(Translation from Arabic into English)

A Guide to Institutional Governance and Management of Information and Communication Technology (ICT) in the Banking Sector

National Bank of Iraq

Reviews

Event	Date	Accreditation Party	Version Number
Publication	9 Jan 2020	ScanWave C.T.S.	1.0
Review	9 June 2022	ScanWave C.T.S.	1.0

This guide was developed based on the instructions of the Central Bank of Iraq No. 14/611 in 25/4/2019 and the COBIT 2019 framework issued by Information Systems Audit and Control Association (ISACA).

Contents

1. Introduction

The National Bank of Iraq, represented by the Board of Directors and its executive management, realizes the importance of information and communication technology, like the rest of the banking units operating in the bank. Where the bank, represented by the Board of Directors, its executive management, and all business units, whether banking and information and communication technology units, worked to cooperate and work together to include information and communication technology under the umbrella of governance and its administrative style.

In response to the instructions of the Central Bank of Iraq No. 14/611 on 25/4/2019, the Bank took the initiative to adopt the COBIT 2019 framework for the governance and management of information and associated technology in compliance with the instructions issued in this regard.

COBIT 2019 provides a comprehensive framework that helps the bank achieve its objectives related to the governance and management of information and communication technology at the level of the entire bank. As this framework helps the bank to reach the highest levels of benefit from information technology
By maintaining a balance between the highest benefit of information and communication technology and the least risks and resources.

The COBIT framework enables the bank to fully implement the governance and management of all business units, in other words, covering all business, ICT functions and responsibilities in the bank.

2. An overview of the National Bank of Iraq

Since its establishment as a public shareholding company within the private sector in 1995, the National Bank of Iraq has been diligent to provide a full range of banking services to companies and individuals in Iraq. In view of the success of the bank and to support its future growth, the bank’s capital was increased from 400 million Iraqi dinars at inception to 250 billion Iraqi dinars (215 million US dollars) in December 2013.

In 2005, Capital Bank (Jordan) purchased a majority shares of the National Bank of Iraq (68%), which enabled the National Bank of Iraq to develop its products and services, enhance its foothold internationally and enhance financial inclusion at the country level.

By virtue of its extensive network of correspondent banks, Capital Bank represents the National Bank of Iraq's gateway to the global economies, facilitating sending and receiving internal and external remittances, granting credit facilities, and providing trade finance services.

In addition to the above, the National Bank of Iraq can trade for the benefit of its clients in the Jordanian market and in international markets through Capital Investments, the investment arm of Capital Bank - in addition to providing trading services in the Iraq Stock Exchange through its wholly owned subsidiary, the Iraqi Money Company.

Scope and Mechanism of Application and Related parties

This guide applies to all operations of the National Bank of Iraq that depend on information and communication technology in all departments and branches of the bank. All related parties must take into account compliance with this guide, each according to his job title and position.

This guide also applies when signing attribution agreements with third parties to provide human resources, services, programs and information technology infrastructure in order to run the bank's operations, services, programs and infrastructure provided before and during the contracting period, and in a manner that does not relieve the Board and the senior executive management of the final responsibility for fulfilling the instructions requirements.

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

- The chairperson, board members and external experts hired to take charge of the overall direction of the project/program, approve tasks and responsibilities within the project, and support and provide the necessary funding
- The Managing Director, his deputies, his assistants, operations and branch managers assume the responsibilities of naming the appropriate persons with experience in the Bank's operations to represent them in the project and describing their duties and responsibilities.
- The IT Director and the steering committees and project managers assume the responsibilities of managing the project or program, directing and supervising it directly, recommending the provision of the necessary resources to complete it, and ensuring the correct understanding by all parties of the requirements and objectives of the instructions.
- Internal Audit: assume its responsibilities entrusted to it under the instructions directly, and participate in the project/program, which represents the role of the internal audit in operational matters as an independent consultant and observer to facilitate and succeed in completing the project/program.
- Risk, Information Security, Compliance and Legal Departments: Take over the responsibilities of participating in the project and program, representing the role of those departments, and ensuring that the project/program is represented by all concerned parties.
- Specialists and holders of technical and professional certificates related to the framework (COBIT Assessor, Implementation COBIT Foundation, CGEIT, who are hired from inside and outside the bank, to assume the role of guide to spread knowledge of the framework and facilitate the application process.

3. Objectives of ICT Governance Controls in the Iraqi Banking Sector

The National Bank of Iraq set the following objectives for the governance and management of information and technology framework accompanying it:

3.1. To meet the needs of related parties and achieving the bank's objectives through the use of a well-established governance framework that ensures:

- Prudent management of ICT resources and projects to benefit from those resources and reduce waste.
- Providing high quality information as a basis that supports decision-making mechanisms in the bank.
- Ensuring the provision of technological infrastructure that enables the Bank to achieve its objectives.
- Ensuring raising the level of banking operations through the use and employment of effective and reliable technological systems and that they are selected to achieve the desired objectives.

- Ensuring that ICT risks are strictly managed to ensure the necessary protection of the Bank's assets.
- Providing assistance in achieving compliance with the requirements of laws, legislation and controls, as well as compliance with internal work strategy, policies and procedures.
- Improving the internal control system.
- Maximizing the level of satisfaction with information and communication technology by its users by meeting business needs efficiently and effectively.
- Managing the services of customers and third parties entrusted with the implementation of operations and tasks of services and products related to information and communication technology.

3-2 Separate the board of directors from the executive management in accordance with the best internationally recognized standards and practices for the governance and management of information and associated technology.

3-4 Adopting practices and rules of work and organization according to the best international standards as a starting point to build upon in the areas of governance and management of IT operations, projects and resources.

Enhancing self-monitoring mechanisms, independent oversight, and compliance examination in the areas of governance and management of information and associated technology, in a way that contributes to the continuous improvement and development of performance.

4. Public Policies

4-1. This guide is based on the instructions of the Central Bank of Iraq No. 14/611 on 4/25/2019, and this guide should be reviewed and updated regularly and in line with the updates that occur to the bank.

4-2. The guide is approved by the Board of Directors. The Bank, through the Information and Communication Technology Governance Committee emanating from the Board of Directors, reviews this guide and updates it when necessary. This guide expresses the bank's view of the governance and management of information and associated technology in terms of its concept, importance and principles.
the basic.

4-3. The bank shall publish this guide in any appropriate way for the public to see, and the bank shall disclose in its annual report that there is a special guide for the governance and management of information and the accompanying technology or that includes its institutional governance guide, and it also discloses information of interest to related parties, including the guide, and the extent of its commitment to apply its contents.

4-4. Committees

- **IT Governance Committee:**
  - In line with the instructions of the Central Bank of Iraq, the Board of Directors has formed a committee of the members of the Board of Directors concerned with the governance of information and communication technology.

- The committee may seek assistance, when necessary, and at the expense of the bank, from external experts, in coordination with the chairman of the board, in order to compensate for the shortfall in this field on the one hand, and to enhance the objective opinion on the other hand. And the committee has the right to invite any of the bank's administrators to attend it meetings to take their opinion, including those concerned with the internal audit and members of the senior executive management, such as the Director of Information Technology and Communications or those concerned with the external audit, and the board determines its objectives and delegates powers to it by it, in accordance with a charter that clarifies this, and that it submits periodic reports to the board, noting that delegating the board's powers to the committee or any other committee does not absolve it as a whole from bearing its responsibilities in this particular.

- This committee meets at least quarterly, and the records and minutes of the meeting are kept and duly documented. It undertakes the following tasks:

1- Adopting strategic plans for information and communication technology and appropriate organizational structures, including steering committees at the level of senior executive management, in particular the steering committee for information and communication technology, in a manner that ensures the achievement and fulfillment of the strategic objectives of the bank and achieving the best added value from projects and investments of information and communication technology resources and the use of tools And the necessary standards to monitor and ensure the extent to which this is achieved, such as the use of IT Balanced Scorecards, calculating the rate of return on investment (ROI) and measuring the impact of contributing to increasing financial and operational efficiency.

2- Adopting the general framework for managing, controlling and monitoring information and communication technology resources and projects in a manner that simulates the accepted international best practices in this regard, specifically COBIT in all its versions to achieve the objectives and requirements of these controls by achieving the institutional objectives mentioned in Attachment No. (1) in a sustainable manner, and achieving a matrix of objectives The information and technology associated with it, contained in Attachment No. (2), and covers information and communication technology governance processes contained in Attachment No. (3).

3- Adopting the importance and prioritization of the organization objectives (Organization Objectives) contained in Attachment No. (1), and the objectives of information and related technology contained in Attachment No. (22), and considering their data as a minimum, and describing the sub-objectives necessary to achieve them.

4- Adopting a matrix of RACI CHART responsibilities towards the main operations of the governance of information and communication technology in Attachment No. (3), and the sub-processes emanating from it in terms of the entity, entities, person, or parties that are initially responsible (Responsible), those responsible finally (Accountable) and the consulting parties (Consultant) and those that are informed about all operations (Informed) in the facility mentioned in this regard.

5- Ensuring the existence of a general framework for information and communication technology risk management that is compatible with the overall framework for risk management in the bank and integrates with it in accordance with international standards such as (ISO 31000, ISO73) that takes into account and meets all information and communication technology governance processes.

6- Approving the budget for information and communications technology resources and projects in line with the strategic objectives of the bank.

7- General supervision and review of the progress of information and communication technology operations, resources and projects to ensure their adequacy and effective contribution to achieving the requirements and business of the bank.

8- Viewing audit reports for information and communication technology, take the necessary measures to address deviations, and make recommendations to take the necessary measures to correct any deviations.

- **Information Technology Steering Committee:**
  The senior executive management formed this committee in order to ensure the application of the strategic alignment between the objectives of information and communication technology to achieve the strategic objectives of the bank in a sustainable manner. Accordingly, a committee called the Information and Communication Technology Steering Committee was formed, headed by the Managing Director and with the membership of the directors of the senior executive management, including the Director of Information Technology and Communications and the Director of Risk management and information security manager, and the board elects one of its members to be an observer member in this committee in addition to the director of internal auditing, and it can invite others when needed to attend its meetings.

This committee meets at least quarterly, and in particular undertakes the following tasks:

1- Preparing strategic and operational plans for managing risks that ensure reaching the strategic objectives set by the Board and supervising their implementation to ensure their achievement and continuously monitoring the internal and external factors affecting them.

2- Linking the matrix of institutional objectives with the matrix of relevant information and technology objectives, as contained in Attachment No. (2), and adopting and reviewing them on an ongoing basis, in a way that ensures the achievement of the strategic objectives of the institution and the objectives of controls, taking into account the definition and review of a set of measurement standards and assigning those concerned of the executive management to monitor them continuously and acquaint the committee with them.

3- Recommending the allocation of financial and non-financial resources necessary to achieve the objectives and ICT governance processes contained in Attachment No. (2) and (3), respectively, as a minimum, using the appropriate human element through organizational structures that include all the processes necessary to support the objectives, taking into account the separation of tasks and non-conflict. interests, adapting the technical infrastructure and other services related to it to serve the objectives, and supervise the progress of the implementation of projects and operations of information and communications technology governance.

4- Arranging information and communication technology projects and programs according to priority.

5- Monitoring the level of technical and technical services and working to raise their efficiency and improve them continuously.

6- Submit the necessary recommendations to the ICT Governance Committee regarding the following matters:

- Allocating the necessary resources and mechanisms to achieve tasks for Information technology governance.
- Any deviations that may negatively affect the achievement of strategic objectives.
- Any unacceptable risks related to technology, security and information protection.

- Performance reports and compliance with the requirements of the general framework for managing, controlling and controlling resources and information and communication technology projects.

7- Providing the Information and Communications Technology Governance Committee with the minutes of its meetings on an up-to-date basis, and obtaining information useful for seeing them.

5.4. Policy Regulation:

- The Board or whomever it delegates from its committees must adopt the set of principles, policies and frameworks necessary to achieve the general framework for managing, controlling and monitoring information and communication technology resources and projects, in a way that meets the requirements of the objectives and processes of information and communication technology governance contained in Appendices No. (2) and (3), respectively.
- The Board or its delegated committees shall approve the principles, policies and frameworks, particularly those related to information and communication technology risk management, information security management and human resources management, which meet the requirements of information and communication technology governance operations contained in Attachment No. (3).
- The Board or whoever is delegated from its committees must adopt the set of policies necessary to manage the resources and processes of information and communication technology governance contained in Attachment No. (6), and consider this set of policies as a minimum with the possibility of merging those policies as required by the nature of the work, provided that other policies are developed to keep pace with the development Bank objectives and mechanisms the work.

6.4. Information, Data and Reports

- The board of directors and senior executive management ensure the development of the necessary infrastructure and systems to provide information and reports to its users with the aim of contributing to sound decision-making in the bank.
- The board of directors or the authorized bodies adopt the information systems and reports contained in Attachment No. (7). These systems are considered the minimum, and it determines the owners of these information and reports through which the review and use authority is determined and delegated according to the need for work.
- The Bank's policies and reports are reviewed and updated regularly to best reflect the Bank's objectives and operations practices and standards.

7.4. Organizational Structure:

- The Board shall approve organizational structures (hierarchies and committees, particularly those related to the management of information and communication technology resources, operations and projects, information security management and human resource management, which meet the requirements of information and communication technology governance operations and achieve the bank’s objectives efficiently and effectively.

- Ensuring the separation of tasks that are conflicting in nature and the requirements of regulatory protection related to bilateral control as a minimum, and adequacy and updating the job description when approving and amending the organizational structures of the bank.

8.4. Services and ICT Infrastructure:

- The Board or whomever it delegates from its committees and the senior executive management must approve the system of services, programs and infrastructure of information and communication technology contained in Attachment No. (8), and consider that system as a minimum, provided that it is provided and developed continuously to keep pace with the development of the organization’s objectives and operations, and in accordance with international best practices. accepted in this regard.

- The Board or whomever it delegates from its committees and the senior executive management must approve the system of services, programs and infrastructure for information and communication technology that support and assist in achieving information and communication technology governance operations, and then the objectives of information and associated technology, and the institutional objectives.

9.4. Knowledge, Skills, and Experience:

- The Board or its delegated committees shall approve the qualifications matrix (HC Competences) and human resources management policies necessary to achieve the requirements of information and communication technology governance operations mentioned in Attachment No. (3), and the requirements of these controls in general, and place the right person in the right place.

- The management of the disbursed must employ qualified and trained human resources from among the persons with experience in the fields of information and communication technology resource management, risk management, information security management and information and communication technology audit management, based on standards of academic and professional knowledge and practical experience recognized by qualified international associations according to international accreditation standards for institutions that grant professional certificates each According to his specialization, provided that the currently employed cadres are rehabilitated and trained to meet the requirements of this guide.

- The executive management of the bank shall continue to provide its employees with training and continuing education programs to maintain a level of knowledge and skills that meet and achieve the information and communication technology governance processes contained in Attachment No. (3).

- The executive management of the bank should include mechanisms for the annual evaluation of cadres with objective measurement criteria that take into account the contribution through the job position to the achievement of the bank's objectives.

10.4. Internal and external audit

- The Board shall allocate adequate budgets and allocate the necessary tools and resources, including the qualified human element, through departments specialized in auditing information and communication technology, and ensure that both the internal audit department in the bank and the external auditor are able to review and audit the recruitment and management of resources and projects of information and communication technology and operations the bank is based on it through qualified and internationally accredited professional cadres in this field, holding valid professional accreditation certificates such as CISA.

- On the one hand, the Board Audit Committee, and the external auditor. On the other hand, must provide the Central Bank of Iraq with an annual report for internal auditing and another for external auditing, respectively, that includes the response of the executive management and the briefing and recommendations of the Board regarding it, according to what is stated in Clause (D/2) of this article and according to the audit report form (risks - controls of information and related technology The relevant report is in Attachment No. (4), during the first quarter of each year, and these reports replace their counterparts or those that include them from the reports required under previous controls.
- The audit committee must include the responsibilities, powers, and scope of work for auditing information and communications technology within the audit charter on the one hand, and within procedures agreed upon with the external auditor on the one hand.
- other. The board shall ensure, through its audit committee, that the internal auditor and the external auditor of the bank, when carrying out the specialized auditing of information and the accompanying technology, adhere to the following:

1- Information and communication technology audit standards according to the latest update of the international standard ITAF issued by the Audit and Oversight Association ISACA, including:

- Implementation of audit missions within an approved plan in this regard that takes into account the relative importance of operations, the level of risks, and the degree of impact on the objectives and interests of the bank.
- Providing and adhering to plans for training and continuing education by specialized staff in this regard.
- Commitment to standards of professional and administrative independence and ensuring non-conflict of interests.
- Adhering to the standards of objectivity, exerting professional care, and continuously maintaining the level of competitiveness and professionalism of the knowledge and skills that must be enjoyed, and deep knowledge of the various mechanisms and operations of the institution based on information and communication technology, and other audit reports.

2- Examining, evaluating and reviewing the processes of employing and managing information and communication technology resources, the bank's operations based on them, and giving a general opinion regarding the level of risks of the entire information and associated technologies within an audit program.

3- Regular procedures for following up on the results of the audit to ensure that the observations and deficiencies contained in the auditor's reports are addressed in a timely manner. And work to gradually raise the level of importance and risks in the event of non-response, and put the Council in a manner in this whenever necessary.

4- Including annual evaluation mechanisms for information and communication technology investigation cadres with objective measurement criteria, provided that the evaluation processes are carried out by the board represented by the Audit Committee emanating from it and according to the organizational administrative hierarchy of the audit departments, or whoever replaces them in foreign banks.

It is possible to assign the role of the internal auditor of the information and its accompanying technologies to a specialized external party that is completely independent of the external auditor accredited in this regard, provided that all the requirements of these instructions and any other related instructions are met and that the Audit Committee emanating from the Board and the Board itself maintain their role with regard to examining compliance and ensuring that these requirements are met at least.

5. Set Objectives and follow them

Each organization operates in a different context and this context is determined by both external and internal factors. External factors include the general policies of the state, laws, geographical distribution, external threats and risks, etc.; As for the internal factors, they include culture, organization, susceptibility to risk...etc. This institutional context requires a commensurate governance and management system.

Related parties' needs must be transformed into an implementable institutional strategy. COBIT's integrated objectives constitute a mechanism for translating stakeholder needs into feasible, actionable institutional objectives that are customized as required, and alignment objectives are derived from them. This translation allows setting specific objectives at every level and in every area of the organization to support the overall objectives and stakeholder requirements, thus harmonizing the bank's needs with IT solutions and services and effectively supporting them.

The Bank has adopted the COBIT mechanism for successive objectives to translate stakeholder needs into specific and implementable objectives. This translation allows setting specific objectives at each level and in each area of the bank to support the general objectives and requirements of related parties and thus effectively supports the alignment between the bank's needs and ICT solutions and services.

Appendix A: Policy Framework (minimum)

* The list below is based on the instructions of the Central Bank of Iraq contained in Attachment No. (6)

The Bank adopts the following list of minimum policies to organize and manage operations in the Bank:

- Governance of information and communication technology regulation
- Information security and protection
- Payment card data security and protection
- Business continuity plans and disaster recovery plans
- ICT risk management
- IT Compliance
- Data Privacy
- Outsourcing
- Project Portfolio Management
- Asset Management
- Acceptable use of information and communication technology resources
- Change Management
- peripheral computers
- portable devices
- User Access Management
- System Development Lifecycle
- Service Level Management
- Backup and Restore
- Retention
- Purchasing systems and equipment
- Remote Access
- Networks
- Wireless Networks
- Firewalls
- Penetration Testing and Vulnerability Assessment
- Public Branch Exchange
- Private Branch Exchange

Appendix B Minimum Reports and Information

* The list below is based on the instructions of the Central Bank of Iraq contained in Attachment No. (7)

The Bank will adopt the list of minimum reports given below to ensure that proper reports are maintained in the Bank, and the reports serve as an anchor for the decision-making processes.

- Matrix of powers and privileges
- Analysis of information and communication technology risk factors
- Scenario analysis of information and communication technology risks
- Information and communication technology risk register
- Table of responsibilities for each service provided RACI Chart
- Information and communication technology risk profile
- Information and communication technology risk report
- ICT risk map
- Risk Universe, Appetite and Tolerance
- Key risk indicators
- Risk Taxonomy
- Risk and Control Activity Matrix (RCAM)
- Balancing information security and protection
- MIS Report
- ICT audit strategy or methodology
- audit charter
- Information and communication technology audit plan
- Qualifications Matrix
- ICT audit log
- ICT audit file
- The best international standards for managing information and communication technology resources and projects, information and communication technology risk management, security, protection and auditing of information and communication technology.

Appendix C: Services, Software, and IT Infrastructure

* The list below is based on the instructions of the Central Bank of Iraq contained in Attachment No. (8)

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

- Incident Management Services
- Inventory of ICT assets
- Raising awareness of good information security practices
- Logical Security and protection of data and information
- Control of information security
- ICT auditing software
- Hosting and physical and environmental security controls for the main server rooms, communication and electricity supply rooms
- International standards and specifications adopted in the establishment of data centers

Definitions

- **Governance:** Governance ensures that the needs, conditions and options of related parties are assessed in order to define balanced and agreed organization-wide objectives that are achieved; defining institutional directions through setting priorities and making decisions; Monitor performance and compliance towards agreed targets.
- **COBIT:** formerly known as Information Control Objectives and Related Technology; It is now used only now as a noun only. It is a complete, internationally accepted framework for the governance and management of organization information and technology that supports organization executives and management in defining and achieving business objectives and related compliance objectives. COBIT supports organizations in developing, implementing, improving and monitoring good governance and management practices related to ICT.
- **Technology and Information Governance in the Organization:** A vision for governance that ensures information and related technology support and contributes to achieving the organization's objectives.
- **Board of Directors**: The Board of Directors of the Bank.
- **Senior Executive Management**: includes the General Manager of the Bank or the Regional Director, the Deputy General Manager or the Deputy Regional Director, the Assistant General Manager or the Assistant Regional Director, the Financial Director, the Director of Operations, the Director of Risk Management, the Head of Treasury (Investment), the Compliance Manager, as well as any employee of the Bank who enjoys With an executive authority parallel to any of the above-mentioned authorities, and functionally and directly related to the General Manager.
- **Related parties**: Any interested party in the Bank, such as shareholders, employees, creditors, customers, suppliers or relevant external regulatory bodies.