Safwa Islamic Bank

Rooted Principles, Innovative Solutions

Guide for Information and Associated Technology Governance and Management

[1] Status: Confidential for the Bank

The documents have been categorized as highly confidential, "the data mentioned in this document is highly confidential to Safwa Islamic Bank. They cannot be duplicated or distributed without Safwa Islamic Bank's authorization.

Guide for Information and Associated Technology Governance and Management

Table of Contents

Introduction

Safwa Islamic Bank (formerly Jordan Dubai Islamic Bank) was established in Amman in the Hashemite Kingdom of Jordan. It was registered as a joint stock company in the company directory on 23/6/1963 under Article 8 by the name of Industrial Development Bank, which was established under Law No. 5 of 1972, which was repealed by virtue of the Industrial Development Bank Repealing Law No. 26 of 2008, and Safwa Islamic Bank has legally taken its place.

In alignment with the directives governing information and technology governance, the Board of Directors and Executive Management of Safwa Islamic Bank have adopted several strategic measures to elevate the Information Technology Department to a level equivalent to other key business divisions within the Bank. Safwa Islamic Bank implements the (COBIT 2019) framework to govern and manage information, technology, and IT-related projects. This framework enables the Bank to optimize the value derived from technology by maintaining a balance between delivering benefits, managing risk, and efficiently utilizing resources. (COBIT 2019) provides a comprehensive structure for overseeing IT projects across their entire lifecycle. It accounts for both functional and technical responsibilities from initiation to completion and considers the interests of both internal and external stakeholders. The Bank is also working to implement an integrated IT risk management framework aligned with its overall enterprise risk management practices. This approach supports sound, risk-based decision-making processes that enhance value creation, reduce costs, and mitigate expected risks and losses, all in accordance with the Bank's vision and within its acceptable risk appetite.

Definitions:

Unless otherwise indicated by the context, the following terms and expressions shall have the meanings assigned to them below wherever they appear in this document:

Term	Definition
Bank	Safwa Islamic Bank.
Board	Safwa Islamic Bank Board of Directors
Committee	Governance and management of information and associated technology.
Organizational Structure	Organizational structure of the Bank.
Senior Executive Management	Includes the Bank General Manager CEO and his deputies, CFO, COO, Head of Credit, Chief of Treasury and Investment, Head of Risk Management, Head of Internal and Sharia Audit, Head of Sharia Compliance, as well as any employee in the Bank.

Stakeholders	Any Bank stakeholders such as shareholders, employees, creditors, customers, external providers, relevant regulatory authorities, or investment account holders.
Guide	A governance and management guide for information and associated technology that provides recommendations and guidance.
Information Governance and Associated Technology	Division of roles and responsibilities and defining relationships between various parties and stakeholders, such as the Board of Directors and executive management, in order to increase the institution's added value and define strategic directions and Bank objectives and mechanisms for monitoring and assessment of compliance with its achievement, which guarantees the sustainability and development of the Bank.
Information Management and Associated Technology	A set of ongoing activities that fall under executive management's responsibilities. They include planning for the purpose of achieving strategic objectives, which include alignment and organization, construction and development activities plus procurement and execution, operational activities such as service delivery and support, and monitoring activities such as measurement and assessment. This guarantees the sustainability of achieving the Bank's objectives and strategic directions.
Information Technology Governance Processes	A set of practices and activities stemming from the institution's policies, necessary to achieve IT governance goals.
Information Objectives and Associated Technology	Group of main and sub-objectives related to information governance and management activities, and associated technology necessary for achieving institutional objectives.

Institutional Objectives	Group of objectives related to institutional governance and management, necessary to meet stakeholder needs and objectives of these instructions.
Auditor	The legal or actual person or entity responsible for assessing the Bank's IT-dependent operations consistent with instructions and requirements approved by the Bank's management in this regard, for no less than 3 consecutive years, and no more than 6 consecutive years.
Cyber Adaptation	The ability of the organization to quickly detect, respond to, and recover from cyberattacks, minimizing business disruption.
Cybersecurity	The ability of the Bank to safeguard confidentiality and availability of its information and information assets in the cyber realm against any cyber threats, by using a group of methods, policies, instructions and best practices in this regard.
On-Site	The operation is located in the Bank's General Administration in Jordan.
Off-Site	The operation is located in a building other than that of the Bank's General Administration in Jordan, yet in the same county.
Near-Site	The operation is located in a governorate other than that of the Bank's General Administration in Jordan.
Off-Shore	Operation is located in a country other than that of the Bank's General Administration.

Scope of Work

The Information Technology Department is the primary authority responsible for this governance guide. Compliance with its implementation is monitored by the Bank's oversight departments. This guide is subject to review as needed.

The scope of this guide covers all operations across Safwa Islamic Bank that utilize information technology, including all departments and branches. All relevant stakeholders are expected to support its implementation, each according to their role and area of responsibility.

General Policies and Guidelines

1. Responsibilities of Key Stakeholders

- Chairman, Board Members, and External Experts:
  Their responsibilities include overseeing and guiding the governance program, approving the program's objectives and responsibilities, providing strategic direction and support, and ensuring the allocation of necessary resources.
- General Manager and Senior Executive Management:
  Responsible for appointing qualified and experienced individuals to represent their respective departments in the governance program and clearly defining their roles and responsibilities.

Page 6:

- Information Technology Department and Project Management Office (PMO):
  Tasked with the direct management and execution of the governance program.
- Internal Audit and Sharia Audit Departments:
  Actively involved in the program as independent advisors and monitors, performing their responsibilities in accordance with the Bank's governance framework to support the success and integrity of the implementation.
- Risk Management, Information Security, Compliance, and Legal Departments:
  Participate in the program in line with their respective functions, ensuring that their areas of expertise are represented in the governance process.
- Certified Professionals and Subject Matter Experts, internal and external (including COBIT, COBIT 2019 Foundation/Design holders):
  Serve as facilitators and knowledge leaders, supporting the dissemination of best practices and aiding in the successful implementation of the framework.
- The Board is ultimately responsible for overseeing the implementation of the five key governance practices, including establishing structures, evaluating, directing, and monitoring performance, along with "Ensure Risk Optimization" (EDM03) and "Manage Risk" (APO12). This is in line with the Information Governance Instructions issued by the Central Bank of Jordan.

Objectives of Information and Associated Technology Governance and Management

The Information and Technology Governance Committee is responsible for approving a set of bank-wide and IT-specific objectives, guided by the COBIT 2019 framework. These objectives are periodically reviewed and updated to ensure they remain aligned with the evolving needs of stakeholders. The IT Steering Committee & Cyber Security Steering Committee are primarily responsible for ensuring compliance and achieving these objectives. Meanwhile, the IT Governance Committee, a subcommittee of the Board, along with the Board

itself, holds ultimate accountability. All departments across the Bank, particularly the IT Department, Information Security, and the Project Management Office, are required to define and align their operations with the full scope of IT governance processes.

Safwa Islamic Bank has adopted a structured set of objectives under the COBIT 2019 framework to translate stakeholder needs into clearly defined, actionable, and demand-driven outcomes. These include IT-related goals and enabling components, helping to cascade strategic objectives across all levels, departments, and branches of the Bank. The Board and Risk Management Department are directly responsible for "Ensuring Prudent Management of IT-Related Risks" (EDM03) and "Managing Risk" (APO12).

Key governance objectives of information and associated technology include:

a. Meeting stakeholder expectations and supporting the Bank's strategic goals by leveraging the governance framework to:
   - Deliver value through digital services that comply with information and technology governance standards, which include addressing risks in a controlled and proactive manner.
   - Ensure optimal utilization of resources.
   - Provide reliable and high-quality information to support decision-making.
   - Establish a robust infrastructure that enables the delivery of digital services aligned with the Bank's goals.
   - Drive continuous improvement through increased automation and the implementation of reliable, efficient, and purpose-driven technology systems.
   - Manage IT risks to safeguard the Bank's information assets and critical infrastructure.
   - Build a digital ecosystem that complies with applicable laws, regulations, and supervisory guidelines.
   - Enhance the reliability and effectiveness of the internal control environment.
   - Maximize user satisfaction by delivering efficient and effective IT services that meet business needs.
   - Manage services provided by third-party vendors or partners (outsourcing), ensuring that external providers delivering products or services on behalf of the Bank meet all necessary standards and requirements.

b. The use of COBIT 2019 is adopted as the reference framework for the design of all electronic systems and effective solutions, ensuring they align with the objectives of Safwa Islamic Bank and meet the expectations of all stakeholders.

c. A clear distinction is maintained between governance and management, in accordance with internationally recognized standards for information and technology governance. Governance responsibilities assigned to the Board are separated from those assigned to executive management, particularly with respect to information and technology, in line with global best practices.

d. The governance and management of information and associated technology take a holistic approach, encompassing not just technology itself but also the seven enablers as defined by the COBIT 2019 framework.

e. Policies and operational practices are developed and structured based on leading

international standards related to IT governance, IT project management, and technology resource oversight.

f. Mechanisms for self-monitoring, independent oversight, and compliance verification are strengthened to ensure continuous development and improvement in the governance and management of information and technology.

g. The objectives outlined in COBIT 2019, along with the seven related enablers, are directly linked to critical areas such as cybersecurity, risk management, data privacy and protection, compliance, auditing, monitoring, and strategic alignment — all considered high-priority Focus Areas.

h. The capability level of all activities related to the COBIT 2019 framework and its enablers must be proportionate to their assessed importance and priority, as determined by the IT Governance Committee reporting to the Board. For high-priority objectives, the capability level must not fall below Level 3 (Fully Achieved), as defined in the COBIT 2019 maturity model. No more than nine out of the 35 strategic management objectives may be classified as lower priority, based on the governance and IT management framework assessment approved by the IT Governance Committee.

Internal Sharia and IT Audit Department and External Auditor

a. The Board of Directors, through its Audit Committee, is responsible for allocating adequate budgets and resources, including qualified human capital within specialized IT audit departments, to ensure comprehensive and professional IT auditing. The Internal Sharia and IT Audit Department at the Bank, along with the external auditor, must be fully equipped to audit IT resource management, project oversight, and technology-dependent operations. These audits must be carried out by internationally certified professionals (e.g., CISA), accredited in accordance with ISO/IEC 17024 or equivalent international certification standards.

b. The Internal Sharia and IT Audit Department must provide an annual report to both the Audit Committee and the IT Governance Committee of the Board. Similarly, the external auditor must submit an annual report to the IT Governance Committee. These reports must include management's response, in line with the requirements set out under section (d/2) below and according to the reporting template defined in the information and technology governance guidelines issued by the Central Bank of Jordan. Reports must be submitted during the first quarter of each year. The IT Governance Committee is responsible for approving the reports and submitting them to the Central Bank of Jordan, in coordination with the relevant departments at the Bank and within the timelines specified in the applicable regulatory guidelines.

c. The responsibilities, authority, and scope of IT audit must be clearly defined within the Internal and Sharia Audit Charter, which is approved by the Audit Committee and the Board of Directors. The Charter must be circulated across the Bank and reviewed at least annually. Any revisions must be presented to senior executive management and approved by the Audit Committee or the Board. For external auditors, their responsibilities, authority, and scope must be formalized in written agreements and aligned with the relevant regulatory frameworks and the governance and IT management guidelines.

d. In conducting specialized audits of information and associated technology, the Internal Sharia and IT Audit Department and the external auditor must comply with the following:

1. IT audits must conform to the most recent version of the Information Technology Assurance Framework (ITAF) issued by ISACA, including:
    - Executing audit tasks under an approved audit plan that considers the materiality, risk levels, and potential impacts on the Bank's objectives and stakeholders.
    - Ensuring that audit staff engage in continuous professional development and training.
    - Upholding organizational and professional independence, and avoiding any present or future conflicts of interest.
    - Maintaining objectivity, applying due professional care, and preserving a high level of competency and proficiency, including a thorough understanding of the Bank's IT systems and operations. Auditors must also be capable of interpreting various audit reports (financial, operational, legal), gathering appropriate evidence, and identifying unacceptable practices or violations of laws and regulations.
2. The audit must include a review of the recruitment and management of IT resources and related Bank operations. Auditors must issue a general opinion regarding the overall level of IT-related risk. The audit program should, at a minimum, cover the key focus areas outlined in the Central Bank of Jordan's governance guidelines. The frequency and scope of these audits, whether full or partial, must align with the Bank's approved annual audit plan and the regulatory requirements. Audit findings must be submitted to the Central Bank (in coordination with the relevant departments within the Bank). The report must include the agreed-upon corrective actions that management intends to implement, along with clearly defined deadlines for their completion.
3. Implement structured procedures to follow up on audit results to ensure that all observations and deficiencies highlighted in audit reports are addressed within the specified timeframes. Escalation measures must be taken in the event of noncompliance, based on the level of importance and risk. The Board, through the Audit Committee, must be kept informed as necessary.
4. Annual performance evaluations of IT audit staff must include objective measurement criteria that take into account all considerations outlined in section (c) above.

e. IT auditors within the Internal Sharia and IT Audit Department at the Bank, as well as the external auditor, must adhere to the ethical standards and professional practices adopted by the Bank. These must include, at a minimum, the ethical code outlined in the Information Technology Assurance Framework ITAF issued by ISACA and its most recent updates. Reports issued by both internal and external auditors must be approved by the IT Governance Committee of the Board, and the Board must be kept informed of such reports.

Risk, Compliance, and Legal Affairs

A key role in the governance of information and related technology is played by the Risk Management Department, which ensures the existence of a general IT risk management framework aligned with the Bank's overall enterprise risk management framework. The Legal

Department contributes by providing legal advice and guidance, when consulted, on relevant legal matters and proposed legal safeguards. The Compliance Department ensures that all Bank activities remain compliant with applicable regulations, whether issued by local regulatory authorities in Jordan or by international bodies, and that the Bank continues to meet all legal and regulatory requirements.

References

1. This Guide is based on the Central Bank of Jordan's Instruction No. 65/2016 and Circular No. 984/6/10 dated 21/01/2019, as well as the COBIT 2019 framework. It must be reviewed and updated regularly by the IT Governance Committee of the Board or whenever relevant directives are issued by the Central Bank of Jordan.
2. The Bank will publish this Guide on its website and may also make it available to the public through other appropriate means. The Bank shall disclose in its annual report the existence of this Guide and the extent of compliance with its provisions.

Committees

Safwa Islamic Bank has formed the following committees:

1. IT Governance Committee of the Board
2. IT Steering Committee
3. Cybersecurity Steering Committee

The Board of Directors of Safwa Islamic Bank has approved the Bank's overall organizational structure, along with specific structures related to the management of IT resources and projects, risk management, information security, and cybersecurity. These are designed to meet the operational needs of the information and technology governance framework and ensure both efficiency and effectiveness.

IT Governance Committee of the Board

1. In accordance with the Central Bank of Jordan's directives, the Bank has formed the IT Governance Committee of the Board. The Committee comprises four members who have been selected based on their strategic expertise and experience in information technology.
2. The Committee meets at least quarterly and maintains documentation of its meetings. Its responsibilities, as outlined in its charter, include the following:
    a. Approving strategic IT objectives and appropriate organizational structures, including executive-level steering committees, particularly the IT Steering Committee, to ensure alignment with the Bank's strategic goals and maximize value from IT investments and projects. The Committee also ensures the use of appropriate monitoring tools and standards, such as the Balanced IT Scorecards and Return on Investment (ROI) calculations, to measure financial and operational efficiency.
    b. Approving the overarching framework for managing, controlling, and monitoring IT resources and projects in accordance with globally accepted best practices, specifically COBIT 2019, to meet the goals and requirements of the Central Bank

of Jordan's Instruction No. 65/2016 on information and technology governance and management, enabling sustainable achievement of corporate objectives and fulfillment of the related information and technology objective matrix.

c. Approving the matrix of corporate objectives and associated information and technology objectives, considering these as minimum standards, and defining the necessary sub-objectives required to achieve them.

d. Approving a RACI chart (Responsible, Accountable, Consulted, Informed) for the key IT governance processes and their sub-processes, identifying the parties with primary responsibility, final accountability, advisory roles, and those to be informed, based on the enabling processes and guidance of COBIT 2019.

e. Ensuring that a comprehensive IT risk management framework exists and is integrated with the Bank's overall enterprise risk framework, addressing all aspects of IT governance operations.

f. Approving the budget for IT resources and projects in alignment with the Bank's strategic objectives.

g. Exercising overall oversight and monitoring of IT operations, resources, and projects to ensure their adequacy and effective contribution to meeting the Bank's requirements and objectives.

h. Reviewing IT audit reports and taking necessary actions to address any deviations.

i. Recommending to the Board any required corrective actions for identified deviations.

j. Submitting periodic reports to the Board.

k. Approving the prioritization and importance of Governance and Management Objectives and their alignment with Enterprise Goals and Alignment Goals, as well as their relevance to the seven Enabler Components outlined in the relevant regulations. This shall be based on qualitative and/or quantitative studies conducted for this purpose at least once a year, and shall take into consideration the Design Factors set out in the COBIT 2019 Design Guide.

IT Steering Committee

The Bank has formed an Executive IT Steering Committee composed of members from senior executive management, to ensure strategic alignment of IT with the Bank's long-term goals and to sustainably achieve strategic objectives. The committee is chaired by the General Manager and includes senior executives such as the Head of IT, Head of Risk Management, and Head of Information Security. A Board member is appointed as an observer, along with the Head of Internal and Sharia Audit. Other parties may be invited to meetings as needed, as specified in the Terms of Reference (TOR). The committee documents its meetings and convenes at least once every three months.

The responsibilities of this committee are as follows:

1. Reviewing and recommending the approval of annual plans aimed at achieving the strategic objectives approved by the Board, overseeing their implementation, and continuously monitoring internal and external factors affecting them.
2. Linking the Enterprise Goals Matrix with the Information and Technology Goals Matrix,

approving and continuously reviewing them to ensure alignment with the Bank's strategic goals and regulatory requirements. This includes defining performance measurement criteria, regularly reviewing them, and assigning responsible executives to monitor these indicators and report to the committee.

3. Recommending the allocation of financial and non-financial resources necessary to achieve the objectives and to support IT governance processes. This includes appointing qualified personnel in suitable roles through organizational structures that uphold task separation and prevent conflicts of interest. The IT infrastructure and related services should be customized to support the objectives, while the committee also supervises the implementation of IT governance projects and processes.
4. Prioritizing IT projects and programs.
5. Monitoring the quality and efficiency of technical and technological services, and working on their continuous improvement.
6. Submitting recommendations to the IT Governance Committee concerning the following:
   - Allocation of the resources and mechanisms necessary to fulfill the duties of the IT Governance Committee.
   - Any deviations that could negatively impact the achievement of strategic objectives.
   - Any unacceptable risks related to IT, information security, or cybersecurity.
   - Performance and compliance reports related to the overarching framework for managing, controlling, and monitoring IT resources and projects.
7. Providing the IT Governance Committee with its meeting minutes on a regular basis and ensuring their review and follow-up.

Cybersecurity Steering Committee

The Bank has formed a Cybersecurity Steering Committee composed of senior executive management members to ensure strategic alignment of information security and to sustainably achieve the Bank's strategic objectives. The committee is chaired by the General Manager and includes senior executives such as the Head of Information Security, Head of Risk Management, Head of Compliance, Chief of Retail Banking, and Chief Business Transformation and Operating Officer. The Head of Internal and Sharia Audit serves as an observer. Other parties may be invited to meetings as needed, as outlined in the Terms of Reference (TOR), which are approved by the Board. The committee documents its meetings and convenes at least once every three months. The responsibilities of the committee are as follows:

1. Reviewing and providing input to the Board's Risk Management Committee regarding regular assessments of cybersecurity risks and the Bank's Cyber Risk Appetite.
2. Reviewing the cybersecurity strategy and policy to ensure alignment with business objectives.
3. Reviewing cybersecurity risk management processes, including Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) for the cybersecurity program.
4. Assessing the Bank's resilience to cyber risks and its current cybersecurity posture, through Cyber Risk Resiliency and Posture Assessments Reports.

5. Ensuring the availability of necessary resources to implement cybersecurity programs.
6. Reviewing cybersecurity awareness programs.
7. Monitoring the evolving landscape of cyber threats and supporting initiatives related to cybersecurity.
8. Approving, supervising, and monitoring the implementation of Bank projects related to information security and cybersecurity, and providing related recommendations.
9. Approving and reviewing the annual and strategic cybersecurity plan.
10. Ensuring the alignment of information security with the Bank's strategic objectives.
11. Reviewing and evaluating security incidents related to cybersecurity.
12. Approving the formation of a Security Incident Response Team and defining its responsibilities and authorities.
13. Recommending the approval of information security and cybersecurity policies and their amendments.
14. Recommending the approval of exceptions to information security and cybersecurity policies.
15. Reviewing periodic reports on the results of vulnerability and penetration tests.

The Seven IT Governance System Components

The seven enablers of the IT governance system are:

1. Processes and Objectives
2. Organizational Structures
3. Principles, Policies, and Frameworks
4. Information and Reports
5. Ethics, Values, and Behaviors
6. Knowledge, Skills, Experience, and Competencies
7. Services, Programs, and IT Infrastructure

First: IT Governance Processes and Objectives

1. The Bank shall prepare and approve a Responsibility and Information Matrix (RACI) in accordance with the objectives and processes outlined in the COBIT 2019 reference framework, identifying for each process:
    - Responsible party
    - Accountable
    - Consulted
    - Informed

This matrix shall be guided by COBIT 2019 and approved by the committees referenced in the regulations.

2. Bank shall provide the means to achieve IT Governance Goals and Alignment Goals as outlined in the COBIT 2019 reference framework.
3. Bank shall develop an overarching IT Risk Management Framework that aligns with and integrates into the Bank's enterprise-wide risk management framework. This framework should address and fulfill all IT governance objectives stated in the COBIT 2019 reference framework.

The IT Governance Goals and Alignment Goals listed in COBIT 2019 and their accompanying elements represent a minimum standard that executive management must comply with and continually work to achieve. The IT Steering Committee is primarily responsible for ensuring compliance with these requirements, while the Governance Committee and the Board of Directors bear the ultimate accountability. All Bank departments, especially Information Systems, Information Security, Cybersecurity, and Project Management, must define and restructure their operations to reflect and cover all IT governance processes.

Second: Organizational Structures

The Board must approve the Bank's overall organizational structure, particularly those structures related to IT resources, operations, project management, risk management, human resources, information security, and cybersecurity. These structures must fulfill the objectives and requirements of IT governance processes as defined in the COBIT 2019 framework. This includes ensuring segregation of duties for inherently conflicting functions, meeting minimum requirements for organizational control and dual oversight, and updating job descriptions and modifying organizational structures as needed.

Third: Principles, Policies, and Frameworks

- The Board, or any of its delegated committees, shall approve the set of principles and frameworks required to establish the overall framework for managing, controlling, and monitoring IT resources and projects, in accordance with the IT governance objectives and processes outlined in COBIT 2019.
- The Board, or its delegated committees, must also approve the principles, policies, and frameworks, especially those related to IT risk management, information security and cybersecurity, and human resources, that align with IT governance goals and requirements specified in the COBIT 2019 framework.
- The Board, or its delegated committees, must approve a system of policies governing IT governance resources and operations, as outlined in the COBIT 2019 reference framework. This policy system shall be considered a minimum standard. However, combining and integrating policies may be permitted based on business needs. Additional policies may also be developed to reflect the Bank's evolving objectives and operational mechanisms. Each policy must clearly identify the owning entity, and the scope of application, responsibilities, and related procedures.
- When developing policies, it is important to ensure the involvement of all relevant internal and external parties and to adopt international best practices and their updates as references for policy formulation. The committee may, when necessary and at the Bank's expense and in coordination with the Board Chairman, seek the assistance of external experts, both to fill gaps in expertise and to reinforce objectivity. The committee may also invite any Bank executives to attend its meetings

to obtain their input, including those involved in internal audit and senior executive management (such as the IT Director), or those related to external audit.

Below are the principles of the IT Governance Framework, which are divided into two groups:

Group One: Core and Foundational Principles that Constitute the Governance System

- Principle 1: Implementing a Flexible Governance System
  The adopted governance system must be flexible, adaptable, and responsive to internal and external changes and developments.
- Principle 2: Ensuring Inclusiveness
  Governance must encompass all technological aspects and related business operations as defined in the COBIT 2019 reference framework.
- Principle 3: Creating Added Value for Stakeholders
  Added value is achieved by establishing a clear governance framework that defines tasks and responsibilities for work teams.
- Principle 4: Implementing an Integrated Governance System
  The availability of policies and procedures ensures the effective use of IT resources to meet the objectives and governance processes outlined in the COBIT 2019 reference framework.
- Principle 5: Aligning with Bank Requirements and Needs
  The objectives and governance processes in the COBIT 2019 reference framework must align with the specific needs and requirements of the Bank.
- Principle 6: Separating Governance from Management
  Governance should ensure oversight and supervision, while management handles operational execution.
- Group Two: Principles Related to the Governance Framework Needed to Build the Governance System Across the Bank
- A flexible framework that is modifiable and updatable
- Based on a conceptual model serving as an analytical tool
- Adoption of practices, rules, and organizational structures according to key standards

Fourth: Information and Reports

The Board and executive management are responsible for developing the infrastructure and information systems necessary to provide information and reports to users as a foundation for decision-making within the Bank. The Board, or any of its delegated committees, must approve the information and reporting system outlined in the COBIT 2019 reference framework, which should be treated as a minimum standard. Information/report owners must be identified to manage permissions for access and usage, based on business needs and relevant stakeholders. This system must be reviewed and developed regularly to keep pace with the Bank's evolving goals and operations and in line with internationally accepted best practices.

Fifth: Values, Ethics, and Behavior Framework

- The Board, or any of its delegated committees, must approve a professional institutional code of ethics that reflects internationally accepted behavioral standards in dealing with

information and its accompanying technologies. This code must clearly define desirable and undesirable behaviors and their consequences.

- The Board and executive management are responsible for implementing mechanisms that promote desired behaviors and discourage undesirable ones by applying governance methods.
- Sixth: Knowledge, Skills, and Expertise
- The Board, or any of its delegated committees, shall approve an HR Competencies matrix and HR management policies necessary to fulfill the requirements of IT governance operations and the broader requirements of these guidelines, ensuring the right person is placed in the right position.
- The Bank's management shall employ qualified and trained personnel with expertise in managing IT resources, risk management, information security, and internal and external IT audit. This should be based on academic and professional knowledge standards and practical experience, recognized by internationally accredited organizations according to the international certification standards (ISO/IEC 17024), and/or other equivalent standards based on each field of specialization. Existing staff must be requalified and trained to meet the requirements outlined in these guidelines.
- Executive management is responsible for continuously providing its staff with training and ongoing education programs to maintain the level of knowledge and skills required to achieve IT governance operations.
- Executive management is also responsible for incorporating annual performance evaluation mechanisms based on objective performance measurement standards, taking into account the role and contribution of each position in achieving the Bank's goals.

Seventh: IT Services, Programs, and Infrastructure

The Board, or any of its delegated committees, along with senior management, shall approve the suite of programs and supporting infrastructure necessary to achieve the Bank's objectives and reach an acceptable level of governance for information and its associated technologies.