البنك العربي الاسلامي الدولي
ISLAMIC INTERNATIONAL ARAB BANK

IT Governance and Management Manual

May 2019

Contents

Introduction

1. Introduction

1.1 IT Governance and Management Overview:

The IT Governance and Management Framework at Islamic International Arab Bank (IIAB) is established to ensure that IT objectives are aligned with business objectives and to meet the stakeholder needs to maximize value from IT and to create a balance between benefit realizations, risk optimization and resource utilization.
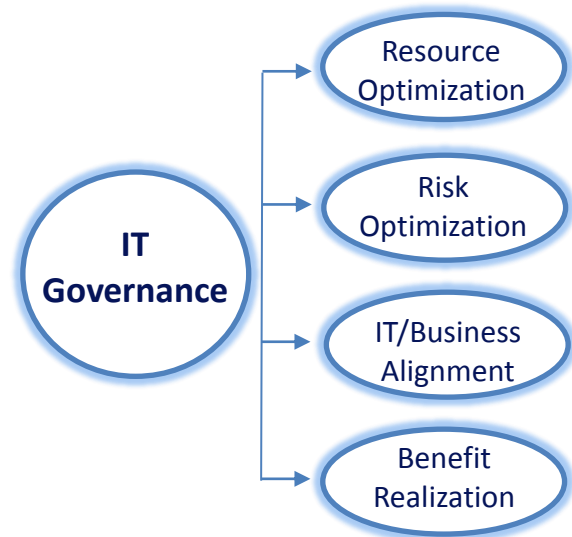
1.2 IT Governance and Management Objectives:

The IT Governance and Management framework aims to achieve the following objectives:

1. Meet stakeholders' needs and achieve the Bank's goals and objectives through achieving the alignment goals to ensure:
   – Providing high-quality information as a pillar supporting decision-making in the bank.
   – Prudent management of resources and projects of information technology and maximize the use of those resources and reduce waste.
   – Providing a unique and supportive technological infrastructure enabling the Bank to achieve its objectives.
   – Improving the Bank's various operations through the use of an efficient and reliable technological system.
   – Prudent risk management of information technology to ensure the necessary protection of the assets of the bank.
   – Compliance with the requirements of domestic laws, legislation and internal regulations.
   – Improving the system of internal control and control.
   – Maximize the level of satisfaction with information technology by users to meet the needs of work efficiently and effectively.
   – Management of the services of the external parties entrusted with the implementation of operations, functions, services and products.

2. Achieving inclusiveness in the governance and management of information and associated technology in terms of taking into account not only the technology itself but also the provision of seven enabling elements that are complementary and complementary to IT services.

3. Adopting business practices and rules as a starting point for governance and management of IT processes, projects and resources.
4. Separate the operations, functions and responsibilities of the Board in the area of governance over the talc which fall within the limits of the responsibility of the executive management regarding the information and technology accompanying it.
5. To strengthen the mechanisms of self-monitoring and independent control and to examine compliance in the areas of governance and management of information associated with them and contribute to the improvement and development of performance on an ongoing basis.

Governance and Management of
Enterprise IT Framework

2. Governance and Management of Enterprise IT at Islamic International Arab Bank

The following diagram represents the overall framework for the Governance of Enterprise IT at Islamic International Arab Bank that is based on CoBIT 2019 framework and principles:
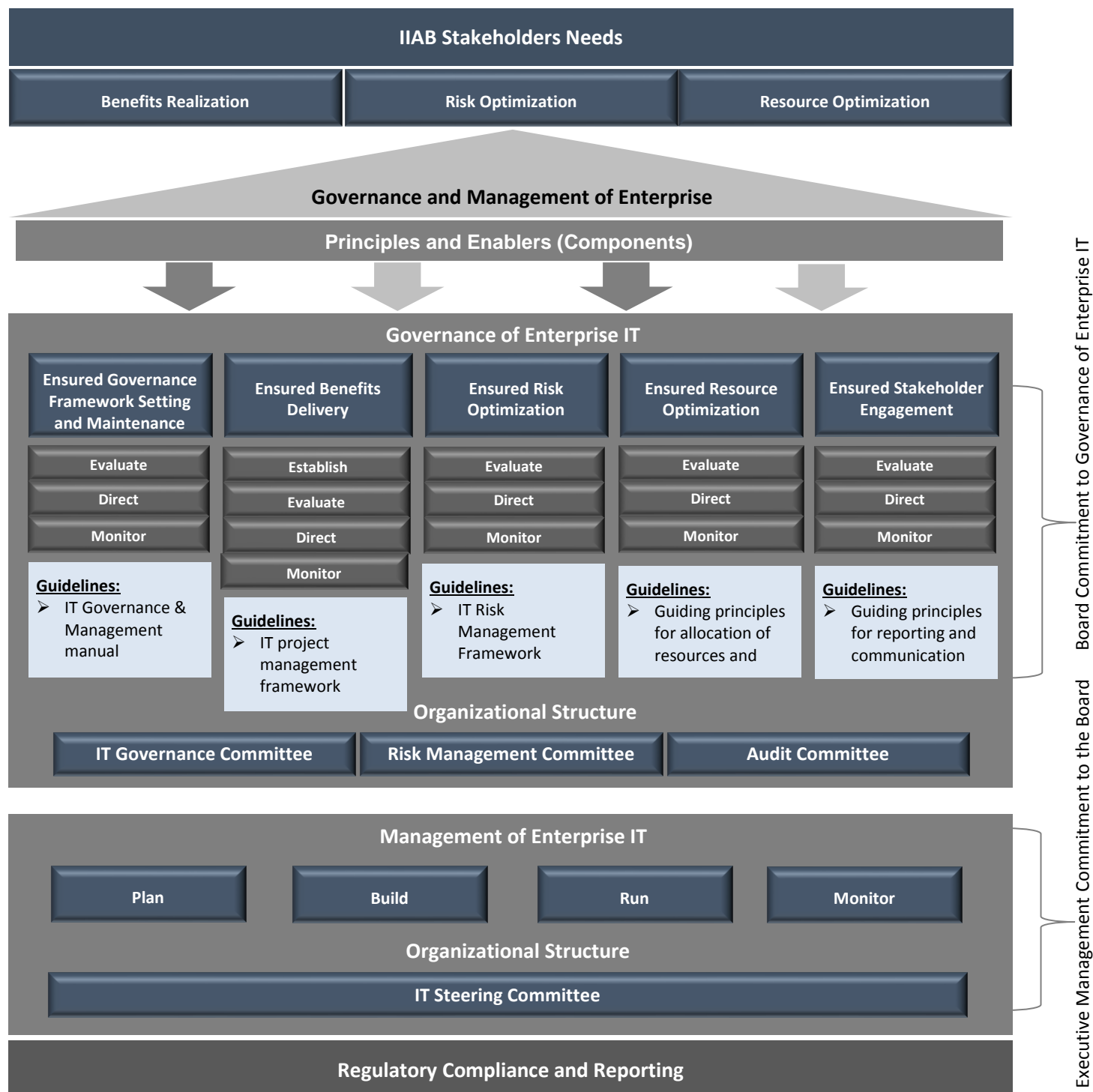

Illustrative Figure 1: Governance of Enterprise IT Overall Framework

3. Governance of Enterprise IT:

3.1 Board Commitment to Governance of Enterprise IT:

Islamic International Arab Bank's Board is committed to adopting a holistic approach to ensure proper Governance of Enterprise IT. The Board is accountable to Evaluate, Direct and Monitor (EDM) governance processes that entails the following:

1. Ensured Governance Framework Setting and Maintenance by endorsing the "IT Governance and Management Manual";
2. Ensured Risk Optimization by endorsing the "IT Risk Management Framework";
3. Ensured Resource Optimization by endorsing the "Guiding Principles for Allocation of Resources and Capabilities";
4. Ensured Benefits Delivery by endorsing the "Project Management Framework"; and,
5. Ensured Stakeholder Engagement by endorsing "Guiding Principles for Reporting and Communication".
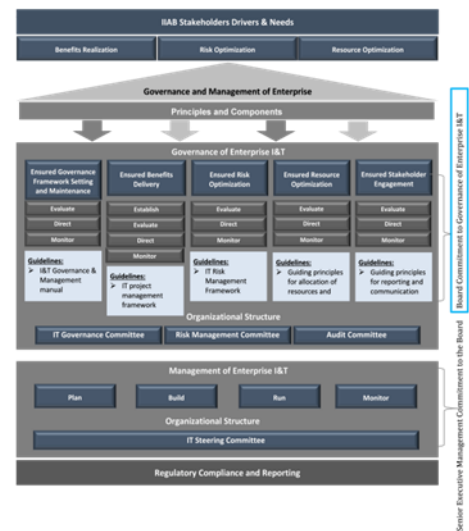
3.2 Organization Structure:

The following committees are established to support and enable the Governance of Enterprise IT:

1. Risk Management Committee

Risk Management Committee is responsible for IT Risk Management and Business Continuity Management.

2. Audit Committee

The Audit Committee is responsible to provide reasonable assurance over the compliance with the IT governance framework practices.

3. IT Governance Committee

IT governance committee is established to support the board of directors with regards to the Governance of Enterprise IT.

Scope and purpose: The scope and purpose of the IT Governance Committee is to ensure IT objectives are in line with the bank's strategic direction and to ensure that the stakeholders' needs are met by creating a balance between benefit realization, risk optimization and resources optimization.

Members: The IT Governance Committee is comprised of three board members.

Meeting Frequency: The IT Governance Committee meets on a quarterly basis or as required.

The IT Governance Committee aims to achieve the following objectives:

1. Ensured Governance Framework Setting and Maintenance;
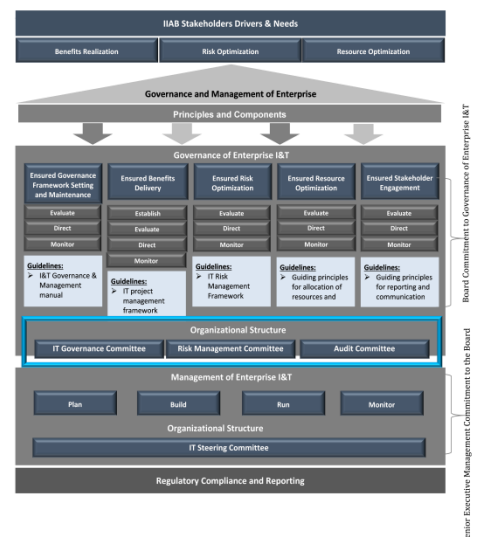
2. Ensured Risk Optimization;

3. Ensured Resource Optimization;

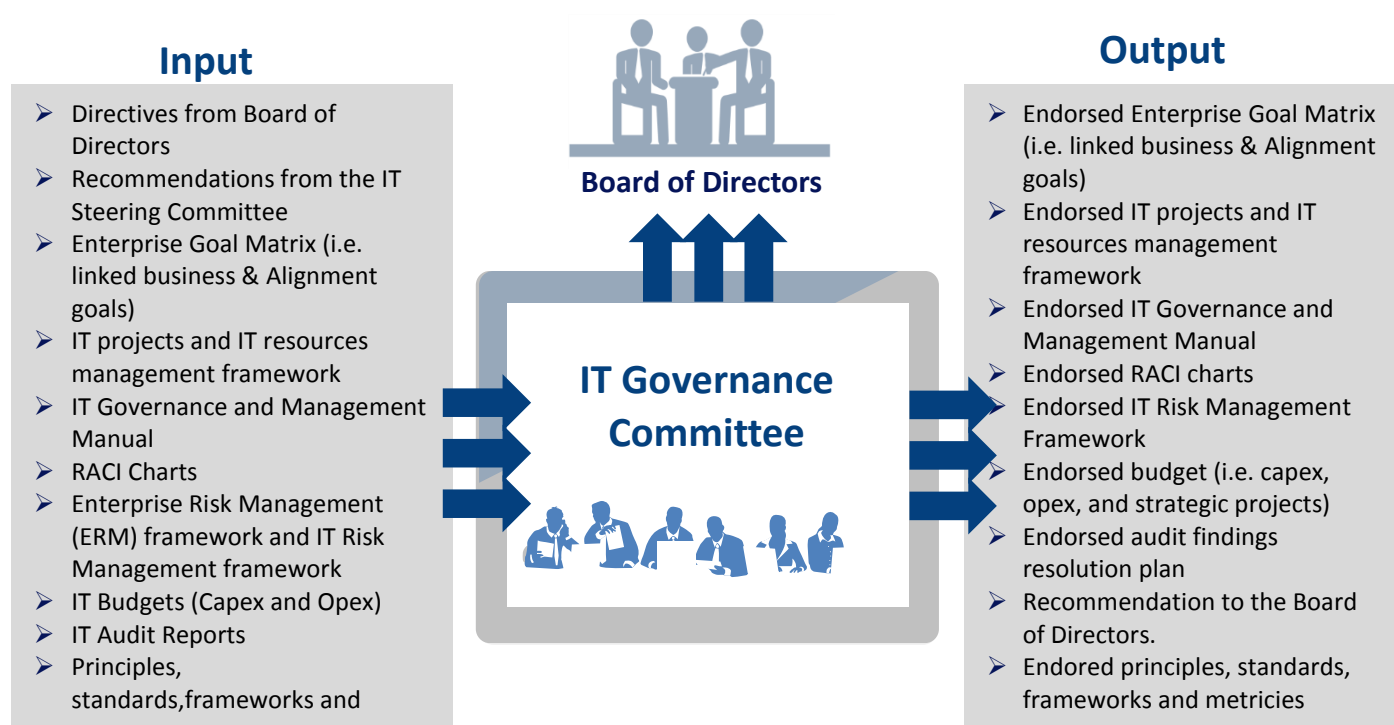4. Ensured Benefits Delivery; and,

5. Ensured Stakeholder Engagement.

Roles and Responsibilities:

1. To endorse alignment goals and appropriate organizational structures including steering committees in a manner that fulfills and achieves strategic objectives and maximizes added value of IT projects and investments.

2. To monitor the realization of strategic objectives through utilizing appropriate tools and standards such as IT Balanced Scorecards and Return on Investments (ROI) calculation.

3. To endorse the IT governance, processes, projects and resources control, monitoring and management framework that is aligned with leading practises in order to achieve improved operational and financial efficiency.

4. To endorse an Enterprise Goals Matrix that links business and alignment related goals & sub goals.

5. To endorse the governance and management objectives and sub practices roles and responsibilities (i.e. RACI Charts).

6. To endorse the importance and prioritization of the objectives of governance and management in terms of their association with the goals and the other six components by preparing a qualitative / quantitative study prepared for this purpose at least annually, Taking into account that the objectives/processes related to cybersecurity, risk management, privacy, data protection, compliance, control, auditing and strategic compliance Are high priority objectives.

7. To ensure the availability of an IT Risk Management Framework that is aligned with the Enterprise Risk Management (ERM) Framework.

8. To endorse IT projects and IT resources budgets in alignment with the bank's strategic goals.

9. To monitor and oversee the IT operations, projects and resources to ensure alignment with the bank's strategic goals and the realization of expected benefits.

10. To review the IT audit reports and ensure that corrective actions are implemented to resolve reported deviations.

11. To raise necessary recommendations on corrective actions to resolve deviations to the Board of Directors.

12. To endorse the following principles, standards, frameworks and matrices:

    ➢ IT projects and resources management principles, policies and frameworks.

    ➢ IT Risk Management, Information Security Management and Human Resources Management frameworks.

    ➢ Policies matrix required to manage IT governance and resources along with the policies' development principles, ownership, and scope.

    ➢ Information and reports matrix that defines owners and access privileges according to business needs.

    ➢ IT services, programs and infrastructure matrix that supports the IT governance objectives.

- IT services, programs and infrastructure matrix that supports the bank operations.

- IT Human Resources Policy and Competency Matrix covering the IT governance objectives required skills in HR Management, Risk Management, Information Security Management, and Internal Audit areas. Further, to ensure that the annual performance evaluation process measures the achievement level of the Banks' goals.

- A Code of conduct that reflects acceptable IT usage professional & behavioural rules and to ensure that proper internal and external audit procedures are available to monitor behaviours.

*The following diagram represents the IT Governance Committee's inputs and outputs:*

Input

Board of Directors

- Directives from Board of Directors
- Recommendations from the IT Steering Committee
- Enterprise Goal Matrix (i.e. linked business & Alignment goals)
- IT projects and IT resources management framework
- IT Governance and Management Manual
- RACI Charts
- Enterprise Risk Management (ERM) framework and IT Risk Management framework
- IT Budgets (Capex and Opex)
- IT Audit Reports
- Principles, standards,frameworks and

IT Governance Committee

Output

- Endorsed Enterprise Goal Matrix (i.e. linked business & Alignment goals)
- Endorsed IT projects and IT resources management framework
- Endorsed IT Governance and Management Manual
- Endorsed RACI charts
- Endorsed IT Risk Management Framework
- Endorsed budget (i.e. capex, opex, and strategic projects)
- Endorsed audit findings resolution plan
- Recommendation to the Board of Directors.
- Endored principles, standards, frameworks and metricies

Illustrative Figure 2: IT Governance Committee Inputs and Outputs

4. Management of Enterprise IT:

4.1   Senior Executive Management Commitment to the Board:

Senior Executive Management is responsible for implementing the Board's vision and strategy by:

1. Aligning, planning and organizing alignment goals and initiatives as indicated by the Board's strategic direction and vision for business and IT;
2. Building, acquiring and implementing needed infrastructure, applications and services.
3. Running and maintaining the established business services.
4. Monitoring, evaluating, and assessing the performance and compliance of all the IT related processes, practices and activities.
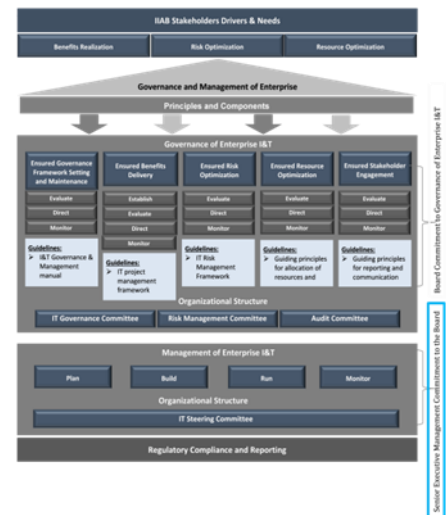
## 4.2   Organizational Structure\ IT Steering Committee:

The IT Steering Committee is established to support the IT Governance Committee in relation to the Management of Enterprise IT implementation practices.

Scope and Purpose: The scope and purpose of the IT Steering Committee is to ensure business and IT alignment and create a balance between benefit realization, resources optimization and IT risk optimization.

Members: The IT Steering Committee is comprised of the following members:

- General Manager (chair of the committee);
- Chief of Business and Investment;
- Chief of Support and Operations;
- Chief of Risk Management;
- Head of Information Technology;
- Head of Operations;
- Head of Projects Management & Enterprise Architecture
- Head of Performance Evaluation & Quality
- Information Security and Business Continuity Manager;
- IT Governance & Quality Manager; and,
- Two observers, which include a Board member and Head of Internal Audit.

Meeting Frequency: The IT Steering Committee meets on a quarterly basis or as required.
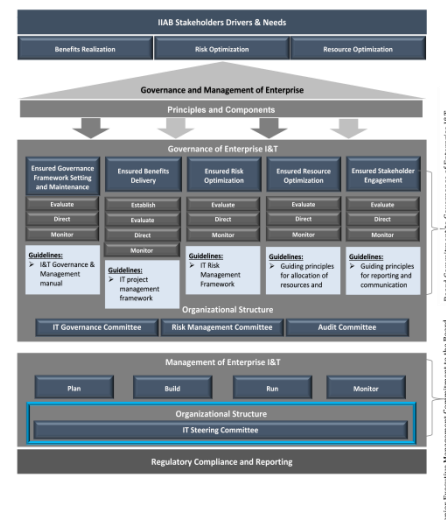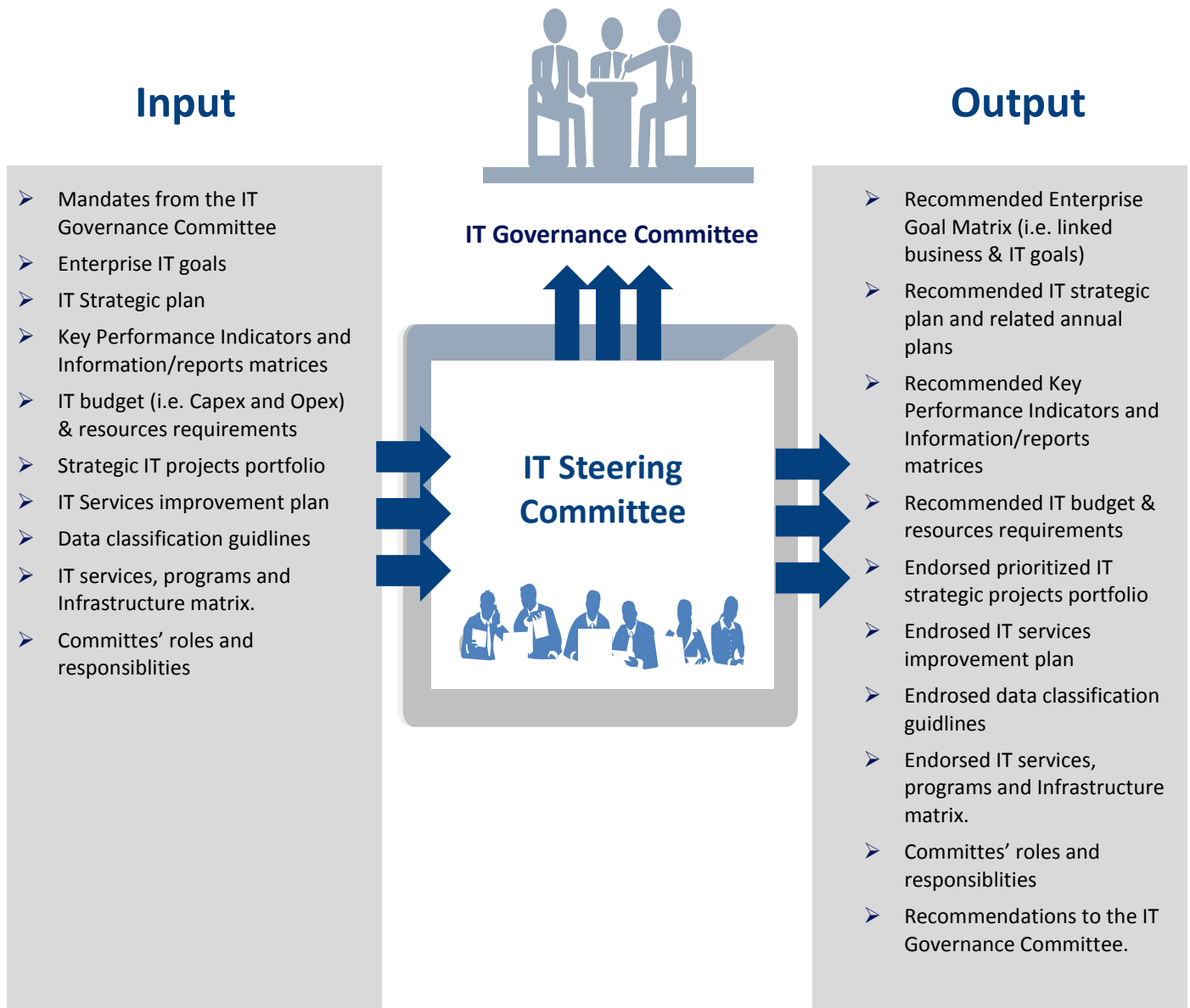
The IT Steering Committee aims to achieve the following objectives:

1. Aligning, planning and organizing alignment goals and initiatives as indicated by the Board's strategic direction and vision for business and IT;
2. Building, acquiring and implementing needed infrastructure, applications and services.
3. Running and maintaining the established business services.
4. Monitoring, evaluating, and assessing the performance and compliance of all the IT related processes, practices and activities.

Roles and Responsibilities:

1. To manage and oversee the implementation of the IT Governance and Management requirements.
2. To approve IT annual plans required to achieve the bank's strategic objectives and to continually monitor the internal and external factors that may affect their completion.
3. To link and regularly review the Enterprise Goals Matrix with the related Alignment Goals Matrix to ensure the achievement of the bank's strategic objectives.
4. To define a set of metrics to measure goals achievement and to assign members from the Senior Executive Management to continuously monitor it and report to the committee.
5. To recommend financial and non-financial resources to acquire appropriate infrastructure and services that are required to achieve IT governance objectives. Further, to supervise IT Governance projects' and objectives' implementation activities.
6. To endorse & prioritize the annual IT programs and projects.
7. To monitor IT services performance and provide recommendations to improve its effectiveness and efficiency.
8. To report necessary recommendations to the IT Governance Committee, on the following:
   ➢ Resources and enablers to achieve IT governance committee roles.
   ➢ Deviations that may adversely affect the achievement of strategic objectives.
   ➢ Unacceptable IT and IS risks.
   ➢ IT projects' and resources' framework performance and compliance reports.
9. To develop information systems and infrastructures required to provide information/reports that supports the IT decision making process and to define requirements for the integrity, confidentiality and availability of information/reports based on the data classification guidelines.
10. To approve the IT services, programs, and infrastructures matrix required to support the IT Governance and Management objectives.
11. To approve the IT services, programs, and infrastructures matrix as detailing minimum requirement and endorse it by the Board or its mandated committees. Further, this matrix should be updated continuously to accommodate the bank's goals and processes development.
12. To report to the IT Governance Committee through formal minutes of meeting.
13. To review and update the committee roles and responsibilities annually.

The following diagram represents the IT Steering Committee's typical inputs and outputs:

Input

Output

IT Governance Committee

IT Steering Committee

- Mandates from the IT Governance Committee
- Enterprise IT goals
- IT Strategic plan
- Key Performance Indicators and Information/reports matrices
- IT budget (i.e. Capex and Opex) & resources requirements
- Strategic IT projects portfolio
- IT Services improvement plan
- Data classification guidlines
- IT services, programs and Infrastructure matrix.
- Committes' roles and responsiblities

- Recommended Enterprise Goal Matrix (i.e. linked business & IT goals)
- Recommended IT strategic plan and related annual plans
- Recommended Key Performance Indicators and Information/reports matrices
- Recommended IT budget & resources requirements
- Endorsed prioritized IT strategic projects portfolio
- Endrosed IT services improvement plan
- Endrosed data classification guidlines
- Endorsed IT services, programs and Infrastructure matrix.
- Committes' roles and responsiblities
- Recommendations to the IT Governance Committee.

**Illustrative Figure 3: IT Steering Committee Inputs and Outputs**

Regulatory Compliance and Reporting

5. Regulatory Compliance and Reporting

5.1 The Board's Commitment to regulatory compliance:

The Board is responsible to ensure that Governance and Management of Enterprise IT practices is established in line with the CBJ's IT Governance and Management regulation (Regulation No: 65/2016) issued on 25/10/2016 & New Circulation (No: 10/6/984) issued on 21/01/2019.

Additionally, the Board shall ensure that Islamic International Arab Bank complies with the applicable IT related requirements of external laws, regulations and instructions as well as internal policies and procedures derived from external laws and regulations.
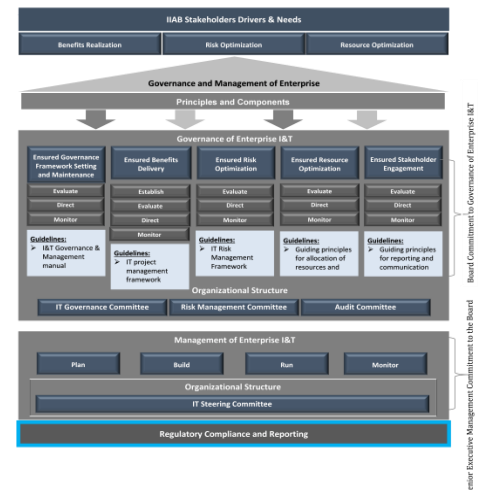
5.2 Reporting:

5.2.1 Annual Reporting

The Bank shall disclose the existence and compliance with the "IT Governance and Management Manual" within the Bank's annual report and shall ensure that it is formally updated at regular intervals or when required.

5.2.2 Internal Audit Reporting

The Internal Audit Department shall:

➢ Conduct risk based IT audits and report to the IT Governance Committee on the effectiveness of the IT Governance Framework in alignment with the CBJs IT Governance and Management regulation (Regulation No: 65/2016) and New Circulation (No: 10/6/984) issued on 21/01/2019.
➢ Ensure that the audit charter scope includes IT Governance and Management objectives in line with the new CBJ Circulation (No: 10/6/984).
➢ Comply with the latest version of IT Assurance Framework International Standard (ITAF) issued by Information System Audit and Control Association (ISACA).

5.2.3 The Audit Committee

➢ The Audit Committee will provide the CBJ with the annual IT audit report during the first quarter of every year.
➢ The Audit Committee shall include the responsibilities, terms of reference and scope of the IT audit work in the Audit Charter on the one hand and in the framework of procedures agreed upon with the External Auditor, in accordance with these instructions.
➢ The Audit Committee should ensure that the internal auditor and the external auditor, when conducting specialized audits of the information and technology accompanying them, must:
  – Comply with the latest version of IT Assurance Framework International Standard (ITAF) issued by Information System Audit and Control Association (ISACA).

- Review, evaluate and review the processes of recruitment and management of IT resources and the operations of the Bank based on them and give an opinion on the overall risk level of information and associated technology.
- Regular procedures for monitoring the results of the audit to ensure follow-up observations and imbalances contained in the auditor's reports on deadlines.
- The Audit Committee shall carry out the annual evaluations of the IT audit staff according to objective measurement criteria that take into consideration all the provisions of Article (d) of Article 9 of the Governor's Instructions and the management of information and technology accompanying them.

5.2.4 External Audit Reporting

- The Bank's external auditor shall perform risk based independent review(s) of the IT Governance and Management objectives, and shall report to the CBJ on the effectiveness of implemented controls.
- The Bank's external auditor shall comply with the latest version of IT Assurance Framework International Standard (ITAF) issued by ISACA.

Principles and Enablers
(Components)

6. Principles & Enablers (Componenets)

6.1 Principles of IT Governance and Management:

Core principles of Islamic International Arab Bank's IT governance and management system are built on the CoBIT 2019 Governance of Enterprise IT principles as follows:

1. Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.

2. A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.

3. A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.

4. A governance system should clearly distinguish between governance and management activities and structures.

5. A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.

6. A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise:

   – The Board level via establishing a stable IT governance system and scope with the objective to achieve stakeholder needs.

   – The Senior Executive Management level via implementing Board level directions to achieve the the agreed on goals and by reporting to the Board on the execution progress and monitoring activities.
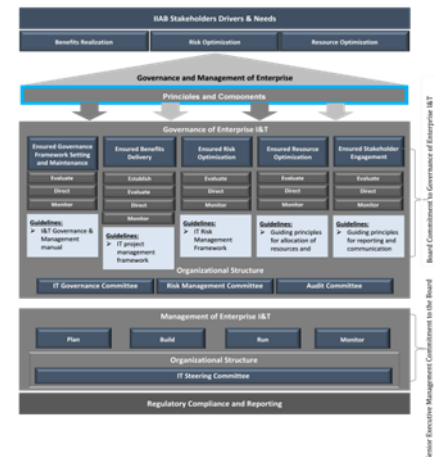
6.2   Enablers (Components)

The following represents the key components that support Islamic International Arab Bank's IT Governance & Management system:

Component 1: Processes/ Governance & Management Objectives

The Board or mandated committees shall endorse governance & management objectives derived from the Bank's policies, procedures, principles, enterprise goals and related IT related goals.

Component 2: Organizational Structures

The Board or his authorized representatives shall endorse Organizational Structures and related committees to achieve IT governance objectives, these structures should clearly illustrate delegation of authority, escalation procedures, decision-making process and segregation of incompatible duties.
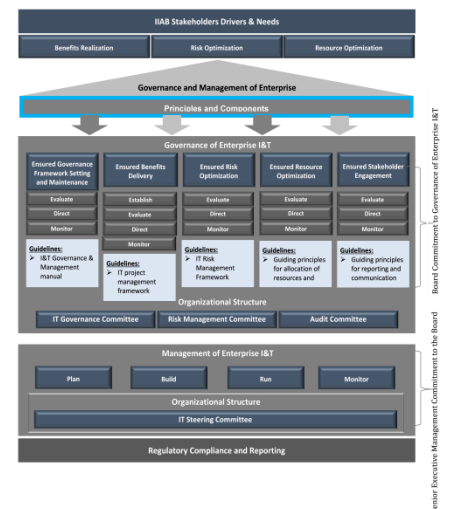
Component 3: Information

The Board or mandated committees shall endorse information and reporting matrix, with assigned owners responsible to authorize access to these information/reports based on business needs. In addition to, ensure that information/reports are regularly updated to accommodate the enterprise objectives and processes improvement in alignment with international leading practices.

Component 4: People, Skills, and Competencies

The Board or mandated committees shall endorse a competency matrix and human resources policies required to achieve IT governance processes requirements, In addition to recruiting qualified and trained personnel from experienced persons and continuing to provide their staff with training and continuing education programs to maintain a level of knowledge and skills that meets and achieves the objectives of governance and management.

Component 5: Principles, Policies and Framework

The Board shall express the bank's core values via its "principles", "policies" and "Framework" that are made available to provide its audience with detailed guidance on how to apply the principles into practices. Further, "principles", "policies" and "Framework" shall be effective & efficient and shall include compliance, management and update requirements, And the policies referred to in the instructions may be considered as a minimum, with the possibility of combining and incorporating those policies as required by the nature of the work.

Component 6: Culture, Ethics and Behavior

The Board or mandated committees shall endorse an enterprise code of conduct that reflects the professional and ethical rules in alignment with acceptable international behaviour rules. This code shall clearly state the desirable and undesirable behaviours and consequences of conduct. Further, the board or Senior Executive Management shall employ diversified mechanisms to encourage desirable behaviours and to avoid undesirable behaviours.

Component 7: Services, Infrastucture and Applications

The Board or mandated committees shall endorse appropriate services, infrastructure and applications to support governance practices and objectives.

Appendices
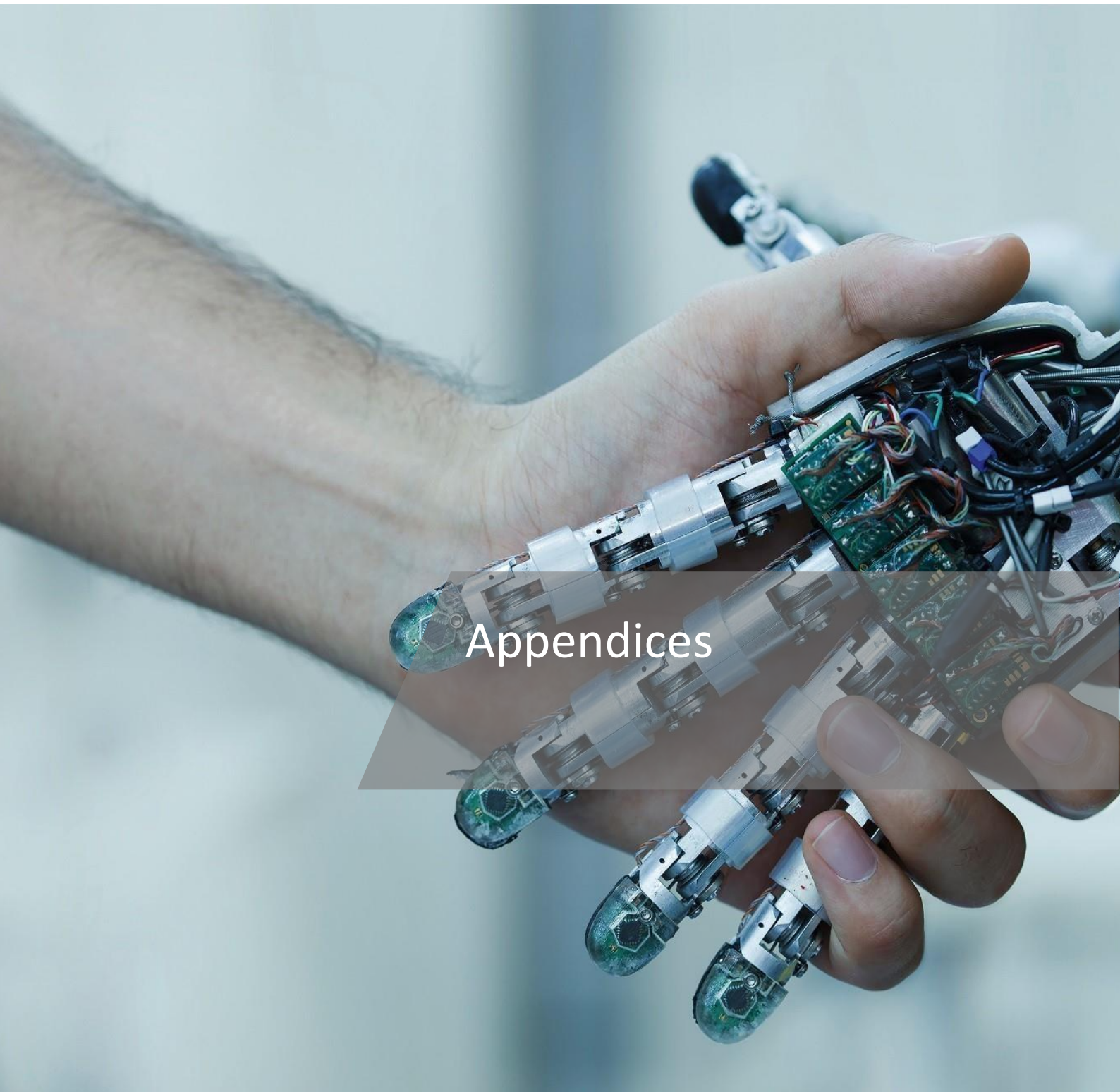
Appendix 1: Definitions

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

1. **Governance of Enterprise IT:** is defined as the objectives that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

2. **Management of Enterprise IT:** Is the set of activities that achieve the strategic objectives through the coordination, organization, construction, development, etc., in order to ensure the sustainability of the objectives and direction of the Bank.

3. **COBIT 2019:** Control Objectives for Information and related Technology – a good-practice business framework developed by ISACA (Information Systems Audit and Control Association) for the governance and management of IT.

4. **The Board:** The Board of Directors of the Bank.

5. **Management:** A body comprised of Senior Executive Management responsible for planning, building, running, and monitoring activities in alignment with the direction set by the governance body to achieve enterprise objectives.

6. **Governance & Management Objectives:** A set of practices and activities emanating from the policies of the institution necessary to achieve the Alignment goals.

7. **Alignment Goals:** A set of main and subsidiary objectives related to the governance and management activities of the information and technology accompanying the objectives necessary to achieve the Enterprise goals.

8. **Enterprise Goals:** Set goals related to enterprise governance and management needed to meet the needs of stakeholders.

9. **Stakeholders**: Any interest in the Bank such as shareholders, employees, customers, creditors, external suppliers or regulatory authorities concerned.

10. **The auditor:** The person (natural or moral) or the competent authority to examine the operations of the bank based on information technology and agreed with him by the bank's management to achieve the requirements of governance and the management of information and technology associated with it.