# IT Governance and Management Manual

## March 2017

ARAB BANK
البنك العربي

# Contents

# Section 1

# Introduction

# 1. Introduction

## 1.1. IT Governance and Management Overview:

The Governance of Enterprise IT Framework at Arab Bank is established to ensure that IT activities are aligned with business objectives and that stakeholder needs of risk optimization, resources optimization and benefit realization are met.

This IT Governance and Management manual represents Arab Bank's Board of Directors commitment to enable the Governance of Enterprise IT.
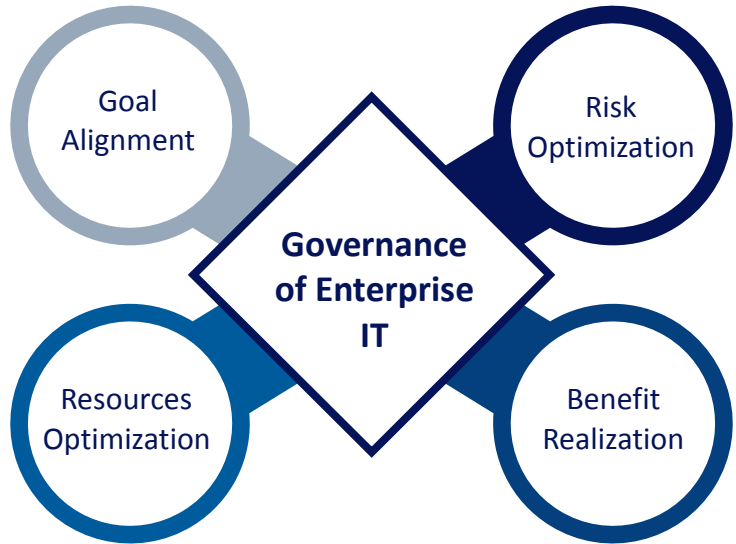


## 1.2. IT Governance and Management Objectives:

The Governance of Enterprise IT framework aims to achieve the following objectives:

1. Align IT goals with business goals.

2. Meet stakeholders' needs of risk optimization, resources optimization and benefit realization.

3. Provide sufficient information and reports to support the decision making process regarding governance and management of enterprise IT.

4. Achieve effective and prudent IT project management and IT resources management processes.

5. Develop technological infrastructure and information systems that enables the banks' business strategies

6. Optimize IT risk management to ensure the necessary protection of the Bank's assets.

7. Comply with laws and regulations' requirements, internal controls and monitoring, and related policies and procedures.

8. Maximize end user's satisfaction level of IT services.

9. Manage third parties/vendors relationships.

البنك العربي
ARAB BANK

# Section 2

# Governance and Management of Enterprise IT at Arab Bank

البنك العربي
ARAB BANK

Governance and Management of Enterprise IT at Arab Bank

The following diagram represents the overall framework for the Governance of Enterprise IT at Arab Bank:
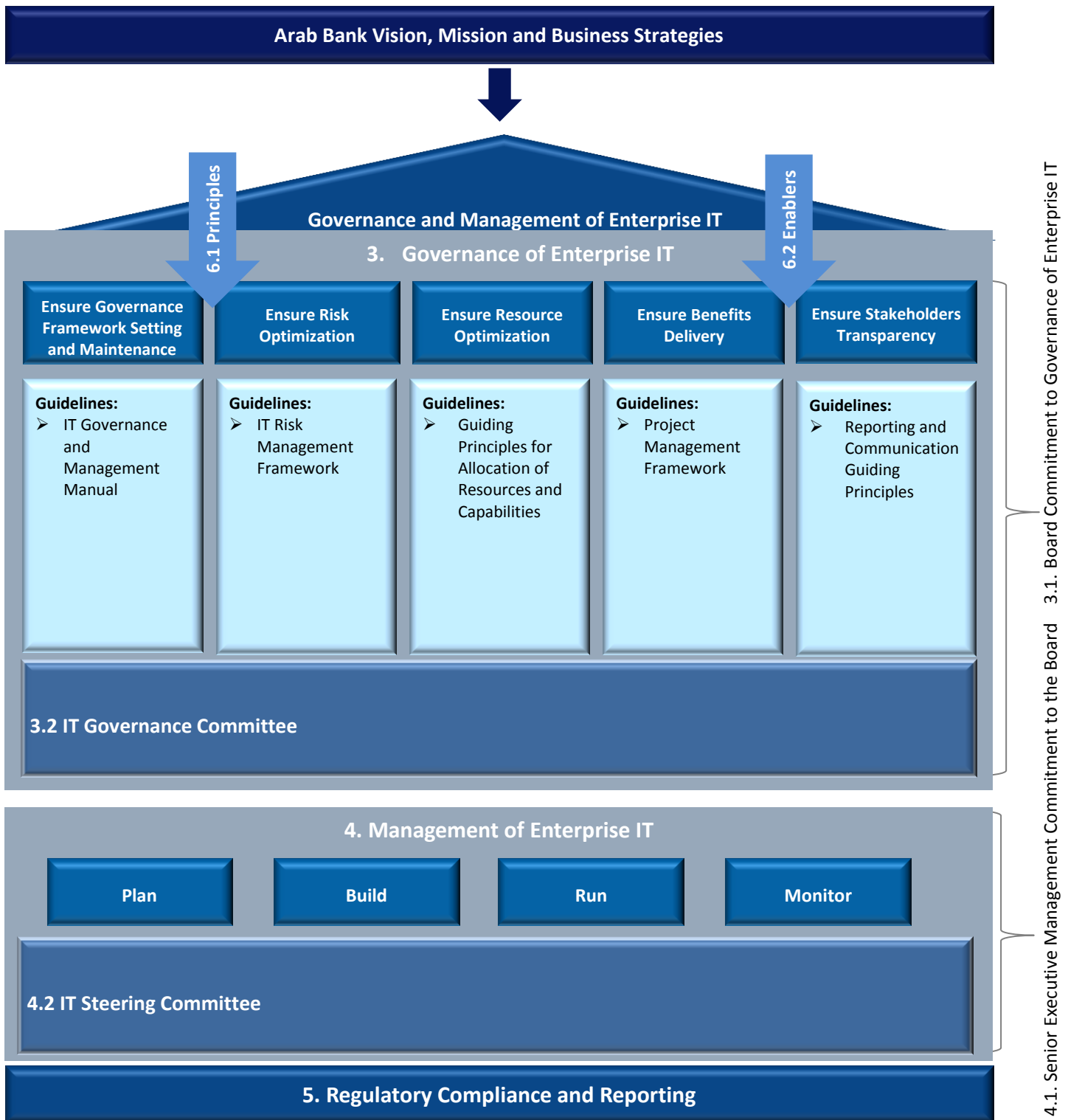


**Illustrative Graph (1): Overall Framework for the Governance and Management of Enterprise IT**

# 2. Governance of Enterprise IT:

## 2.1.    Board Commitment to Governance of Enterprise IT:

Arab Bank's Board adopts 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. Ensure Governance Framework Setting and Maintenance by endorsing the "IT Governance and Management Manual".
2. Ensure Risk Optimization by endorsing the "IT Risk Management Framework".
3. Ensure Resource Optimization by endorsing the "Guiding Principles for the Allocation of Resources and Capabilities".
4. Ensure Benefits Delivery by endorsing the "Project Management Framework".
5. Ensure Stakeholder Transparency by endorsing the "Reporting and Communication Guiding Principles".

## 2.2.    IT Governance Committee:

The IT Governance Committee is established to support the Board of Directors in relation to Governance of Enterprise IT practices.

**Scope and purpose:** The scope and purpose of the IT Governance Committee is to govern IT activities in line with the bank's strategic direction and to ensure that the stakeholders' needs are met including 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 at least a quarterly basis.

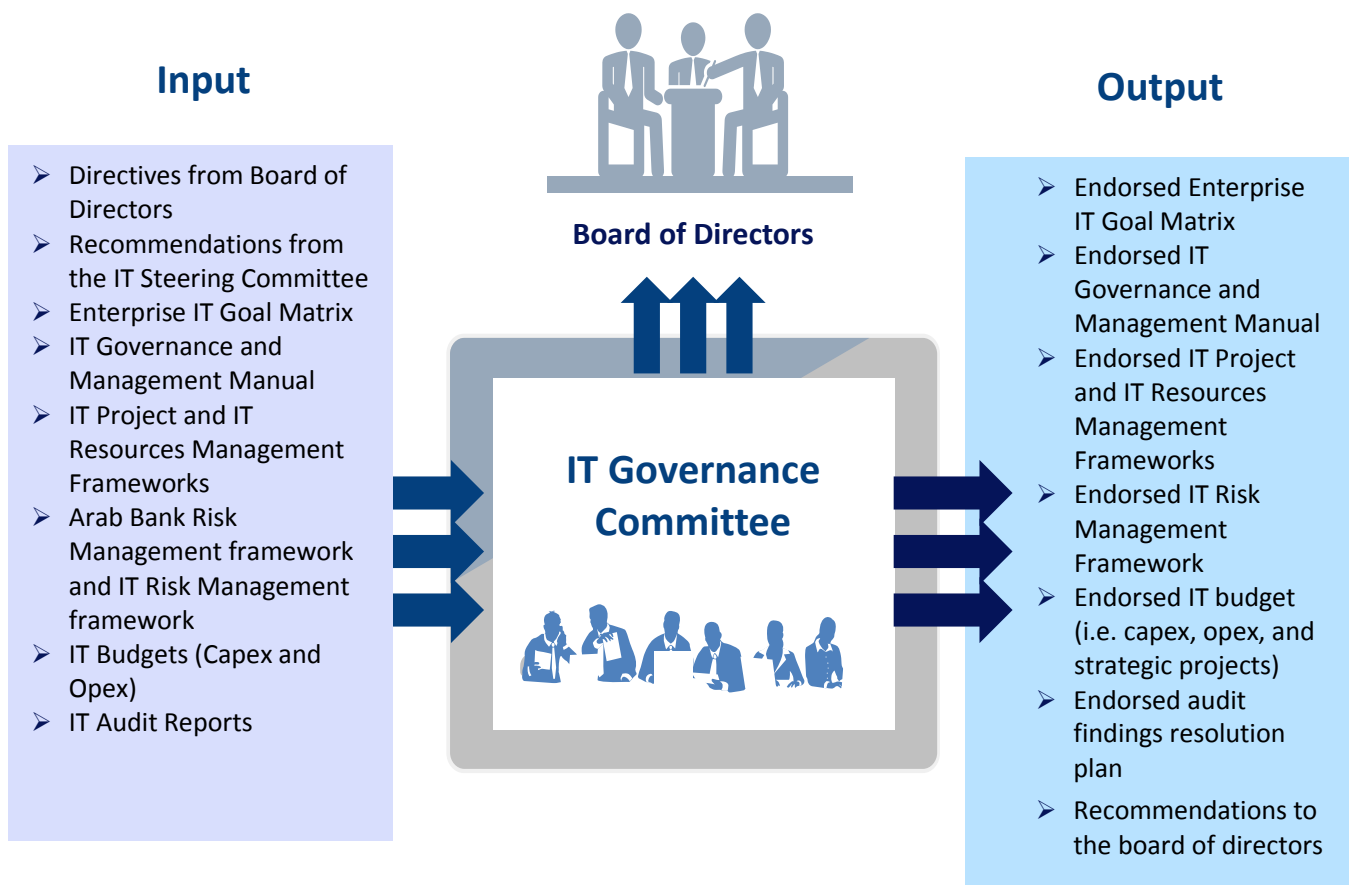**The IT Governance Committee aims to achieve the following objectives:**

1. Ensure alignment of business and IT strategic plans.
2. Nurture and manage innovation for the benefit of Arab Bank and its stakeholders.
3. Ensure the ecosystem and infrastructure is in place to enable appropriate service delivery.
4. Encourage transparency and effective program and project oversight.
5. Ensure independent audit over IT activities.

**Roles and Responsibilities:**

1. To endorse IT strategic goals and appropriate organizational structures including steering committees at the Senior Executive Management level, specifically the IT Steering Committee, in a manner that fulfills and achieves strategic objectives and maximizes added value of IT projects and investments. Further, utilize adequate tools and standards to monitor achievement of IT strategic goals.
2. To endorse the management, control and monitoring framework for IT projects and resources that aligns with the best acceptable international standards in that matter; and precisely Control Objectives for Information and related Technology standard (COBIT), in addition to having the framework in line with the Central Bank of Jordan's regulations.

3. To endorse Enterprise IT Goals Matrix that links business and IT related goals and to define the related sub goals for the achievement of the Matrix.

4. To endorse the governance and management practices roles and responsibilities (i.e. RACI Charts) towards key IT Governance processes and related sub processes, whereby individuals/parties initially (Responsible) to achieve the key processes are to be identified, individuals/parties ultimately (Accountable) to achieve the key processes are to be identified, individuals/parties (Consulted) are to be identified, and lastly, individuals whom are (Informed) of all processes are to be identified.

5. To ensure that an IT Risk Management Framework aligned with the Enterprise Risk Management (ERM) Framework is available.

6. To endorse budgets for IT strategic projects/initiatives and business as usual activities.

7. To monitor the IT operations, projects and resources to ensure alignment with business strategic goals and realization of expected benefits of the Bank.

8. To review the IT audit reports and ensure that corrective actions are implemented to close reported gaps.

9. To raise recommendations on corrective actions to the Board of Directors.

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

## Input

**Board of Directors**

**IT Governance Committee**

## Output

- Directives from Board of Directors
- Recommendations from the IT Steering Committee
- Enterprise IT Goal Matrix
- IT Governance and Management Manual
- IT Project and IT Resources Management Frameworks
- Arab Bank Risk Management framework and IT Risk Management framework
- IT Budgets (Capex and Opex)
- IT Audit Reports

- Endorsed Enterprise IT Goal Matrix
- Endorsed IT Governance and Management Manual
- Endorsed IT Project and IT Resources Management Frameworks
- Endorsed IT Risk Management Framework
- Endorsed IT budget (i.e. capex, opex, and strategic projects)
- Endorsed audit findings resolution plan
- Recommendations to the board of directors

**Illustrative Graph (2): IT Governance Committee Typical Inputs and Outputs**

# 3. Management of Enterprise IT:

## 3.1. 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 IT goals and initiatives as per 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.

## 3.2. IT Steering Committee:

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

**Scope and Purpose:** The scope and purpose of the IT Steering Committee is to ensure business and IT alignment, IT resources and IT risk management optimization

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

➢ Chief Executive Officer (CEO) (chair of the committee);
➢ Deputy CEO (DCEO) (Deputy chair of the committee);
➢ Chief Operating Officer (COO);
➢ Chief Risk Officer (CRO);
➢ Head of Information Technology; and,
➢ Two observers, which include a Board member and Head of Internal Audit.

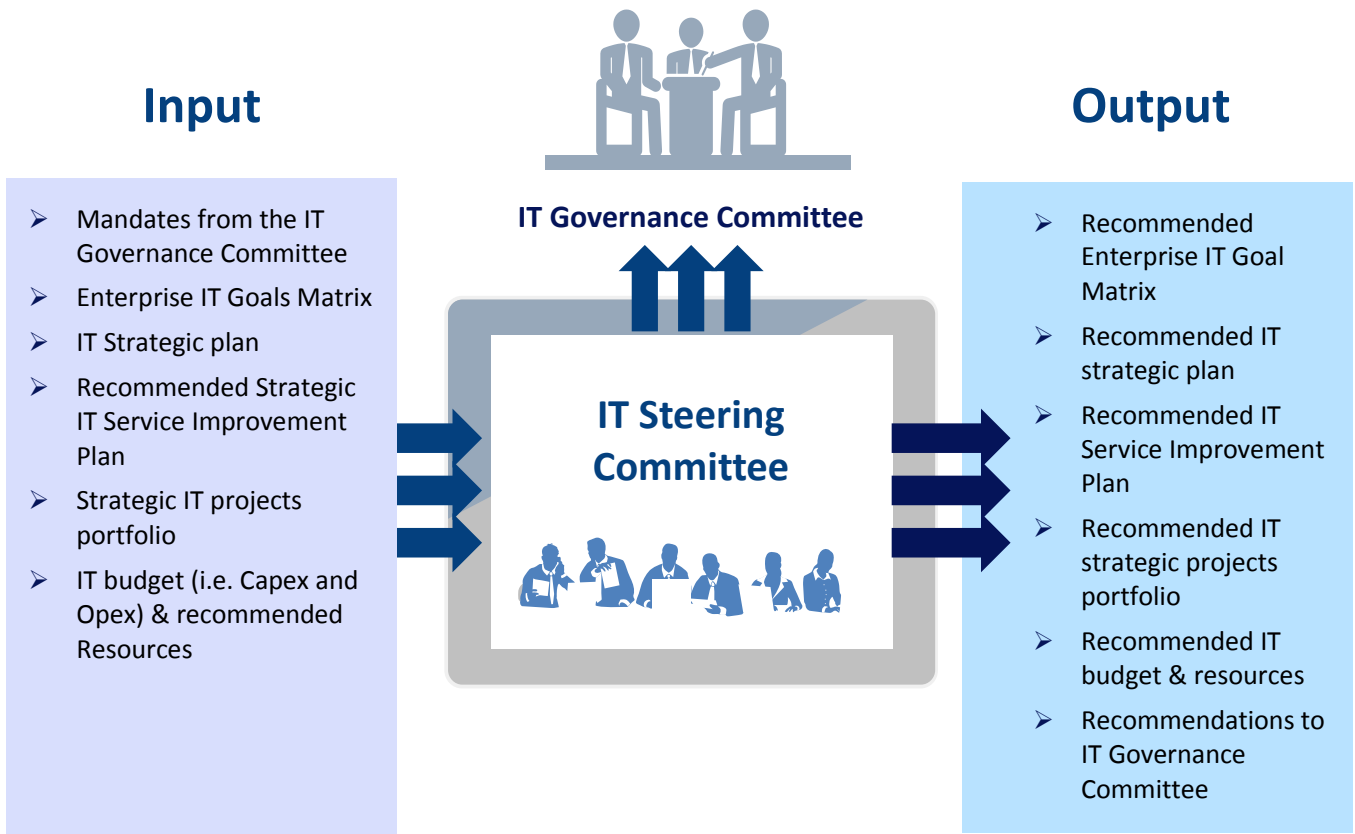**Meeting Frequency:** The IT Steering Committee meets on a quarterly basis or as required.

**The IT Steering Committee aims to achieve the following objectives:**

1. Ensure IT strategic goals are achieved.
2. Ensure IT programs/project are properly prioritized and executed in alignment with their business strategic purpose(s).
3. Optimize usage of IT resources.
4. Optimize IT risk management.

**Roles and Responsibilities:**

1. To establish annual plans required to achieve the bank's strategic objectives and to monitor the internal and external factors that may affect their completion.

2. To link the Enterprise Goals Matrix with the related IT Goals Matrix and endorse/regularly review the Enterprise IT Goals Matrix accordingly to ensure the achievement of the Bank's strategic objectives and Governance of Enterprise IT objectives as well. In addition to the consideration of defining and reviewing related metrics, and assign Senior Executive Management with the responsibility of the monitoring of these metrics on a continuous basis and to report to the committee of the metrics' status accordingly.

3. To recommend financial and non-financial resources required to achieve IT governance objectives. In addition to the utilization of competent human resources through organisational structures that formulate required processes to support IT governance objectives, while maintaining adequate segregation of incompatible duties and conflicts of interest. Further, to recommend the recruitment of the technological infrastructure and its related services to support IT governance objectives achievement. Lastly, to monitor IT Governance related projects and processes.

4. To prioritize the annual IT programs and projects portfolio.

5. To monitor IT services performance and provide recommendations to continually improve its effectiveness and efficiency.

6. To raise necessary recommendations to the IT Governance Committee, on the following:
   ➢ Allocation of resources and enablers to achieve IT governance objectives.
   ➢ Deviations that may adversely affect the achievement of strategic objectives.
   ➢ Unacceptable IT and IS risks.
   ➢ Actions to enhance resources, projects and Information technology performance and compliance levels.

7. To report to the IT Governance Committee through formal minutes of meeting.

البنك العربي
ARAB BANK

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



## Input

**IT Governance Committee**

## Output

- ➢ Mandates from the IT Governance Committee
- ➢ Enterprise IT Goals Matrix
- ➢ IT Strategic plan
- ➢ Recommended Strategic IT Service Improvement Plan
- ➢ Strategic IT projects portfolio
- ➢ IT budget (i.e. Capex and Opex) & recommended Resources

**IT Steering Committee**

- ➢ Recommended Enterprise IT Goal Matrix
- ➢ Recommended IT strategic plan
- ➢ Recommended IT Service Improvement Plan
- ➢ Recommended IT strategic projects portfolio
- ➢ Recommended IT budget & resources
- ➢ Recommendations to IT Governance Committee

**Illustrative Graph (3): IT Steering Committee Typical Inputs and Outputs**

# 4. Regulatory Compliance and Reporting

## 4.1. Commitment to laws and regulations related to IT Goverancne processes objectives

The Board and Senior Executive Management are committed to ensure compliance with Central Bank of Jordan's regulation for the Governance and Management of Enterprise IT (65/2016), as well as complying with the regulation-derived internal policies and procedures.

## 4.2. Annual Reporting

The Bank is committed to disclose the existence of the "IT Governance and Management Manual" within the Bank's annual report and to publish it on the Bank's website accordingly.

## 4.3. Internal & External Audit

➢ Internal and external risk-based IT audits shall be conducted in alignment with the CBJs IT Governance and Management regulation (Regulation No: 65/2016).

➢ Internal and external auditors shall comply with the latest version of IT Assurance Framework International Standard (ITAF) issued by ISACA.

➢ The Audit Committee and the external auditor shall provide the CBJ with the annual internal and external IT audit reports during the first quarter of every year.

# 5. Principles & Enablers

## 5.1. Principles of IT Governance and Management:

Core principles of Arab Bank's IT governance and management system are built on the COBIT 5.0 Governance of Enterprise IT principles as follows:

1. Meeting the stakeholder needs by creating value for stakeholders and by maintaining a balance between risk optimization, resource utilization and realization of benefits.
2. Separating governance and management responsibilities by differentiating between each levels' and committees' roles and responsibilities.
3. Covering the enterprise end to end which requires the commitment of the Board and Management as follows:
   ➢ The Board level via a stable IT governance system with the objective to achieve stakeholder needs.
   ➢ The Management level via implementing Board level directions through the operation and execution of the agreed on objectives and lastly reporting on the status of operation and execution activities to the Board level.
4. The application of a single integrated framework in alignment with relevant international standards and leading practices.
5. Enabling a holistic approach to IT governance and management through the 7 enablers which include:
   ➢ Principles, policies, and frameworks;
   ➢ Processes;
   ➢ Organization Structures;
   ➢ Culture, Ethics, and Behaviour;
   ➢ Information;
   ➢ Services, Infrastructure, and Applications; and,
   ➢ People, Skills, and Competencies.

Enablers

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

## Enabler 1: Principles, Policies, and Frameworks

The Board or delegated committees endorses "principles", "policies" and "frameworks" to achieve IT Governance objectives and requirements. These Policies should be effective, efficient and should include compliance requirements related to improvement, updates, clarity, flexibility, completeness and alignment with international leading practices. Each policy should include information about the ownership, scope, update periods, access authorities, circulation requirements, objectives, responsibilities, associated procedures and disciplinary actions in case of non-compliance in addition to compliance review mechanisms.

## Enabler 2: Processes

The Board or delegated committees endorses governance processes to deliver its desired outcome.

ARAB BANK البنك العربي

## Enabler 3: Organizational Structures

The Board endorses Organizational Structures (hierarchies and committees) that meet with the requirements of IT Governance processes while maintaining adequate segregation of incompatible duties, ensuring independence, applying dual control, and maintaining up-to-date job descriptions.

## Enabler 4: Culture, Ethics, and Behaviour

The Board or delegated committees endorses an enterprise code of conduct that reflects the professional and ethical rules in alignment with acceptable international behaviour rules and it shall clearly state the desirable and undesirable behaviours and consequences of conduct. Further, the board employs diversified mechanisms to encourage desirable behaviours and to avoid undesirable behaviours.

## Enabler 5: Information

The Board or delegated committees endorses an information and reporting matrix, and shall assign 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.

## Enabler 6: Services, Infrastructure, and Applications

The Board or delegated committees endorses appropriate services, infrastructure and applications matrix to support IT governance processes and practices and shall ensure that the matrix is regularly updated and enhanced to accommodate the enterprise objectives and processes improvement in alignment with international leading practices

## Enabler 7: People, Skills, and Competencies

The Board or delegated committees endorses a competency matrix and human resources policies required to achieve governance processes requirements. The Senior Executive Management shall employ qualified human resources and qualify current human resources through training and continuous education programs to achieve governance processes objectives and requirements. Further, Senior Executive Management ensures that annual cadres' performance evaluation mechanisms include objective key performance indicators that considers enterprise goals achievement.

Section 3

Appendices

ARAB BANK

# Appendix I: Definitions

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

1. **IT Governance and Management:** A systematic approach towards structuring the alignment between business and IT to achieve enterprise needs via optimizing resources, optimizing risks, and realizing benefits.

2. **COBIT:** 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.

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

4. **Senior Executive Management:** Comprised of Chief Executive Officer (CEO), deputy CEO, Chief Financial Officer (CFO), Chief Operations Officer (COO), Chief Risk Officer (CRO), Chief Compliance Officer (CCO), and Head of IT whereby this body is responsible for planning, building, running, and monitoring activities in alignment with the direction set by the governance body to achieve enterprise objectives.

5. **IT Governance Committee:** A group of appointed individuals comprising of 3 board members that has the overall responsibility to govern Information Technology (IT) activities and align them to the bank's strategic direction.

6. **IT Steering Committee:** A group of appointed individuals comprising of the CEO (chair of the committee), DCEO, COO, CRO, Head of IT, and observers whom of which include one board member and Head of Internal Audit. This committee has the overall responsibility of providing recommendations, decision making, driving IT related initiatives to ensure business and IT alignment, IT resources and IT risk management optimization.

7. **COBIT 5.0 Five Principles:** Five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimizes information and technology investment and use for the benefit of stakeholders. These 5 principles include:
   ➢ Meeting the stakeholders needs.
   ➢ Covering the Bank end-to-end.
   ➢ Applying a single integrated framework.
   ➢ Enabling a holistic approach.
   ➢ Separating governance from management.

8. **COBIT 5.0 Seven Enablers:** 7 enablers/factors that individually and collectively influence the enablement of COBIT 5.0 processes. These 7 enablers include:
   ➢ Principles, policies, and frameworks.
   ➢ Processes.
   ➢ Organizational Structures.
   ➢ Culture, ethics, and behaviour.
   ➢ Information.
   ➢ Services, infrastructure, and applications.
   ➢ People, skills, and competencies.

البنك العربي
ARAB BANK