Enterprise Governance and Management of Information and Related Technology Manual

Bank of Jordan

Date : May/2019

Version : 2.0

Contents

1. Introduction

Bank of Jordan has recognized that the board and executives need to embrace IT like any other significant business asset in the Bank. The Board of Directors and executive management in both the business and IT functions collaborated and worked together to include IT within the governance and management approach.

The bank has taken the initiative to use the COBIT framework for the Governance and Management of Information and Related technology to assist the bank in achieving its objectives for the governance and management of enterprise IT. Simply stated, to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT enables the bank to govern and manage the IT in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

This manual should be read together with the bank's corporate governance manual.

2. Definitions

Governance	Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
COBIT	Formerly known as Control Objectives for Information and related Technology (COBIT); now used only as the acronym in its fifth iteration. A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT describes six principles for the governance system, three principles for the governance framework, and seven components that support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices.
Control	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure.

Enterprise goal	Business goal
Governance of enterprise IT	A governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives. It also includes the functional governance of IT, i.e., ensuring that IT capabilities are provided efficiently and effectively.
IT goal	A statement describing a desired outcome of enterprise I&T in support of enterprise goals. An outcome can be a significant change of a state or a significant capability improvement.
Alignment Goal	Alignment goals emphasize the alignment of all IT efforts with business objectives. It replaced the term IT Goals to avoid the frequent misunderstanding that these goals indicate purely internal objectives of the IT department within an enterprise.
Process	Generally, a collection of practices influenced by the enterprise’s policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services).
The Board	The Board of Directors of the Bank
Senior Executive Management	Comprised of General Manager (GM), Assistant General Manager, Chief Financial Officer (CFO), Chief Operations Officer (COO), Chief Risk Officer (CRO), Chief Compliance Officer (CCO), and Head of IT whereby this body is responsible for planning, building, running, and monitoring activities in alignment with the direction set by the governance body to achieve enterprise goals.
Stakeholders	Any interested party in the bank, such as shareholders, employees, creditors, customers, suppliers or external concerned regulatory bodies.

3. Scope

The scope of implementing this guide includes - on group level each country according to its local regulations - all the bank’s operations based on information technology in various branches and departments. All stakeholders shall be concerned with applying the instructions, each in its respective role and location.

Key stakeholders and their responsibilities:

- **Chairman and Board of Directors:** Shall be assigned the responsibilities of overall direction of the governance project/program, approve tasks and responsibilities within the project, and support and provide needed funds.
- **General Manager, Assistants, and Executive Managers:** Shall be assigned the responsibilities of hiring the right experienced people in the Bank's operations to represent them in the project and characterize their tasks and responsibilities.
- **General Manager, the Steering Committee of Information Technology, and the project managers:** take over the responsibilities of the project/program management and recommend the necessary resources.
- **Internal Audit:** participate in the IT governance project/program, representing the role of internal audit in executive matters as a consultant and independent Rapporteur to facilitate the success and completion of the project/program.
- **Risk, Information Security, Compliance and Legal Departments:** take over the responsibilities involved in the IT governance project/program, representing the role of those departments, and to ensure the representation of project/program by all interested parties.
- **The Bank’s Board and the Risk Management Department** shall take over direct responsibility for the process of "Ensure Risk Optimization (EDM 03)” and the process of “Manage Risk (APO12)”

4. Objectives

The Bank has set the following objectives of the governance and management of information and related technology framework:

4.1. Meet stakeholder needs and achieve the objectives of the bank through the utilization of an established IT governance framework

4.2. Facilitate the creation of value by delivering expected benefits, optimizing risk, and optimizing resources.

4.3. Provide the relevant and credible information that lead to effective and efficient decision making.

4.4. Provide technological infrastructure that aligns with the bank's objectives.

4.5. Enhance the bank's operations by employing efficient, reliable and purpose-driven technological systems.

4.6. Optimize IT risk management to ensure the necessary protection of the bank's assets.

4.7. Comply with the relevant laws, regulations, contractual agreements and internal policies.

4.8. Improve the reliability of the internal control environment.

4.9. Improve alignment between business needs and IT objectives.

4.10. Manage external party's services entrusted with carrying out operations, services and products to deliver the expected value.

4.11. Adopt international standards as baseline to govern and manage the information and related technology.

5. Key Principles of the Governance Framework

5.1. The enterprise governance of information and related technology in the bank is based on the six principles for the governance system of COBIT framework:

- **Principle 1: Provide Stakeholder Value**

  Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.

- **Principle 2: Holistic Approach:**

  A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.

- **Principle 3: Dynamic Governance System:**

  A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future proof EGIT system.

- **Principle 4: Governance Distinct from Management:**

  A governance system should clearly distinguish between governance and management activities and structures.

- **Principle 5: Tailored to Enterprise Needs**

  A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.

- **Principle 6: End to End Governance System:**

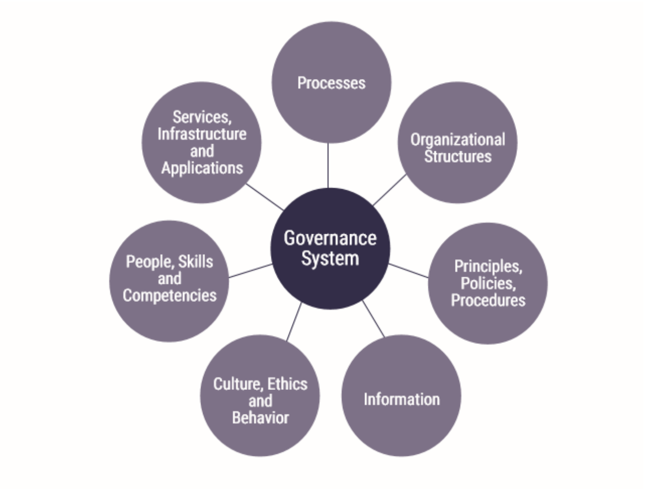
  A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise.

5.2. In addition to the above mentioned six principles, there are three principles for the governance framework of COBIT 2019 in the bank:

- Based on Conceptual mode
- Open and Flexible
- Aligned to Major Standards.

5.3. To satisfy governance and management objectives, the bank establishes, tailors and sustains a governance system built from a number of components:

- Principles, policies, and procedures
- Processes.
- Organization Structures.
- Culture, Ethics, and Behavior.
- Information.
- Services, Infrastructure, and Applications.
- People, Skills, and Competencies.


Processes
Services, Infrastructure and Applications
Organizational Structures
Governance System
People, Skills and Competencies
Principles, Policies, Procedures
Culture, Ethics and Behavior
Information

6. Committees

The following committees were established to govern and direct the governance framework in the bank.

6.1. **Information Technology Governance Committee\Board.**

6.1.1. Scope and purpose:

To govern IT activities are aligned with the business objectives and that stakeholder needs of benefit realization, risk optimization and resources optimization are met.

6.1.2. Members:

This committee shall be formed with at least three members from the board of directors itself, and preferably include people with experience or strategic knowledge in information technology.

The committee may invite General Manager and/or assistants, and/or executive managers to the meeting when needed.

6.1.3. Meeting Frequency:

The committee shall meet on at least quarterly basis and maintain documented records of the meetings.

6.1.4. Objectives:

6.1.4.1. To ensure alignment between business and IT strategic plans.

6.1.4.2. To manage innovation for the benefit of stakeholders.

6.1.4.3. To ensure that the infrastructure is in place and the related services are delivered.

6.1.4.4. Encourage transparency and effective program and project oversight.

6.1.4.5. Ensure independent audit over IT activities.

6.1.5. Committee Duties

6.1.5.1. To endorse the bank's Enterprise / Alignment Goals Matrix that links BOJ business Objectives and IT related goals/alignment goals and to define the related sub goals for the achievement of the Matrix.

6.1.5.2. To endorse the importance and priority of the Governance and Management Objectives and their relevance to the Enterprise Goals and IT/Alignment Goals, in addition to their related components. This endorsement should be based on an annual study that considers the design factors of COBIT 2019 framework guidance.

6.1.5.3. Endorse the strategic goals of information technology and organizational chart, including the steering committee at the executive management level and in particular "Information Technology Executive Steering Committee" to be aligned with enterprise strategic goals.

6.1.5.4. Endorse monitoring framework to manage, control and monitor the IT projects and their resources based on international best practices in this regard to achieve enterprise goals and the IT-related goals.

6.1.5.5. Endorse the RACI (Responsible, Accountable, Consulted, Informed)

chart for the IT governance and management processes.

6.1.5.6. Ensure the effectiveness of IT risk management, and aligned with overall risk management of the enterprise.

6.1.5.7. Endorse the IT budgets for IT strategic projects based on the enterprise goals

6.1.5.8. Monitor and review processes, resources, and IT projects to ensure their efficiency and effectiveness to fulfill the business requirements.

6.1.5.9. Review audit reports for information technology and take the necessary corrective action for any deviations

6.1.5.10. Escalate recommendations to the Board regarding taking corrective action.

6.1.5.11. To endorse the Information Security Policy, Cloud Policy, Cybersecurity policy, cybersecurity program and any related policy for Information and Security Technology.

6.1.5.12. Review and develop the Governance and Management of Information and Related Technology manual whenever needed to be in line with regulation, legislation and best practices

6.2. **Information Technology Executive Steering Committee.**

6.2.1. Scope and Purpose:

To ensure the alignment between the business and the IT, IT resources and IT risk management optimization.

6.2.2. Members:

Shall be formed and headed by the General Manager and with membership of senior executive managers, including the head of information technology, Risk Management, and Information Security Manager.

The Audit Executive manager and a member from the board are elected to be Rapporteur members in this committee.

The minimum quota to conduct a meeting is two thirds of the members including the head of the committee should be attended.

The committee can invite third parties to attend the meetings when needed.

6.2.3. Meeting Frequency:

The committee shall meet on at least quarterly basis, and maintain documented records of meetings.

6.2.4. Objectives:

6.2.4.1. To ensure that IT strategic goals are achieved.

6.2.4.2. To ensure that IT projects are prioritized properly and aligned with their business strategic purposes.

6.2.4.3. To optimize the employment of IT resources.

6.2.4.4. To optimize IT risk management.

6.2.5. Committee Duties:

6.2.5.1. To review and endorse to the IT Governance Committee, the importance and priority of the Governance and Management Objectives and their relevance to the Enterprise Goals and IT/Alignment Goals, in addition to their related components. This endorsement should be based on an annual study that considers the design factors of COBIT 2019 framework guidance.

6.2.5.2. Prepare, and supervise the execution of the annual plan based on enterprise strategic plan that is approved by the board and monitor all elements that effect the execution.

6.2.5.3. Align the enterprise goals with IT-related goals; and review continuously to ensure they achieve the strategic plan based on defined KPIs. The committee can delegate monitoring of the KPIs to the executive managers to report to the committee.

6.2.5.4. Recommend resource allocation to achieve the goals and related processes of IT governance and make sure of applying segregation of duties and conflict of interest principles.

6.2.5.5. Postpone, reject, and accept new projects and prioritize current and new projects.

6.2.5.6. Monitor the services and related technologies to improve their effectiveness.

6.2.5.7. Recommend to Governance of Information Technology Committee in regard to:

6.2.5.7.1. The necessary resources and mechanism to achieve the strategic goals

6.2.5.7.2. Any deviation that effects the achievement of strategic goal

6.2.5.7.3. Any unacceptable risk that is related to IT or information security

6.2.5.7.4. Reports related to performance, compliance with general framework of manage, control, and monitor of IT projects and their resources.

6.2.5.8. Provide the Committee of Governance of Information Technology with minutes of meetings.

6.2.5.9. Forming/reforming temporary committees for the banking and IT projects.

6.2.5.10. Supervise the execution of the bank’s projects and the related IT governance processes.

6.2.5.11. Review the cybersecurity strategy, policy and program and make sure of applying it in the enterprise; and ensure the alignment of cyber risk registry with IT risk profile.

6.2.5.12. Review continuously the cybersecurity risk level and the related events.

6.2.5.13. Endorse authorization matrix related to cybersecurity risk and security management in order to define related party to manage, control and monitor these risks.

7. Risk Management, Audit and Reporting

7.1. Risk Management

COBIT supports risk management and governance by establishing and maintaining an effective risk function based on COBIT's seven components, where it should be reflected on banks' main risk framework- reporting, operations, and committees duties.

7.1.1. Duties:

7.1.1.1. Taking over the direct responsibility for the process related to "Ensure Risk Optimization" and "Manage Risk"

7.1.1.2. To ensure of publishing this manual on the Bank's website and within the Bank's annual report.

7.1.1.3. To manage IT related risk and to ensure risk optimization.

7.2. Internal and External Audit

The Board shall monitor adequate budgets and allocate the necessary tools and resources, including qualified personnel, through specialized IT audit departments.

The Internal Audit Department of the Bank and the External Auditor should be qualified and holding international professional certification related to the field.

7.2.1. Duties:

7.2.1.1. Both Internal and External Audit will review and audit the allocation of resources and its management, IT projects, and the bank's operations based on a specialized technical review

7.2.1.2. The External Audit to provide an annual report in the first quarter of each year to Central Bank of Jordan. The report shall cover Risk and Control of IT and related technology and includes the Executive Management's response and the Board's recommendations regarding it.

7.2.1.3. The Audit Committee shall include the responsibilities, authorizations and scope of the IT audit process within audit charter and within agreed process with external audit.

8. Disclosure

This manual will be published on the Bank's website and within the Bank's annual report.