البنك الأهلي الأردني
Jordan Ahli Bank

Enterprise Governance of Information and Related Technologies Guide

Prepared for Jordan Ahli Bank

2019

Revision History

Changes	Reviewed by	Approval	Date	Version
Author	ISACA	Peter Tessin	Feb 2017	1.0
Reviewer	ScanWave C.T.S	ScanWave C.T.S	Feb 2017	1.0
Update	ScanWave C.T.S	ScanWave C.T.S	May 2019	1.1

Disclaimer

This guide is developed based on the Central Bank of Jordan regulations number No.: (65/2016), and its adjustments number (984-6-10)and ISACA's COBIT framework.

Contents

1. Introduction

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

In response to the Central Bank of Jordan's regulations number (65/2016) and its adjustments number (984-6-10), **JAB** has taken the initiative to use the COBIT framework for the Enterprise Governance of Information and technology (EGIT),to comply with the regulation.

COBIT provides a comprehensive framework that assists **JAB** in achieving its objectives for the governance and management of enterprise IT. Simply stated, it helps **JAB** create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT enables IT to be governed and managed 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.

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**: 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, 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 framework:** A framework is a basic conceptual structure used to solve or address complex issues; an enabler of governance; a set of concepts, assumptions and practices that define how something can be approached or understood, the relationships amongst the entities involved, the roles of those involved, and the boundaries (what is and is not included in the governance system).
- **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 IT in support of enterprise goals. An outcome can be an artefact, 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:** 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:** Includes Bank's general manager or regional director, deputy director-general or deputy regional director, assistant general manager or assistant regional director, CFO, COO, Director of Risk Management, Head of Treasury (Investment), director of compliance, as well as any employee of the bank that has executive authority parallel to any of any of the above-mentioned authorities and functionally and directly linked to director general.
- **Stakeholders**: Any interested party in the bank, such as shareholders, employees, creditors, customers, suppliers or external concerned regulatory bodies.

3. Context

Jordan Ahli Bank (JAB) (previously Jordan National Bank) is a Jordanian institution founded in 1955 and its main offices are in Amman. Ahli Bank was the sixth public shareholding company to be established in Jordan. JAB has two international offices in Cyprus and Palestine.

JAB organization consists of the following main sectors: Business Sector, Credit Sector, and Support Sector. Human Resources and Finance. Jordan Ahli Bank owns three companies fully: Ahli Microfinance, Ahli Brokerage and Ahli Financial Leasing. JAB offer financial products and services in corporate banking, project finance, Small and Medium banking, consumer (retail) banking, Treasury and investment. All bank's products and services are managed through a products and services development unit.

JAB operates through 52 branches, 3 VIP Halls, 1 Corporate branch and 8 SME business centers cross all Jordan governorates. JAB operates more than 109 ATMs in addition to electronic channels that include: Personal Internet Banking, Mobile Internet Banking, Corporate Internet Banking, SMS, Interactive Teller Machine (ITM, ChatBot, Social Media, Interactive Voice Recognition (IVR), and Call Center. JAB offers a set of different personal banking products such as:

Deposits: which include savings, current and call accounts in addition to fixed term deposits. Loans: which covers different types of personal loans such as housing and car loans.

Through its SME unit, JAB offers commercial loans and overdraft facility in addition to a unique chance for small and medium enterprise owners to develop their business and overcome obstacles that they face, which differ from those faced by corporations. We give you financial solutions and advisory to assist the growth of your business with well researched methods. JAB offers a set of Corporate banking services and products through its dedicated corporate branch. This includes syndicated loans, letters of credit and guarantees, commercial loans and overdraft accounts. The Treasury unit of JAB offers services in portfolio management, cash management and correspondent banking.

In addition, JAB has implemented the following service quality activities

1. Activating phone feedback related to services at the business centers.
2. Preparing working schemes to expose clients' experience with the bank and prepare plans and implementation strategies for the year 2016.
3. Developing a mechanism to follow-up on the complaints received as well as ensuring it is in accordance with the Central Bank's instructions on transparency.
4. Participating in implementing the action plans for the SMEs, especially, Service Level Agreements (SLA).
5. Participating along with the New Banking System implementation team to develop a methodology intended to elaborate and follow up on Service Level Agreements (SLA).


الهيكل التنظيمي العام
مجلس الإدارة
سعد المعشر (الرئيس)
أمانة سر المجلس
الرئيس التنفيذي/ المدير العام
محمد موسى داود
نائب الرئيس التنفيذي/ المدير العام
أحمد الحسن
المخاطر
التدقيق الداخلي
الامتثال ومكافحة غسل الأموال
مكتب الاستراتيجيات وإدارة المشاريع
الرقابة الداخلية
قطاع الأعمال
قطاع الائتمان
قطاع الدعم
الإنتاج والابتكار
إدارة الموارد البشرية
الإدارة المالية
Ahli Fintech

4. Scope

The scope of implementing this guide includes all **JAB** operations based on information technology in various branches and departments. All stakeholder parties shall be considered concerned with applying the instructions, each in its respective role and location.

The following parties and their key responsibilities are defined in CBJ regulations in this regard:

- Chairman and members of the Board and outsourced experts:

  Shall be assigned responsibilities of overall direction of the IT governance project, approve tasks and responsibilities within the project, and support and provide needed funds.

- JAB CEO and its deputies and assistants, and directors of operations and branches: Shall be assigned responsibility of hiring the right experienced people in the Bank's operations to represent them in the project and characterize their tasks and responsibilities.

- JAB CEO and the directive/steering committee of information technology and the project managers: take over the responsibilities of the project/program management.

- Internal Audit: take over their responsibilities directly upon the instructions, and participate in the project/program, representing the role of internal audit in executive matters as a consultant and independent observer to facilitate the success and completion of the project/program.

- Risks, information security, compliance and legal departments: take over the responsibilities involved in the project/program, representing the role of those departments, and to ensure the representation of project/program by all interested parties.

- Specialists, holders of technical and professional certificates of (COBIT Foundation COBIT Assessor, COBIT Implementation, CGEIT) standard, who are hired from inside and outside the bank: take over the role of the mentor to disseminate knowledge of the standard and to facilitate the implementation process.

- According to CBJ regulations, **JAB** Board shall have direct responsibility for the five processes of Governance (EDM) (Evaluate, Direct and Monitor).

- **JAB** Board and Risk Management Department shall take over direct responsibility for the process of "Ensure Risk Optimization" (EDM 03) and the process of "APO12 Manage Risk."

5. Objectives

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

5.1. Meet stakeholder needs and achieve the objectives of the bank through the utilization of an established governance framework that:

- Facilitates the creation of value by delivering expected benefits, optimizing risk, and optimizing resources.
- Provides assurance of information quality to support decision-making.
- Provides for technological infrastructure that enables the bank to achieve its objectives.
- Upgrade the bank operations by employing efficient, reliable and purpose-driven technological systems.
- Strict the risk management of information technology to ensure the necessary protection of the bank's assets.
- Assist in achieving compliance with the requirements of laws, regulations and instructions as well as to comply with **JAB** policies, strategy and internal working procedures.
- Improve the reliability of the internal control environment.
- Maximize the level of satisfaction of information technology users by efficiently and effectively meeting the needs of their work.
- Management of external party's services entrusted with carrying out operations, services and products.

5.2. Utilizes the COBIT process reference model to design efficient and effective solutions to delivery of value to stakeholders.

5.3. Separates governance from management consistent with internationally recognized standards for the governance and management of information and related technology.

6. General Policies

6.1. This guide is based on the Central Bank of Jordan's regulations No: (65/2016) and its adjustments number (984-6-10) , and it is created based on the COBIT framework. It should be reviewed and updated on regular basis to ensure its consistency with any updated regulations, or framework update by ISACA.

6.2. **JAB** shall, through the committee of Information Technology Governance emanating from the Board, review this guide and update it whenever necessary.

6.3. The bank shall publish this guide in any appropriate method for public inspection.

6.4. **Committees**

- **JAB** has established the required committees to govern and direct the governance framework in the bank; IT Governance Committee, and IT steering Committee.
- **IT Governance Committee**:
  - As per the Central Bank of Jordan instruction, the Board shall form a committee of governance of information technology from its members, and this committee shall be formed from three members at least, and preferably include people with experience or strategic knowledge in information technology.
  - The committee shall meet on a quarterly basis at least, maintains documented records of the meetings, and shall have the tasks mentioned in CBJ regulations.
- **IT Steering Committee:**
  - The senior executive management shall form necessary directive committees to ensure a strategic alignment of information technology to achieve the strategic objectives of the bank and that shall be in a sustainable manner. Therefore, a committee named the Directive Committee of IT shall be formed and headed by general director and with the membership of senior executive management managers, including the director of information technology, director of risk management and director of information security. One of its members shall be elected to be an observer member in this committee as well as the director of internal audit, and can invite third parties to attend the meetings, when needed.
  - The committee shall document its meetings, provided that periodic meetings shall be once every three months at least, and shall, in particular, carry out the duties mentioned in CBJ regulations

6.5. **Enterprise Goals and Alignment Goals**

JAB IT Governance Committee shall 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 a study (at least annually) taking into account COBIT 2019 framework design factors framework guidance, aligned with the Bank's specificity and strategies.
Adopting the matrix of enterprise objectives, and the goals of information and related technology objectives.

6.6. **Policies System**

JAB Board or its delegate committees will adopt the necessary policies system for the management and operations of governance of information technology as per Appendix A, and to consider this policy system a minimum with the possibility of the combination of these policies as the work nature requires.

6.7. **Information and Reports**

- The **JAB** Board and senior executive management will develop the infrastructure and systems necessary to provide information and reports to their users as an anchor for the decision-making processes in the bank.
- **JAB** Board or its delegate will adopt information systems and reports contained in Appendix B, and consider those systems a minimum, determining the owners of such information and reports through which authority to review and use is determined and delegated as needed for the work.
- **JAB** policies and reports will be regularly reviewed and updated to reflect the development of the bank's objectives and operations and in accordance with accepted good practices and standards.

6.8. **Organizational Structures:**

JAB Board will adopt the organizational structures (hierarchical and committee's structures) concerning the management of resources, processes and projects of information technology, risk management, information security, and human resources management.

6.9. **Services, Programs and Infrastructure of Information Technology:**

- **JAB** Board or its delegate committees and senior executive management will adopt systems of services, programs and IT infrastructure supporting information (appendix C) to achieve IT governance and management objectives.

6.10. **Knowledge, Skills and Experiences:**

- **JAB** Management and the Board or its delegate committees shall adopt necessary matrices of competencies (HR Competencies) and policies of human resources management to achieve the requirements of the governance and management objectives, and to ensure that the appropriate human resources are in place.
- The bank's executive management shall continue to enroll its staff in training and continuing education programs to maintain the level of knowledge and skills necessary to meet and achieve the governance of information technology.

6.11. **System of Values, Morals and Behavior:**

- **JAB** Board or its delegate committees shall adopt a code of conduct that reflects professional behavior related to the management of information and its related technology that clearly define the desired behavioral rules and consequences.

The Governance Framework of Information and Related Technology

7. Six key Principles of the Governance System of COBIT Framework

The governance framework of information and related technology **at JAB** is based on six key principles of COBIT:

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:

- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

• **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.

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.

Management: plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

• **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.

1. Principles, Policies and Frameworks
2. Processes
3. Organizational Structures
4. Culture, Ethics and Behavior
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

8. Goals Setting and Cascading

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system.
Consistent with the principles and guidance in COBIT, **JAB** will create a governance structure based on stakeholder requirement and value delivery. **JAB** will also create a sustainable strategy of governance, management and business alignment to stakeholder needs.

JAB has adopted the COBIT goals cascade mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT-related/alignment goals and governance and management objectives goals. This translation allows setting specific goals at every level and in every area of the bank in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between the **JAB** needs and IT solutions and services.

Step 1. Stakeholder Drivers Influence Stakeholder Needs
Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.

Step 2. Stakeholder Needs Cascade to Enterprise Goals
Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard (BSC) dimensions, and they represent a list of commonly used goals that an enterprise may define for itself. Although this list is not exhaustive, most enterprise-specific goals can be mapped easily onto one or more of the generic enterprise goals.

Step 3. Enterprise Goals Cascade to Alignment Goals
Achievement of enterprise goals requires a number of IT-related outcomes/Alignment Goals, which are represented by the Alignment goals. COBIT defines 13 IT-related goals.

Step 4. -Alignment Goals Cascade to Governance and Management Objectives.
Achieving alignment goals requires the successful application and use of a number and target levels of governance and management objectives.

Appendix A: Minimum Set of Policies for the Governance Framework

**The below table is based on CBJ instructions number (6), which is based on ISACA's COBIT framework*

JAB will adopt the below list of minimum set of policies to govern and manage the processes in the Bank.

Policy Name	Purpose	Scope
Governance of information technology.	Setting necessary rules and standards for the management of information technology resources, including administrative form (centralized or decentralized), and organizational structures, including the activities, functions and responsibilities of the management of these resources, including financial resources.	Operations, services and projects of information technology.
Information Security	Development of the standards necessary to ensure the protection and confidentiality requirements, credibility, availability and compliance to manage IT resources according to accepted international standards in this regard, such as (ISO-IEC 27001/2)	All information and technology associated with it.
Business continuity plans and disaster recovery plan	Establish rules needed to build disaster recovery, business continuity plans, including mechanisms for construction, operation, inspection and training and update those plans to ensure high availability of critical bank operations and standards.	Bank operations critical, and the protection of human beings.
IT Risk Management	Rules and standards for the management of information technology risks to be considered as part of the overall risk of the bank, including governing those risks, responsibilities and tasks assigned to the different parties, and evaluation mechanisms and risk control, in order to enhance decision-making processes based on risk and achieve the objectives of the Bank.	All the bank's operations and inputs related to information technology.
IT Compliance	Development of the standards necessary to ensure compliance with the instructions of the Central Bank and other regulatory bodies and the applicable laws and regulations and the policies of the bank.	All bank threads of information technology operations.
Data Privacy	Establish rules necessary for the protection of data. Addressing disclosures and unauthorized use of standards.	All private data.
Outsourcing	Policy for the use of resources in general and resources of information technology in particular, that the bank-own (In-sourcing) or outsourcing. take into account the instructions and regulations, laws and mimic accepted best international practices in this regard, and take into account the operations location "On-site , Off-site, Near-site, Off-shore" and take into account the service level requirements, and activation of the right of Audit (Audit right) by credible third parties, and to achieve the requirements of business continuity and the controls necessary to protect to the confidentiality and credibility as well as the efficiency and effectiveness in the use of resources.	All the bank's operations.
Project Portfolio Management	Development of standards for the management of projects, including phases of the project and the governance necessary to achieve the requirements relating to quality (Quality Requirements) and those relating to the protection and confidentiality (Confidentiality Requirements) and those relating to compliance achieve the objectives of the bank and its operations.	All Bank projects related to information technology.
Asset management	Setting rules for the classification of the degree of risk data and the various regulations and standards, and to identify owners and controls protected during the various stages of their life cycle.	Data, hardware, software and tools associated with it.
Acceptable use of information technology resources	The development of rules and standards to determine acceptable behavior and unacceptable for information technology resources.	Hardware, software, applications and networks, including the Internet and e-mail.
Change Management	Development of standards necessary to ensure the credibility of the change in documenting the necessary approvals from the assets subject to change owners.	All information technology operations.
Mainframes/servers	To establish rules and standards to reduce the processes of access and illegal use of devices.	All organizations and central-owned or managed by the Bank for all development environments, testing, operation, including operating and other tools associated systems.
Client Machines	The development of rules and standards of behavior and other technology to ensure the protection of sensitive data stored on the devices.	All the client machines linked to networks or stand alone machines.

Policy Name	Purpose	Scope
Portable devices	The development of rules and standards to ensure the protection of sensitive data stored on portable devices.	All portable devices such as Laptop, PDA, Smartphone, USB Memory Cards, ... etc.
User Access Management	The development of policy for access management; granting access to the data and the software and hardware, according to the business needs to ensure confidentiality, credibility and availability of the resources of information technology.	All software and hardware, databases.
System Development Lifecycle	Development of policy for the development and acquisition of software.	The new/upgraded software developed in house or purchased.
Service Level Management	The development of rules and criteria for identifying and accepting, documenting and measuring, monitoring and improving the level of services provided both internal and external parties to ensure optimal utilization of resources.	All agreements and contracts and obligations with internal and external parties.
Backup and Restore	The development of policy for backup and recovery mechanisms to ensure high availability of data, credibility and confidentiality.	Data in operating environments where needed.
Data Retention	Development of policy for the amount of the data that should be available either in paper or those located on computers and various applications and the length of time to be retained and the trade-off between the amount of data available and the speed and performance in data access.	All the hardware and software tools, means and data retention.
Purchasing Policy	The development of rules and standards of the evaluation of external suppliers.	All the technical equipment and related programs.
Remote Access	The development of rules and standards for the remote access to the bank's computer networks and devices.	Parties and partners, internal and external, such as service providers, and all development environments and testing and operation of devices and networks, including, but not limited to Internet networks, and networks encrypted, and lines of different communication such as (Frame relay, ISDN, VPN, DSL, MPLS)
Networks	The development of rules and standards to ensure efficiency and effectiveness requirements in the use of the network elements.	All network elements in all environments.
Wireless networks	The development of rules and standards in order to protect sensitive data transmitted over wireless networks from interception and illegal use.	Including all the physical and virtual wireless networks.
Firewalls	Setting minimum rules and standards governing the protection of the bank's firewalls.	All the Firewalls operating in all environments such as (DMZ, Proxy, External DNS, VPN, Routers, Switches, Servers, ... etc)
Penetration Testing and Vulnerability Assessment	Testing the devices and network elements to ensure no security breaches/ vulnerabilities in place.	All the technical assets of the Bank of servers/clients/ and components of the networks and software.
Public Branch Exchange	Setting minimum tandards for the protection of the public branch exchange ensure the protection and confidentiality of the data and the Bank's operations from illegal use.	All owned and non-owned devices in the bank.

Appendix B: Minimum Set of Reports for the Governance Framework

**The below table is based on CBJ instructions number (7), which is based on ISACA's COBIT framework*

JAB will adopt the below list of minimum set of reports to ensure proper reporting is maintained in the bank, the reports are considered as an anchor for the decision-making processes in the bank

1. Authority Matrix
2. IT Risk Factor Analysis
3. IT Risk Scenario Analysis
4. IT Risk Register
5. RACI Chart
6. IT Risk Profile
7. IT Risk Report
8. IT Risk Map or Heat Map
9. Risk Universe, Appetite and Tolerance
10. Key Risk Indicators
11. Risk Taxonomy
12. Risk and Control Activity Matrix (RCAM)
13. Information Security budget
14. MIS Reports
15. Audit Strategy
16. IT Audit Charter and Engagement Letter
17. IT Audit Plan
18. HR Matrix
19. Assurance Findings Register
20. Assurance Report Repository
21. The best international standards for the management of projects and information technology resources, and risk management, information technology, security, protection and checking on information technology

Appendix C: Services and Software Infrastructure for Information Technology

**The below table is based on CBJ instructions number (8) please refer to it for further details.*

JAB will adopt the below list of systems of services, programs and IT infrastructure supporting information to achieve the governance and management objectives of information and related technology.

1. Incident Management Services
2. IT Assets Inventory
3. Awareness of information security good practices
4. Security and protection of data and logical information
5. Surveillance Information Security
6. SOFTWARE auditing IT
7. Hosting and controls the physical security and environmental Physical and Environmental Security for server rooms and chambers of communications and electricity supply.

References

- Central Bank of Jordan regulations number No.: (65/2016), and its adjustments number 984-6-10
- ISACA COBIT framework.