Governance Guide to Information Technology (IT)

Introduction:

Information technology plays a pivotal role in modern business enterprises, especially with the tremendous and accelerated technological progress, given the complexity of the business environment and the intensification of competition between business enterprises by constantly striving to provide the best services and products to customers at the lowest costs and in a safe, low risk environment. This made information technology have an important competitive impact on business enterprises.

Accordingly, the best practices of the IT governance and the management of its operations and resources efficiently and effectively had to be adopted and under prudent risk management, hence appeared the application of international practices in this field, which led to the issuance of the instructions of the Central Bank of Jordan No. 65 / 2016 on 25/10/2016 in the field of governance and management of information and associated technology.

The overall framework of governance and management of information and associated technology consists of a set of basic foundations and principles as follows:

First: Strategic Alignment required to be achieved through the strategic goals of information technology, which should lead to achieving the strategic objectives of the institution, and thus directing the information technology strategically and aligning information technology with business in terms of services and projects.

Second: Added Value: The institution should employ its IT resources within the available options through which it maximizes the Added Value measured mainly against the IT contribution to the achievement of the strategic objectives of the institution, to ensure that:

• The organization of information technology works to maximize the resources and targets of information technology.
• Evaluate return on investment (ROI) of using IT in business.

Third: Risk Management

By working on:

• Managing information technology risks in an integrated manner that complies with the overall risk management processes of the institution.
• Ensuring that operations have been developed to ensure risk.
Governance Guide to Information Technology (IT)
• Evaluating the various fields of the risks of IT investments.

• Monitoring whether risks are identified, managing and measuring cost, utilizing investments and managing risks according to sound procedures and practices that lead to sound risk-based decision-making mechanisms, and ensure the achievement of the value added at lowest costs, while mitigating expected losses and risks in a manner that reflects on the vision of the Bank in this regard, and within the acceptable limits of risks wherever possible.

Fourth: Resource Management:
• Providing guidance (at the highest administrative level) for the processes of obtaining and utilizing IT resources.

• Supervising the institution-wide IT financing process.

• Ensuring that IT resources and infrastructure are provided to support current and future business requirements.

Fifth: Performance Measurement:
• Ensuring that information technology is achieving its strategic objectives.

• Evaluation of the measurement of the performance of information technology and its contribution to business (the value added to business).

Building on the above mentioned, the top management (the board and the senior executive management) must undertake the planning and institutionalization processes by drawing up strategies, policies and action plans, and build and implement hierarchical and cyclical organizational structures (i.e., in the form of committees), in a way that leads to the achievement of the strategic objectives, building mechanisms, tools and standards needed to measure the value added of information technology, and in a way that enables the Board and senior executive management to monitor the institution’s processes to ensure the proper planning, organization, and employment of IT resources for the purpose of obtaining feedback for the continuous improvement and development, all within the foundation of the principle of separation of tasks and roles and the proper distribution of them between the Board on one hand and the Executive management on the other hand.

With regard to the best IT governance practices, it is essential to have a joint work between entities responsible for IT and business stakeholders in the institution to determine and
Governance Guide to Information Technology (IT) control information technology requirements, with the necessity to develop a control and monitoring model applicable to all units in the institution.

Hence the importance of a common and precise vision for IT governance, with the necessity of understanding and the approval of all stakeholders of the scope of IT governance.

Therefore, this guide comes as an organizing framework for the control and management of Information Technology at Societe Generale Bank of Jordan SGBJ and the Bank's information technology operations, in line with the Bank's efforts in managing all its operations and activities efficiently and effectively and within the prudent management of all types of related risks.
Governance Guide to Information Technology (IT)

Article (1): References

In preparing this guide, the Bank has relied on the following sources:

- Governance Instructions and Information and Technology Management associated thereto No. 65/2016 issued by the Central Bank of Jordan, and any subsequent amendments.


- Governance policies and strategies followed at the SGBG level in Lebanon and France.

- General framework for COBIT instructions
  (Control Objectives for Information and Related Technologies)

This guide shall be called “Governance Guide to Information Technology of Societe Generale Bank - Jordan” and shall be effective as of the date of its adoption by the Board of Directors. Any future amendments thereto shall be approved by the Board.

Article (2): Definitions

The terms and phrases included in this guide shall have the meanings assigned thereto hereunder unless the context indicates otherwise:

1. Governance of Information Technology: The distribution of roles and responsibilities, and the identification of relationships between the various parties, entities and stakeholders (such as the Board and the executive management) for the aim of maximizing the value added of the Bank by following the optimal approach that ensures the balance between risks and expected returns, Through the adoption of rules, foundations and mechanisms for decision-making and determining the strategic directions and objectives in the bank and mechanisms to control and check compliance with the extent to achieve the sustainability and development of the bank.

2. Information Technology Management: The group of continuous activities that are under the responsibility of the executive management of the Bank. It includes planning to achieve the strategic objectives including coordination and organization, construction and development activities including procurement and implementation, operating activities including delivery of services and support, and monitoring activities including measurement and evaluation, and ensuring the sustainability of the Bank's objectives and strategic directions.

3. IT Governance operations: A set of Bank policy practices and activities needed to achieve IT objectives.
Governance Guide to Information Technology (IT)

4. IT objectives: A set of key and subsidiary objectives related to the governance and management activities of IT that are necessary to achieve institutional objectives.

5. Institutional Objectives: A set of institutional governance objectives necessary to meet the needs of stakeholders and the objectives of these instructions.

6. Stakeholders: Anybody who has interest in the Bank such as depositors, shareholders, employees, creditors, customers, suppliers or regulatory authorities concerned.


8. Senior Executive Management: includes the General Manager, the Deputy General Manager, the Financial Officer, the Operations Manager, the Risk Manager, the Internal Audit Manager and the Compliance Manager, as well as any officer in the Bank who has executive authority parallel to any of the above mentioned authorities and is directly related to the General Manager.

Article (3): Parties of Information Technology governance

• Board of Directors.
• Senior Executive Management.
• Information Technology Department.
• Security Unit.
• Risk department
• Internal and external audit.
• Bank partners and suppliers in the field of IT.
• The regulatory authorities concerned.
• Customers and shareholders.
• Other stakeholders.
Article (4): IT Governance Objectives

The application of information technology governance is aimed at:

a. Meeting Stakeholders’ Needs and achieving the bank's goals and objectives through achieving IT objectives, ensuring:

1. Providing high-quality information as a pillar that supports the decision-making mechanisms in the Bank.

2. Prudent management of IT resources and projects, maximizing the utilization of these resources and reducing their waste.

3. Providing a special and supporting technological infrastructure that enables the Bank to achieve its objectives.

4. Upgrading the Bank's various operations by employing an efficient and reliable technological system.

5. Prudent risk management of information technology that ensures the necessary protection of the assets of the bank.

6. Assisting in achieving compliance with the requirements of laws, legislations and instructions in addition to complying with internal business strategy, policies and procedures.

7. Improving internal control and monitoring system.

8. Maximizing the level of satisfaction with information technology by its users to meet the needs of the work efficiently and effectively.

9. Management of the services of the external parties entrusted with the implementation of operations, functions, services and products.

B. Achieving inclusiveness in governance and management of information technology in terms of taking into account not only the technology itself but also the provision of seven enablers that are accompanying and complementing IT services, which are:

1. Principles, policies and frameworks

2. IT governance processes

3. Organizational structures

4. Information and reports

5. IT services, software and infrastructure
Governance Guide to Information Technology (IT)

6. Knowledge, skills and experience,

7. System of values, ethics and behaviors,

And the necessity to provide them with specific specifications and dimensions to achieve and serve the requirements and objectives of information and technology associated with it not only in IT operations, but in all operations of the Bank based on information and technology.

C. Adopting business practices and rules and organizing them according to the best international standards as a starting point to be built upon in the areas of governance and management of IT processes, projects and resources.

D. Separating the processes, functions and responsibilities of the Board of governance from those falling within the limits of the responsibility of the executive management regarding information technology.

E. Strengthen self-monitoring and independent control mechanisms, and examine the compliance in governance and management of IT, contributing to continuous improvement and development of performance.
Article (5): Principles of IT Governance

- Increasing the effectiveness of IT management.
- Involving executive management and the Board of directors in IT management.
- Providing appropriate motivations.
- Identification and assignment of responsibilities

Article 6: Scope and mechanism of application

First: The scope of IT governance applies to all the Bank's IT-based operations, and all parties are stakeholders concerned with the application of IT governance.

Second: The instructions of this guide shall be applied in full compliance with the instructions of the Central Bank of Jordan in the field of governance and management of information and technology objectives. The instructions of the Société Générale Group may apply in this area, provided that they do not conflict with the instructions of the Central Bank of Jordan.

Third: The necessity to adapt the following to meet the requirements of IT governance:

1. Principles, policies and frameworks.
2. Organizational structures.
3. Information and reports.
4. IT services, software and infrastructure.
5. Knowledge, skills and experiences.
6. System of values, ethics and behaviors.
7. IT operations.

Fourth: When signing outsourcing agreements with others to provide human resources, services, software and infrastructure for information technology to manage the operations of the bank, it is necessary to ensure that the compliance of others of the provisions of the instructions of IT governance is applied in whole or in part to the extent that it is appropriate to the importance and nature of the Bank's operations, and the services, software and infrastructure provided before and during the contracting period, so as not to exempt the Board and the executive management from ultimate responsibility to meet the requirements of the instructions, including the requirements of auditing.

Article (7): Compliance with information technology governance
Governance Guide to Information Technology (IT)
This guide was adopted by the Board of Directors based on the recommendations of the Information Technology Governance Committee of the Board.

The Information Technology Governance Committee of the Board of Directors directs the preparation, revision and updating of the guide in light of the internal and external developments, reflecting the recent developments in this regard. The Committee shall also ensure the application of all in of this Guide and inform the Board of the results of this evaluation and its recommendations to rectify the positions.

The Bank publishes the Guide on its website in its annual report, in which the Bank's compliance with all provisions of the guide and other information of interest to stakeholders is disclosed. Any copy of this guide shall be provided to any shareholder upon request.

Article (8): Committees

• Information Technology Governance Committee

The Board shall form an Information Technology Governance Committee from among its members. This committee shall consist of at least three members. It shall preferably include persons with expertise or strategic knowledge in information technology. The Committee may, if necessary, at the expense of the Bank, appoint external experts coordinating with the Head of the Board to compensate shortage in this field, and to strengthen the objective opinion on other hand. The committee may invite any of the bank's managers to attend its meetings to use their opinion, including those involved in internal audit and members of the senior executive management (such as, IT Manager) or those concerned with auditing. The Board shall determine its objectives and delegate its powers in accordance with a Charter declares that, and shall submit periodic reports to the Board. The delegation of the Board shall have the powers of the Committee or any other committee which shall not relieve it as a whole of its responsibilities in this regard. The Committee shall meet quarterly at least, and shall maintain minutes of documented meetings and undertake the following tasks:

1. Adopting strategic information technology objectives and appropriate organizational structures, including Steering Committees at the senior executive management level, in particular (the Information Technology Steering Committee), ensuring that the Bank's strategic objectives are met and the best value added of IT resources projects and investments is achieved; and the use of tools and standards needed to monitor and ensure achieving that, such as the use of the IT Balanced Scorecard system and the calculation of return on investment (ROI), and measuring the impact of the contribution to increase Financial and operational efficiency.

2. Adopting the general framework for the management, control and monitoring of IT resources and projects that complies with internationally accepted best practices in this regard, specifically (COBIT)

(Control Objectives for Information and Related Technology), that meets the objectives and requirements of IT governance through achieving organizational objectives in a sustainable
Governance Guide to Information Technology (IT) manner, achieving the IT objectives matrix, and covering information technology governance processes.

3. Adopting the matrix of institutional objectives, information and technology objectives and considering their data as a minimum, and describing the sub-goals necessary to achieve them.

4. Adopting a (RACI Chart) towards the key Processes of IT governance and its sub-Processes in terms of: the entity, entities, persons, or responsible parties, and those who are finally responsible (Accountable), (Consulted), and (Informed) towards all operations guided by the standard (COBIT 5 Enabling Processes) in this regard.

5. Ensure that there is a general framework for IT risk management that complies with and complement with the overall risk management framework of the Bank and takes into consideration all IT governance processes.

6. Adoption of resources and projects budget of information technology in line with the strategic objectives of the bank.

7. General supervision and access to the processes, resources and projects of information technology to ensure their adequacy and effective contribution to the achievement of the bank’s requirements and processes.

8. Viewing the reports of IT auditing, and take the necessary procedures to deal with deviations.

9. Providing recommendation to the Board to take the procedures needed to correct any deviations.

- IT Steering Committee:

The senior executive management shall compose the steering committees needed to ensure IT strategic compatibility to achieve sustainably the Bank’s strategic objectives, therefore a committee named (IT steering committee) is composed, headed by the general manager and the members of the senior executive management including the IT Manager, the Risk Management Manager and the Information Security Manager. The Board elects one of its members to be an observer member of this committee in addition to the Internal Audit Manager. The Committee may invite others when needed to attend its meetings, and it shall document its meetings with fundamental records, provided that the periodicity of the meetings shall be at least once every three months. In particular, the Committee shall undertake the following tasks:

1. Developing annual plans to achieve the strategic objectives approved by the Board, and supervise their the implementation to ensure their achievement, and control of internal and external factors affecting them continuously.

2. Linking the matrix of institutional objectives to the matrix of information and technology
Governance Guide to Information Technology (IT) objectives and adopting and reviewing them continuously to ensure the achievement of the strategic objectives of the bank and the objectives of IT governance instructions, taking into consideration the definition of a set of standards for measuring and reviewing them, and assigning the concerned executive management to monitor them continuously and inform the committee.

3. Recommending the allocation of financial and non-financial resources necessary to achieve the objectives and IT governance processes at a minimum, and to use the efficient and appropriate human element in the right place through organizational structures that include all the processes necessary to support the objectives, taking into account separation of functions and non-conflict of interest; and the adaptation of technological infrastructure and related services, serving the objectives, and supervising on the implementation of IT governance projects and processes.

4. Arranging IT projects and programs by priority.

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

6. Making recommendations to the Information Technology Committee on the following matters:

   A. Allocating the necessary resources and mechanisms to achieve the tasks of the IT Committee.
   B. Any deviations that may negatively affect the achievement of strategic objectives.
   C. Any unacceptable risks related to the technology, security and protection of information.
   D. Performance reports and compliance with the requirements of the general framework for the management, control and monitoring of IT resources and projects.

7. Providing the Information Technology Committee instantly with minutes of its meetings and receive access to information.

Article (9): Internal and external auditing

a. The Board should allocate adequate budgets and allocate the necessary tools and resources, including qualified personnel, through specialized IT audit departments, ensuring that both the Bank's Internal Audit Department and the external auditor are able to review and audit the recruitment and manage IT resources and projects, bank's operations on which a specialized audit is based (IT Audit), through specialized and internationally qualified professionals in this field, with valid professional certification such as CISA from qualified international associations under the International Accreditation Standards for Certification Institutions (ISO / IEC 17024) and / or any other parallel standards.

B. The Audit Committee of the Board and the external auditor shall provide the Central Bank of Jordan with an annual internal and external audit report, respectively, containing the response of the executive management and the Board's recommendations and recommendations in this in accordance with a form of an information and technology audit
Governance Guide to Information Technology (IT)
report (Risks- controls), during the first quarter of each year. These reports replace their counterparts or those which are covered by reports required under prior instructions.

C. The Audit Committee shall include the responsibilities, powers and scope of the IT audit within the Audit Charter on one hand and in agreed procedures with the external auditor on the other, in a manner consistent with and covering these instructions.

D. The Internal Auditor and the External Auditor shall comply with the system of ethics and professional practices adopted by the Board, including the minimum professional ethics system contained in ISACA's Information Technology Assurance Framework (ITAF) and its updates.

E. The Board shall ensure, through the audit committee derived therefrom, that the internal auditor and the external auditor of the Bank, in carrying out the specialized audit of the information and technology, shall comply with the following:
1. Information technology audit standards according to the latest update of the International Standard (ISAFA) Information Technology Assurance Framework (ITAF), including:
   I. Implementing audit tasks within an approved plan that takes into account the relative importance of processes, the level of risk and the degree of impact on the Bank's objectives and interests.
   II. Providing and complying with continuous training and education plans by specialized staff in this regard.
   III. Commitment to the standards of professional and administrative independence (Professional and Organizational Independence) and ensuring that current and future interests do not conflict.
   IV. Commitment to objectivity and due professional care, and continuous maintaining of competitiveness and proficiency level of knowledge and skills due, and the deep knowledge of the various mechanisms and processes of the Bank based on information technology, review and audit reports (financial, operational and legal), and the ability to provide a proportionate evidence suitable for the case, and the general sense of disclosure of unacceptable practices and in violation of the provisions of laws, regulations and instructions.

2. Examining, evaluating and reviewing the recruitment and management of information technology resources and the Bank's operations based on them and providing a (Reasonable Overall Audit Assurance) regarding the overall risk level of the information and technology associated thereto in the audit program, with all or part of the audit being repeated at least once a year if the risk is assessed at a level of 5 or 4 according to the risk assessment scale, and once every two years at least if the risk is assessed at (3), and once every three years at least if the risk is assessed at 2 or 1, taking into account the continuous change in the level of risk and taking into account the significant changes in the environment of information and
Governance Guide to Information Technology (IT)
technology associated thereto during the said audit periods, provided that the Central Bank of Jordan shall be provided with audit reports for the first time regardless of the degree of risk assessment, and the evaluation processes should include the Bank's mechanisms followed in terms of strategic planning, the formulation of written and approved policies, principles and procedures, the mechanisms for employing the various resources, including the resources of information technology and the human element, mechanisms and tools of monitoring, improvement and development, and working on documenting and evaluating audit results based on the importance of deviations and weaknesses (notes) in addition to the effective controls and assessing the level of residual and related risks using the methodology standard for analysis and measurement of risks, including corrective actions agreed upon and intended to be followed by the Bank's management on specific dates for correction, with a reference made in a special table to the job title of the person in charge in the Bank who owns each note.

3. Regular procedures to follow up the audit results to ensure that the observations and deviations contained in the auditor's reports are processed on time, and to gradually raise the level of importance and risks in case of non-response, and putting the Board in perspective whenever necessary.

4. Incorporating objective measurement standards into the annual evaluation mechanisms (Performance Evaluation) for the IT audit staff, provided that the evaluation processes should be carried out by the Board, represented by the Audit Committee derived from it, and according to the regulatory administrative structure of the audit departments.

F. The role of an internal auditor for the information and technology can be outsourced (Internal IT audit) to a specialized external entity independent of the external auditor adopted in this regard, provided that all the requirements of these instructions and any other relevant instructions are met and the audit committee of the Board and the Board maintain their role in relation to the compliance examination and ensuring that these requirements are met as a minimum.

Article (10): The functions of the Board and the Senior Executive Management:
- The Board shall be directly responsible for the processes of evaluation, direction and Monitoring (EDM) (Evaluate, Direct, and Monitor).
- The Board and the Risk Management Department shall be directly responsible for the process of "ensuring a prudent risk management of information technology" and "risk management" process.
- The Board or its authorized committees shall adopt the system of principles, policies and frameworks required to achieve the general framework for the management, control and monitoring of IT resources and projects, in accordance with the requirements of the IT governance objectives and processes.
- The Board or its authorized committees shall adopt the principles, policies and
Governance Guide to Information Technology (IT) frameworks, especially those related to IT risk management, Information Security Department, and HR Department, that meet the requirements of IT governance processes.

- The Board or its authorized committees shall adopt the system of policies required to manage IT governance resources and processes, and to consider these policies as a minimum with the possibility of combining and integrating these policies as required by the nature of the work, provided that other policies should be developed in line with the development of the objectives of the Bank and the mechanisms of work, and that each policy shall specify the owner, the scope of application, the cycle of review and updating, the powers of access and distribution, objectives, responsibilities and working procedures, penalties for non-compliance, and compliance checking mechanisms.

- When establishing policies, consideration should be given to the contribution of all internal and external partners and the adoption of international best practices and their updates as references to the formulation of such policies.

- The Board shall adopt the organizational structures (hierarchies and committees), in particular those related to the management of IT resources, processes and projects, information technology risk management, information security management and human resources management that meet the requirements of IT governance processes and achieve the Bank's objectives efficiently and effectively. It is also necessary to ensure that the conflicting functions are separated by their type and the regulatory protection requirements related to the bilateral control as a minimum, and the sufficiency and update of the functional description when adopting and modifying the organizational structure of the Bank.

- The Board and the Senior Executive Management shall develop the infrastructure and information systems necessary to provide information and reports to its users as a basis for the Bank's decision-making processes, hence, the information quality criteria (Integrity Completeness, Accuracy and Validity), and privacy requirements according to the data classification policy and availability requirements, and compliance with such information and reports shall be provided, as well as other requirements of COBIT 5 - Enabling Information: (Objectivity, Believability, Reputation, Relevance, Appropriate Amount, Concise Representation, Consistent Representation, Interpretation, Understandability, Ease of Manipulation, Restricted Access).

- The Board or its authorized committees shall adopt the information and reporting system and consider that system as a minimum, taking into account the identification of owners of such information and reports through which they determine the powers of access and use according to the need for the work and the concerned partners, to be reviewed and developed continuously to keep pace with the development of the objectives and processes of the Bank in accordance with the best international practices accepted in this regard.

- The Board or its authorized committees shall adopt the HR Competencies and Human Resources Management Policies necessary to meet the IT governance requirements and ensure that the right person is put in the right place.
Governance Guide to Information Technology (IT)
- The Bank's management shall employ qualified and trained personnel from persons with expertise in IT resources management, risk management, information security management and IT audit management based on academic, professional and business knowledge standards recognized by qualified international associations under international accreditation standards for certification institutions ISO / IEC 17024) and / or any other parallel standards in accordance with its competence, with the rehabilitation and training of the staff currently employed to meet the above requirements.
- The Bank's Executive Management shall continue to provide its staff with ongoing training and education programs to maintain levels of knowledge and skills that meet and achieve the governance processes of information technology.
- The executive management of the Bank shall incorporate into the performance evaluation mechanisms of the staff the objective measurement criteria that take into account the contribution through the functional position to achieve the objectives of the bank.
- The Board or its authorized committees shall adopt an ethical, institutional and professional system that reflects the accepted international professional codes of conduct in dealing with the information and associated technologies that clearly define desired and undesirable behavioral rules and their consequences.
- The Board and the Senior Executive Management shall employ different mechanisms to encourage the application of desired behaviors and avoid undesirable behaviors through approaches including, but not limited to, incentives and penalties.