliance Control and any employee of the Bank who has a power similar to any of the above and who is directly related to the CEO / General Manager.

11	The Auditor	The natural person carrying out audit under the supervision of the partner in charge of audit and does not include the additional service auditor beyond the scope of audit services.
12	The Stakeholders	Any stakeholder in the Bank including the shareholders or employees or any of the creditors, clients, suppliers or competent supervisory bodies.
13	On-site	The place of operations in the same building of the Bank's General Management in Jordan.
14	Off-site	The place of operations in a building other than the building of the Bank's General Management in Jordan but in the same Governorate.
15	Near-site	The place of operations in a Governorate other than the Governorate where the Bank's General Management is located in Jordan.
16	Off-shore	The place of operations in a country other than the country where the Bank's General Management is located

Third: Guide Applicability

The scope of applicability covers all the Bank's operations based on information technology in the different branches and departments.

Third: Compliance with the Governance and Management of Information and Related Technologies

1- A board committee shall be formed under the name “IT Governance Committee” and shall consist of at least three Board members. The assistance of external experts may be sought when necessary. The Committee shall approve the IT strategic objectives and the appropriate organizational structures and shall set the general framework, set and control the IT projects and resources, approve the objectives and responsibilities matrix, approve the project budgets and general supervision of the IT projects and resources progress and its achievement of the Bank requirements and businesses.
2- A committee shall be composed of the senior executive management under the name “IT Steering Committee” to be presided over by the General Manager with the membership of the senior executive management directors. The Committee shall set the annual plans, recommend the allocation of financial and non-financial resources to achieve the objectives and arrange for the IT projects and programs based on the priority and to supervise the technical and technological service level, raise its efficiency and improve it.
3- To include in the annual Board report, a report for the public referring to the Guide and showing the compliance with its clauses highlighting the reasons for noncompliance with any clause that has not been implemented.
4- The Bank provides an approved copy of the Guide on the Bank's website www.jordanislamicbank.com
5- This Guide is subject to review whenever necessary.

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

This Guide aims to achieve the following:

1- Meet the stakeholders’ needs and achieve the approaches and objectives of the Bank through the achievement of objectives of the information and related technology. This includes:

a- Provide high-quality information as a basis to support the Bank decision-making mechanisms;

b- Provide prudent management for IT resources and projects which maximizes the benefit of such resources and minimize their waste.

c- Provide excellent and supporting IT infrastructure which will enable the Bank to achieve its objectives.

d- Develop the Bank's different operations through the employment of efficient and reliable technological systems.

e- Provide prudent management for IT risks guaranteeing the necessary protection of Bank's assets.

f- Assist in the achievement of compliance with the requirements of laws, legislations and instructions in addition to compliance with the internal work strategy, policies, and procedures.

g- Maximize the satisfaction of users of Information Technology by meeting the work needs efficiently and effectively.

h- Manage the services of external parties to whom the implementation of processes, tasks, services, and products are assigned.

i- Achieve the inclusion in the Governance and Management of Information and Related Technologies considering not only the technology but also the components which help achieve such inclusion which integrates with each other to achieve such concept. These components are:

1- Operations

2- Organizational Structures

3- Principles, policies, and work procedures

4- Information

5- Code of Ethics and Conduct

6- Persons, Skills and Efficiencies

7- Services, programs and infrastructure of Information Technology which should be provided in certain specifications and dimensions to achieve and serve the requirements and objectives of information and related technology not only in the IT operations but also in all the Bank's operations based on information and technology.

2- Provide dynamic and appropriate governance systems to be continuously updated depending on the changes like the change of strategic or technological approaches.

3- Separate the Board duties and responsibilities in the field of governance from those falling within the executive management limits of responsibility regarding information and related technology.
4- Provide appropriate and suitable governance system for our Bank through the reliance on certain design standards through which the governance system components and its priorities are set.
5- Cover all the Bank's operations and focus not only on the role of IT but on all the operations and procedures related to information and related technology wherever they are located in our Bank.

Fifth: Committees

1- IT Governance Committee

The Board shall form the IT Governance Committee of its members. This Committee shall be composed of at least three members and shall preferably have persons with experience and strategic knowledge in IT as members. The Committee shall meet at least quarterly and keep documented minutes of its meeting. It shall be in charge at least of the following:

a- Approval of the IT strategic objectives and appropriate organizational structures including the steering committees at the level of senior executive management particularly the IT Steering Committee to ensure the achievement of the Bank strategic objectives, the best-added value from the projects and investments of the IT resources and use of necessary tools and standards to control and ensure the achievement thereof. This includes the use of IT Balanced Scorecards, calculation of the return on investment and measurement of the contribution impact on the increase of financial and operational efficiency.
b- Approval of the priority and order of objectives of governance and management of information and related technology No. (65/2016), the objectives of the information and related technology stated in Annex (2) to the instructions of governance and management of information and related technology No. (65/2016), in addition to their relevance to other empowerment elements/components of governance system based on the qualitative/quantitative study conducted for this purpose at least annually considering the design factors stated in COBIT 2019 Design Guide.
c- Approval of the general framework for the management, control, and supervision of the IT resources and projects simulating the international best practices in this regard particularly the Control Objectives for Information and related Technology (COBIT) which conforms to and meets the objectives and requirements of the instructions through the achievement of the organizational objectives matrix stated in Annex (1) to the instructions of governance and management of information and related technology No. (65/2016) in a sustainable manner and achieve the matrix of objectives of the information and related technology stated in Annex (2) to the instructions of governance and management of information and related technology No. (65/2016) and covering the objectives of governance and management stated in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).

d- Approval of the matrix of organizational objectives stated in Annex (1) to the instructions of governance and management of information and related technology No. (65/2016), and achieve the matrix of objectives of the information and related technology stated in Annex (2) to the instructions of governance and management of information and related technology No. (65/2016) considering its outputs as a minimum and description of the secondary objectives necessary for their achievement.

e- Approval of the RACI chart for key processes of the information technology governance in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016) and the sub-processes resulting from them in terms of responsible, accountable, consulted and informed entity(ies) and person(s) towards all the processes stated in the above-mentioned annex in view of the COBIT 5 Enabling Processes in this regard.

f- To ensure the existence of a general framework of IT governance conforming to and integrating with the overall framework of the Bank risk management considering and meeting the objectives of governance and management in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).

g- Approval of the balance sheet of IT resources and projects in line with the Bank's strategic objectives.

h- Overall supervision and review of the IT processes, resources and projects progress to ensure their adequacy and effective contribution to the achievement of the Bank requirements and businesses.

i- Review the IT audit reports and take necessary actions to correct any deviations.

j- Provide recommendation to the Board to take necessary actions to correct any deviations.

2- IT Steering Committee

The senior executive committee shall form the necessary steering committee to ensure the IT strategic conformity for the sustainable achievement of the Bank's strategic objectives. Therefore, a committee entitled “IT Steering Committee” was formed and presided over by the General Manager and the membership of the senior executive management directors including IT Manager, Head of Risk Management Department and Head of IT Security Department. The Board shall elect one of its members to act as the controlling member in the Committee in addition to the Internal Audit Manager. The Committee may invite others to attend its meetings when necessary and its meeting shall be documented in duly issued minutes. The meetings shall be held at least quarterly and shall be in charge of the following in particular:

1- Setting the annual plans aimed to achieve the strategic objectives set by the Board, supervision of their implementation to ensure their achievement and continuous control of the internal and external factors affecting them.

2- Linking the organizational objectives matrix with the objectives of the information and related technology stated in Annex (1) to the instructions of governance and management of information and related technology No. (65/2016), their continuous approval and review to ensure the achievement of the Bank strategic objectives and instructions objectives considering the definition and review of the set of measurement standards and assigning their control to the persons in charge in the executive management and keep the Committee updated.

3- Recommendation of the allocation of necessary financial and non-financial resources to achieve the matrix of objectives of the information and related technology stated in Annexes (2) and (3) consecutively to the instructions of governance and management of information and related technology No. (65/2016) as a minimum. Engagement efficient and right human resources in the right place through organizational structures covering all the processes necessary for the support of objectives considering the separation of duties, avoidance of conflict of interests, adaptation of the IT infrastructure and related services to serve the objectives and assuming the processes of supervision of the implementation of IT governance projects and processes.
4- Arrangement of the IT projects and programs based on priority
5- Control and continuous improvement of the level of technical and technological services
6- Raising necessary recommendations to the Board IT Governance Committee regarding the following:
a- Allocation of necessary resources and mechanisms to achieve the duties of the IT Governance Committee
b- Any deviations that may adversely affect the achievement of the strategic objectives
c- Any unacceptable risks related to information technology, security, and protection
d- Performance reports and compliance with the requirements of the general framework for the management, adjustment, and control of IT resources and projects.
7- Providing the IT Governance Committee with meeting minutes and getting proof of access thereto.

Sixth: Matrix of Objectives of the Information and Related Technologies and objectives of Governance and Management

1- The governance and management objectives and the matrix of objectives of the information and related technology stated in Annexes (2) and (3) consecutively to the instructions of governance and management of information and related technology No. (65/2016) and their inputs are a minimum that the Bank senior management should comply with and continuously achieve in line with the results of governance system design based on the design factors. The IT Steering Committee is primarily responsible for the compliance with the achievement of its requirements while the IT Governance Committee and the overall Board are finally responsible in this regard. All the Bank departments, particularly IT, Information Security Department and IT Projects Department should set and redraft their processes to simulate and cover all the requirements of the objectives of governance and management in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).
2- The Board shall be directly responsible for the governance and management objectives related to EDM (Evaluate,, Direct and Monitor) stated in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).

3- The Board and the Risk Management Department shall be directly responsible for the prudent management of IT risks (EDM 03) and risk management objective (APO 12) stated in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).

Seventh: Internal and External Audit

1- The Board shall allocate the adequate budgets and the necessary tools and resources including human resources through the divisions specialized in IT audit and shall ensure that the Bank Internal Audit Department and the external auditor are both able to review and audit the process of employment and management of the IT resources and projects and the Bank related processes as a specialized and technical audit (IT Audit) through internationally qualified and certified professional resources in this field who hold valid professional certificates like (CISA) from international associations qualified under ISO / IEC 17024 and / or any other equivalent standards.

2- During the first quarter of every year, the Board Audit Committee and the external auditor should provide the Central Bank of Jordan with an annual internal audit report and another external audit report consecutively including the executive management reply and the Board recommendations in this regard as stated in the instructions of governance and management of information and related technology No. (65/2016) issued by the Central Bank of Jordan.

3- The Audit Committee should include the IT powers, responsibilities and scope of work within the Audit Charter and within the processes agreed with the external auditor in line with these instructions.

4- Through its Audit Committee, the Board should ensure that the Bank internal auditor and external auditor, when carrying out the audit operations of information and related technology, comply with the following:

a- Information Technology audit standards according to the last update of the Information Technology Assurance Framework (ITAF) issued by the Information Systems Audit and Control Association (ISACA) including:

1) Implementation of the audit tasks within an approved plan in this regard which considers the relative importance of processes, risk level and the level of impact on the Bank objectives and interests.

2) Providing and compliance with continuous education and training plans by specialized resources.

3) Providing professional and organizational independence and avoiding conflict of current and future interests.

4) Compliance with objectivity standards, acting with due professional care and deep knowledge of the Bank different mechanisms and processes based on the information technology and other audit and review reports (financial, operational and legal), ability to provide evidence commensurate to the case and the public sense in identification of unacceptable practices violating the laws, regulations and instructions.

b- Audit, assessment and review the process of employment and management of the IT resources and the Bank related processes and giving general opinion (Reasonable Overall Audit Assurance) regarding the overall risk level of information and related technology within a special audit program which covers, at least, the elements indicated in annex (5) to the instructions of governance and management of information and related technology No. (65/2016). The frequency of audit of all or part of the elements shall be conducted at least once per year in case of risk assessment degree of 4 or 5 according to the approved risk assessment scale indicated in Annex (4) to the instructions of governance and management of information and related technology No. (65/2016), once every two years at least in case of risk assessment degree of 3 and once every three years at least in case of risk assessment degree of 1 or 2, considering the continuous change of the risk level and the significant changes to the environment of information and related technology during the said audit periods. The Central Bank shall be provided with the audit reports in the first time regardless of the risk assessment degree and the element assessment processes should include the Bank mechanisms in terms of strategic planning, setting approved and written the policies, principles and work procedures, the mechanisms of employment of different resources including the information technology and human resources as well as the monitoring, improvement and development mechanisms and documentation and assessment of the audit results based on the importance of faults and weaknesses in addition to the active controls, and assessment of residual risk level using a methodological standard for the analysis and measurement of risks including the agreed corrective measures to be followed in certain dated of correction with reference to a table with the titles of the responsible officer in the Bank who is the remark owner.

c- Regular procedures for the follow-up of the audit results to ensure the treatment of remarks and faults in the audit report within the set times and gradually raise the level of priority and risks in case of no response and keep the Board informed when necessary.

d- Inclusion of the annual performance evaluation mechanisms for the IT audit resources using objective criteria. Such evaluation processes shall be carried out by the Board represented by the Audit Committee and according to the organizational hierarchy of the Internal Audit Department.

5- It is possible to outsource the role of Internal Audit IT to a specialized third party totally independent from the external audit accredited in this regard. The Board Audit Committee and the Board itself shall keep their roles with regard to the audit of compliance with this Guide as a minimum

Eighth: Principles, Policies, and Frameworks

1- The Board shall authorize the IT Governance Committee to approve the Principles, Policies and Frameworks matrix needed to achieve the general framework of management and control of IT projects and resources that meet the requirements of the Matrix of information and its related technology and the governance and administration Objectives stated in

Annex (2) and (3) consecutively to the instructions of governance and management of information and related technology No. (65/2016).

2- The Board shall authorize the IT Governance Committee to approve the Principles, Policies, and Frameworks particularly those related to the IT risk management, information security management and human resources management which meet the requirements of the matrix of objectives of information and related technology stated in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016).

3- The Board shall authorize the IT Governance Committee to approve the matrix of policies required for the management of resources and objectives of governance and related stated in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016). Such a matrix of policies shall be considered as minimum with the possibility of combination and merger of such policies. Other policies may be developed to cope with the development of the Bank objectives and work mechanisms. Each policy shall set the owner, applicability, frequency of review, access powers, distribution, objectives, responsibilities and work procedures, penalties in case of non-compliance and mechanisms of an audit of compliance.

4- When setting the policies, all the internal and external stakeholders should contribute and the international best practices and their updates shall be approved as references for drafting such policies including (COBIT5, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL, …etc.).

Ninth: Organizational Structures

1- The Board should approve the organizational structures (hierarchies and committees) particularly those related to IT projects and resources and processes management, IT risks management, information security management and human resources management to meet all the requirements of the objectives of governance and management in Annex (3) to the instructions of governance and management of information and related technology No. (65/2016) and achieve the Bank objectives efficiently and effectively.

2- When approving and modifying the Bank organizational structures, the conflicting duties should be separated, the organizational protection requirements related to the dual control as a minimum and job description adequacy and update should be considered.

Tenth: Information

1- The Board and the senior executive management should develop the infrastructure and the necessary IT systems to provide information and reports to its employees as a basis for the decision-making process in the Bank. Moreover, the information quality criteria should be provided including Integrity (Completeness, Accuracy, and Validity or Currency) as well as the confidentiality requirements depending on the policy of data classification, the requirements of availability and compliance with such information and reports and other requirements of COBIT 5 – Enabling Information including Objectivity, Believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, Understandability, Ease of Manipulation, Restricted Access.

2- The Board shall authorize the IT Governance Committee to approve the matrix of information and reports stated in Annex (7) to the instructions of governance and management of information and related technology No. (65/2016), and consider such requirements as a minimum. It shall set the owners of such information and reports through which the powers of access and use shall be set and authorized. Such a matrix shall be continuously reviewed and developed to cope with the development of the Bank objectives and processes according to the international best practices in this regard.

Eleventh: Services, programs, and infrastructure of Information Technology

1- The Board should:

a- Authorize the IT Governance Committee and the senior executive management to approve the matrix of IT infrastructure, services, and programs supporting and helping the achievement of the IT governance processes and, consequently, the objectives of the information and related technology and, hence, the institutional goals. .

b- Authorize the IT Governance Committee and the senior executive management to approve the matrix of IT infrastructure, services, and programs stated in Annex (8) of the instructions of governance and management of information and related technology No. (65/2016), such matrix shall be considered as minimum and shall be continuously provided and developed to cope with the development of the Bank's objectives and operations according to the international best practices in this regard.

Twelfth: Persons, Skills, and Efficiencies

1- The Board shall authorize the IT Governance Committee to approve the matrix of HR Competencies and the necessary human resources management policies to achieve the requirements of the objectives of governance and management stated in Annex (3) of the instructions of governance and management of information and related technology No. (65/2016) and the requirements of these instructions in general and ensure the employment of the right person in the right place.

2- The Bank should employ qualified and trained human resources from those who are experts in the fields of IT resources management, Risk Management Department, IT Security Department, and IT Technology Audit Department based on the criteria of academic and professional knowledge and practical experience with the recognition of qualified international associations under ISO/IEC 17024 and / or any other equivalent standards each in his respective field of specialization.

3- The Bank executive management should provide its employees with continuous training and learning programs to maintain the level of knowledge and skills which meet the objectives of governance and management stated in Annex (3) of the instructions of governance and management of information and related technology No. (65/2016).

4- The Bank executive management should include in the annual performance evaluation mechanisms of its staff with objective measurement criteria which takes into consideration the contribution through the job title in the achievement of the Bank's objectives.

Thirteenth: Code of Ethics and Conduct

1- The Board shall authorize the IT Governance Committee to approve the organizational code of ethics which reflects the best international professional behavioral practices with regard to the treatment of information and related technology clearly setting the desired and undesired behavioral rules and their consequences.

2- The internal and external auditor should comply with the Code of Ethics and professional practices approved by the Board which include at least the code of professional ethics stated in the Information Technology Assurance Framework (ITAF) standard issued by the Information Systems Audit and Control Association (ISACA) and its updates.

3- The Board and the senior executive management should employ the different mechanisms for the encouragement of implementation of desired behaviors and avoidance of undesired behaviors through the motivation and punishment methods for example without limitation.