CITIBANK N.A JORDAN

Governance and Management of Information and Related Technologies Guide

2018

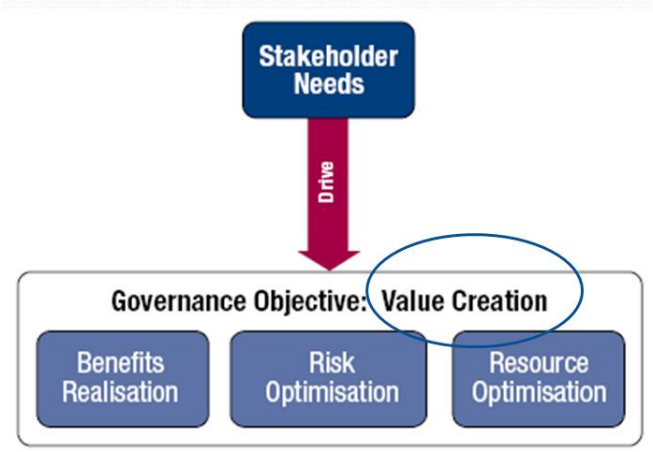
Table of Contents

1. OVERVIEW

Technology has become essential for managing enterprise resources and business processes, dealing with third parties, and increasingly enabling global communications and transactions.

During the last decades and in an incremental momentum, a growing need to comply with regulatory and legal requirements had an impact on technology. The continuity of Business and reliability of most the primary and secondary business processes and operations rely heavily on Information Technology IT.

Having disruptive technologies may impact business competitiveness, income, and existence. Citigroup and its consolidated subsidiaries including Citibank N.A. and its overseas branches collectively herein under referred to as "**Citi**' has foreseen the importance of a governance system for the enterprise IT to provide technology with leadership and organizational capabilities to sustain and extend the enterprise's strategies and value creation for our stakeholders through Benefits realization, Risk and resource Optimization.



Citi has foreseen the high benefit from following the Control Objectives for Information Technology (COBIT) framework, and had adopted it since 2008; Citi worked continuously over the years to upgrade our IT Governance system to the latest versions of COBIT and reflect the best practices on our standards and working environment in order to maximize the value added for the benefit and protection of our stakeholders.

Based on the above, Citibank NA Jordan has created this document in response to the Central Bank of Jordan (CBJ) instructions number 65/2016 regarding "Information Management and related technology Governance" as to ensure that Stakeholders needs and transparency are achieved through aligning IT objectives with Business Objectives.

Citi Governance of Enterprise IT is centralized abroad and applied on all Citi subsidiaries/branches including Citibank, N.A. Jordan, covering more than 160 countries. Therefore, most of our Governance and management system are governed and managed centrally by our Citi global teams.

In addition, Citi governance of enterprise IT has a set of internal policies and standards that supports and enables the IT governance system which covers all the applicable processes related to information and related technology which include but is not limited to Disaster Recovery, Information Security, IT Policy Framework, Vendor Management, Operational Risk Management, and Code of Conduct.

2. Governance of Enterprise IT

As a responsible Corporation, we protect our clients' information entrusted to us as well as ensuring the security and integrity of our own information.

Citi IT governance is the system by which Citi sets the strategy for implementation of technology, supervises the management of Information Technology and Information Security, and establishes a clear reporting structures, including the roles and responsibilities of key governance functions, that supports Citi's IT management on a consistent global basis.

Citibank N.A. Jordan branch adheres to Citi governance of enterprise IT. Technology, Operations and Business should be aware of and comply with the governance of enterprise IT and must ensure that all of their processes that are based on technology comply with IT governance standards. Failure to properly follow the enterprise of IT governance may result in financial loss or damaging our reputation as well as impacting negatively Citi's safety and soundness.

Our governance system is based on and aligned with the following frameworks to the extent that suits our Global organizational structure:

- The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbooks.
- The Control Objectives for Information Technology (CoBIT5) an international framework for managing technology.

COBIT 5 provides a comprehensive framework that assists the bank in achieving its objectives for the governance and management of enterprise IT. The implementation of COBIT5 helps the bank in the creation of optimal value by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

2.1 Management of Technology

The CIO Council (CIOC) manages technology for Citi in line with its Charter; it has defined Process Areas covering all major aspects of IT to maintain an effective governance structure. The CIO Council through its governance functions establishes common policies, standards and operating metrics.

When determining and delivering technology solutions in support of business requirements, technology organizations weigh business objectives against the types of risk that they will need to manage in accordance with Citi's Technology Risk Appetite Statement.

2.2 IT Risk Management

Information Technology (IT) Risk Management Governance is the system by which Citi sets strategic aims, provides leadership to put them into effect, supervises the Information Technology management of Citi Businesses, and reports on the state of the IT Risk to Citi's management, shareholders, and regulators. The establishment of clearly defined management and reporting structures, including the roles and responsibilities of key governance functions, supports Citi's IT Risk management on a consistent global basis.

Collectively and through their members, the CIOC and their subsidiary IT governance functions are responsible for the following:

- Serve as the senior integrated decision-making body for Citi Technology
- Lead Technology strategy, oversight, and execution
- Set technology standards, drive transparency and enforce implementation
- As appropriate, provide direction and monitor progress on meeting enterprise wide regulatory commitments owned by Technology
- Monitor operating metrics and Key Risk Indicators (KRIs)

2.3 Governance of Enterprise IT Goals:

The Governance of Enterprise IT aims to achieve the following goals:

- Maintain high-quality information and reports to support business tactical decisions.
- Generate business value from IT-enabled investments, and realize business benefits through effective and innovative use of IT.
- Achieve operational excellence through the reliable and efficient application and use of technology.
- Optimize IT related risk and maintain it at an acceptable level to protect Bank's assets and Operations.
- Optimize the cost of IT services and technology by prudent IT project and resources management
- Comply with the increasing laws, regulations, contractual agreements and policies.

3. Principles of Governance of Enterprise IT:

Citi Governance system is aligned with COBIT 5 principles for governance and management of enterprise IT:

• **Principle 1: Meeting Stakeholder Needs and creating value** by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. Citi Governance system is based on COBIT5 required processes and other enablers to support business value creation through the use of IT. This is achieved by the strategic alignment and integration between IT and Business

• **Principle 2: Covering the Enterprise End-to-end by integrating the** governance of enterprise IT into enterprise governance; covering all the enterprise functions and processes which depend on information and related technology.

• **Principle 3: Applying a Single, Integrated Framework** by alignment with other relevant standards and frameworks at a high level, which aids in standards integration and facilitating the decision making.

• **Principle 4: Enabling a Holistic Approach** Citi acknowledge the importance of the COBIT 5 seven enablers to support the implementation of an efficient and effective governance and management of enterprise IT, and their fundamental effect for achieving the objectives of 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

• **Principle 5: Separating Governance from Management** Citi is aligned with COBIT 5 framework in the distinction between governance and management, with different organizational structures, type of activities, and purpose. The Board of Directors (BoD) with the several committees evaluate, direct, and monitor the performance of the organization according to the stakeholders objectives, while the management mange the implementation in accordance to the direction of the Board of Directors (BoD). At a country level, Citibank N.A Jordan, has created a new IT steering Committee to cover the tasks required By Central Bank of Jordan.

4. Governance Enablers:

Citi highly acknowledge and continuously works on strengthening the seven enablers of COBIT5 for the importance of these enablers in achieving the organizational overall objectives by sustaining the strategic direction and accommodating with the strategic changes. This set of enablers is an important part of the organizational resources by which it creates the most suitable environment to work in, in an efficient and effective manner. A lack of any of these enablers may affect the ability of the enterprise to create value for our stakeholders.

Citi Set of enablers are:

4.1 Principles, Policies and Frameworks

Citi has a set of global standards, principles, policies and frameworks necessary to achieve the overall objectives of the Governance and Management of the Enterprise IT, these set of standards, principles, policies and frameworks, define the rules for an effective and efficient management and control of the IT resources and projects to meet the organizational objectives.

4.2 Processes

Citi has adopted the 37 COBIT5 processes to the level that meets its global organizational structure, with which it ensures the achievement of the overall objectives of the Governance and Management of the Enterprise IT in an effective and efficient manner.

4.3 Institutional Structures

The Organizational Structure at Citi meets with the requirements of the CBJ and IT Governance while maintaining adequate segregation of duties, ensuring independence, bilateral control regulatory protection requirements, as well as maintaining updated job descriptions.

4.4 Information and reports

Citi has developed the infrastructure and the information systems required to provide responsible stakeholders and as per the work requirements with the information and reports for decision-making processes following the information quality criteria requirements

4.5 Services, programs and infrastructure of information technology

Citi has an extensive range of global IT services, software and infrastructure supporting and assisting governance and management of enterprise processes. These processes are binding to all Citibank branches including Citibank Jordan, supporting the achievement of IT objectives and business objectives.

4.6 Knowledge, skills and experience

Citi ensure that employees are one of the most important enablers. Therefore, Citi emphasizes on selecting and recruiting the right person in the right job. The Bank's management is continuously engaged in recruiting experienced employees and providing its staff with ongoing education and training programs to develop their skills set, and having periodic performance assessment and feedback taking into consideration the contribution of achieving the Bank's objectives.

4.7 Values, Morals and Behaviors

Citi is working on a continuous momentum to build a strong ground through the establishment of an ethical, professional and corporate system that reflects the accepted international professional norms regarding the handling of information and associated technology that clearly define desirable and undesirable rules of conduct and their consequences.

5. Goals Setting and Cascading

Citibank Jordan branch operates as part of Citi global model, having both global and local stakeholders. Citi global goals are built according to the global stakeholder drivers such as regulatory, technology, and strategy changes that influence our global stakeholder needs, from which the overall Global enterprise goals are formulated and cascaded to the global IT goals reflecting on the local countries IT goals.

On the local level, Citibank Jordan local enterprise objectives are built according to the local stakeholders' drivers and needs, and are cascaded to the IT-local goals.

Both global and local IT-goals are consolidated and categorized based on Citi balanced Scorecard, which can be mapped to the regular balance scorecard of; Internal, Knowledge, Customer, and Financials – which are listed below:

- Develops Our People
- Drives Value for Clients
- Works as A Partner
- Champions Progress
- Lives Our Values (including Responsible Finance Goals)
- Delivers Results

6. Committees

Citibank Jordan NA is a foreign branch operating in Jordan having no board of directors locally. Our governance is happening centrally on the group level, setting overall directions and management of Enterprise governance of IT.

On the global level, Citi CIO Council (CIOC) manages technology globally and serves as the single consolidated decision-making and governance body for Citi Technology, driving a unified strategy across the enterprise, setting policies and standards, and managing results. The CIO council has defined Process Areas that are aligned with COBIT 5 covering all major aspects of IT to maintain an effective governance structure at a global level.

The Operations and Technology O&T Committee of Citigroup oversees the scope, direction, quality and execution of Citi's technology strategies. It takes updates from the CIO Council on relevant topics to the O&T committee of the board.

This model supports the group governance structure that is responsible for setting overall directions and management of governance of Enterprise IT.

On the local level, Citi's international franchises have been managed by a globally standardized framework, centered around the Citi Country Officer (CCO) role and the principal governance committees listed below:

1. COUNTRY COORDINATING COMMITTEE (CCC)

- The CCC is the principal management committee in which the principals of the significant front, middle and back offices come together monthly to discuss high level strategic franchise matters.
- The CCC should review the country's business performance, coordinate business strategic planning, optimize investment and very importantly focus on talent management: development, sufficiency, retention and hiring. The CCC helps ensure the mobilization of talent and that there is a talent strategy that aligns with the business strategy.
- The CCC helps to define risk appetite within country and develop target markets and products for the country.
- A part of the agenda for the CCC may include significant material issues from the BRCC and other committees
- The CCC should maintain the right membership, and be monitored carefully to ensure a high rate of attendance.

Agenda includes, but are not limited to:

- Franchise Management (such as country financials, business performance, client relationships, implementation of Citi-wide initiatives, etc.)
- Franchise Protection (such as issues escalated from other committees, regulatory developments, significant current and emerging franchise risks, etc.)
- HR/Talent (such as VOE, turnover, succession planning, etc.)
- External Relations (such as government, regulatory, media and community relations, etc.)

2. BUSINESS RISK, COMPLIANCE AND CONTROL COMMITTEE (BRCC)

- The BRCC supports the ORM Framework and focuses on significant risk and control themes, emerging risks impacting business objectives and other relevant aspects of the business' operational risk profile.
- BRCC is a committee which provides a forum for escalation and reporting of operational risk events, internal control, legal, compliance, Regulatory, Risk and any other significant issues that require attention of the committee.
- One of the principal goals of the Egypt BRCC is to fulfil regulatory requirements. The objective of the BRCC is to discuss and challenge the management of the most significant risk and control issues impacting the business activities, including the proposed associated action and remediation plans & to monitor the management of business risks that affect Citi Jordan franchise and as well as its constituent parts.

- The Committee also serves as the escalation channel on any matters arising from principle or subsidiary governance committees within the business. Accordingly, the BRCC forum shall facilitate the development of a clear understanding of the practices, governance and risks applicable to the Egypt franchise and how those risks may affect the franchise as a whole.
- The committee shall perform any functions in furtherance of the purpose of the committee as outlined above; as may be appropriate in light of changing business, legislative, regulatory or other conditions; or as may be delegated to the Committee by Citi management from time to time
- As per the Operational Risk Management Policy, the country BRCC meets at least quarterly and is owned and chaired by the CCO or the Business Head or delegate responsible for regional or global Businesses. The scope, membership and administration of the BRCC are outlined in Operational Risk Management Policy.
- The objective of the Operational Risk Management Policy ("Policy") is to establish a consistent Operational Risk Management ("ORM") Framework for assessing and communicating operational risk and the overall effectiveness of the internal control environment across Citi. The Operational Risk Management Framework is intended to ensure effective management across Citi of the operational risks and ongoing exposures in the development and delivery of products and services to our clients, and support adherence to regulatory requirements including Basel III.

Based on the above, and on CBJ instructions (2016/65), IT steering Committee is formed with a separate charter to accommodate the new requirements set in CBJ instructions.

3. IT Steering Committee

The IT steering Committee tasks are:

1. Develop annual plans to reach the strategic objectives, supervise and ensure their implementation and monitor the internal and external factors affecting them continuously.
2. Align Bank's Objectives with the information and related technology objectives, adopting and reviewing them on an ongoing basis, ensuring the achievement of the bank's strategic objectives and the objectives of CBJ instructions No (65/2016);
3. Recommend the allocation of financial and non-financial resources and employing the efficient and appropriate human element in the right place, taking account of separation of functions and non-conflict of interest, as well as overseeing the implementation of the IT projects,
4. Prioritize IT projects and programs.
5. Monitor the level of technical and technological services, raise their efficiency and improve them continuously.
6. Review IT audit reports and take action to address the deviations.
7. General supervision and monitoring the processes, resources and projects of information technology to ensure their efficiency and effective contribution to the fulfillment of the bank's requirements and works

8. Submit the necessary recommendations to Branch Risk and Controls Committee with respect to the below:
    a. Allocate the necessary resources and mechanisms to achieve the tasks of the IT Steering Committee.
    b. Any deviations that may adversely affect the achievement of strategic objectives.
    c. Any unacceptable risks related to information technology, security and protection.
    d. Performance reports and compliance with the requirements of the overall framework for the management and control of IT resources and projects.

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

7. Internal and External Audits:

Internal and external Information management and related technology audits shall be conducted in alignment with the CBJ regulation No: 65/2016

7.1 Internal Audit

Internal Audit is an independent function which provides independent, objective, reliable, valued and timely assurance to the Boards of Directors of Citigroup and Citibank, the Audit committees, senior management and regulators regarding the effectiveness of governance, risk management, and controls that mitigate current and evolving risks and enhance the control culture within Citigroup and Citibank, through risk-based audits, other audits, business monitoring and issue validation. This is achieved by the following:

- The Internal Audit function abides by the Citigroup Inc. and Citibank, N.A. Internal Audit Charter, which covers the Objectivity and Independence requirements, Internal Audit's Authority and responsibilities, Standards of Practice and scope of Internal Audit work, and which is reviewed on an annual basis to ensure it remains current and in accordance with current standards.
- The Internal Audit has independent audit teams covering all Bank activities including Technology processes.
- Internal Audit follows the Risk-based Audit Methodology and develops audit programs, which take into account relevant best practices and international standards.
- Internal Audit conducts reviews based on the risk-based multi-year assurance plan, which is refreshed quarterly. This plan captures relevant regulatory coverage requirements and includes technology audit plan, which is an integral part of the risk-based assurance plan.
- Internal audit ensures coverage of key controls established in-country and those outsourced to other Citi affiliates and third party vendors.
- Internal Audit, under the oversight of the Audit committee, ensures appointment of qualified employees with appropriate technical qualifications and related experience to audit all key

activities and operations, including Technology controls, and provides training to enhance their knowledge of product-specific and organization-wide topics.

- Internal Audit continuously monitors the status of audit issues and recommended corrective action plans and reports on them in governance forums to ensure timely implementation and validation.
- Internal Audit maintains all audit work in Internal Audit Management System (AIMS), which is the Internal Audit repository for audit documentation, issues and reports, and follows Citibank's Record Retention policies and applicable local requirements, whichever is more stringent, in retaining the audit documentation and reports, in an organized and secure manner to be available for review by the supervisory authorities and the independent auditors.

7.2 The External Audit shall:

- Perform independent reviews to attest the effectiveness and efficiency of the implemented controls of the Enterprise Governance and management of Information and related technology in line with CBJ regulations (Regulations: No 65/2016)

8. Glossary – from COBIT5 foundation

The following terms shall have the meanings respectively assigned to them herein below:

1. **Alignment:** A state where the enablers of governance and management of enterprise IT support the goals and strategies of the enterprise
2. **Enterprise goal:** The translation of the enterprise's mission from a statement of intention into performance targets and results
3. **COBIT 5:** 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 five principles and seven enablers that support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices.
4. **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.
5. **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.
6. **Governance enabler:** Something (tangible or intangible) that assists in the realization of effective governance
7. **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).
8. **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.
9. **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.
10. **Management:** Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
11. **Process:** Generally, a collection of practices influenced by the enterprise's policies and procedures that take inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services).
12. **Stakeholders:** Any interested party in the bank, such as shareholders, employees, creditors, customers, suppliers or external concerned regulatory bodies.

9. Abbreviations:

CBJ	Central Bank of Jordan
FFIEC	The Federal Financial Institutions Examination Council
CoBIT5	The Control Objectives for Information Technology
O&T	Operations and Technology
CIOC	Chief Information Officer Council
KRI	Key Risk Indicators
BoD	Board of Directors
CCO	Citi Country Officer
CCC	COUNTRY COORDINATING COMMITTEE
BRCC	Business Risk and Controls Committee (BRCC)
VOE	Voice of the Employee
ORM	Operational Risk Management
MCA	Manager's Control Assessment
KOR	Key Operational Risks
AMA	Advanced Measurement Approaches
ICFR	Internal Control over Financial Reporting