IT Governance and Management Manual

March 2017

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 and to create a balance between benefit realizations, risk optimization and resource utilization.
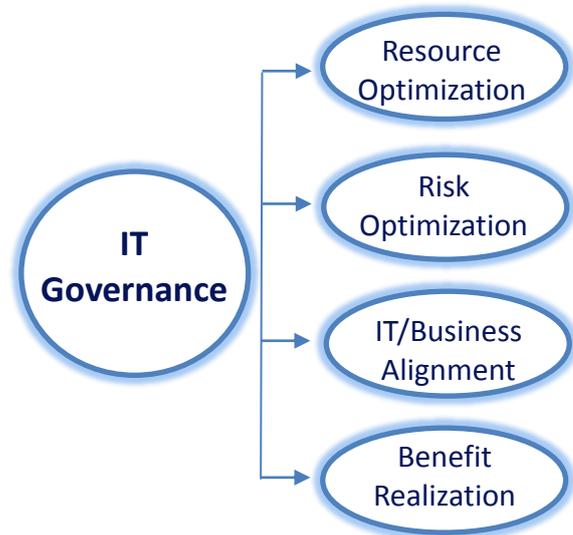
1.2 IT Governance and Management Objectives:

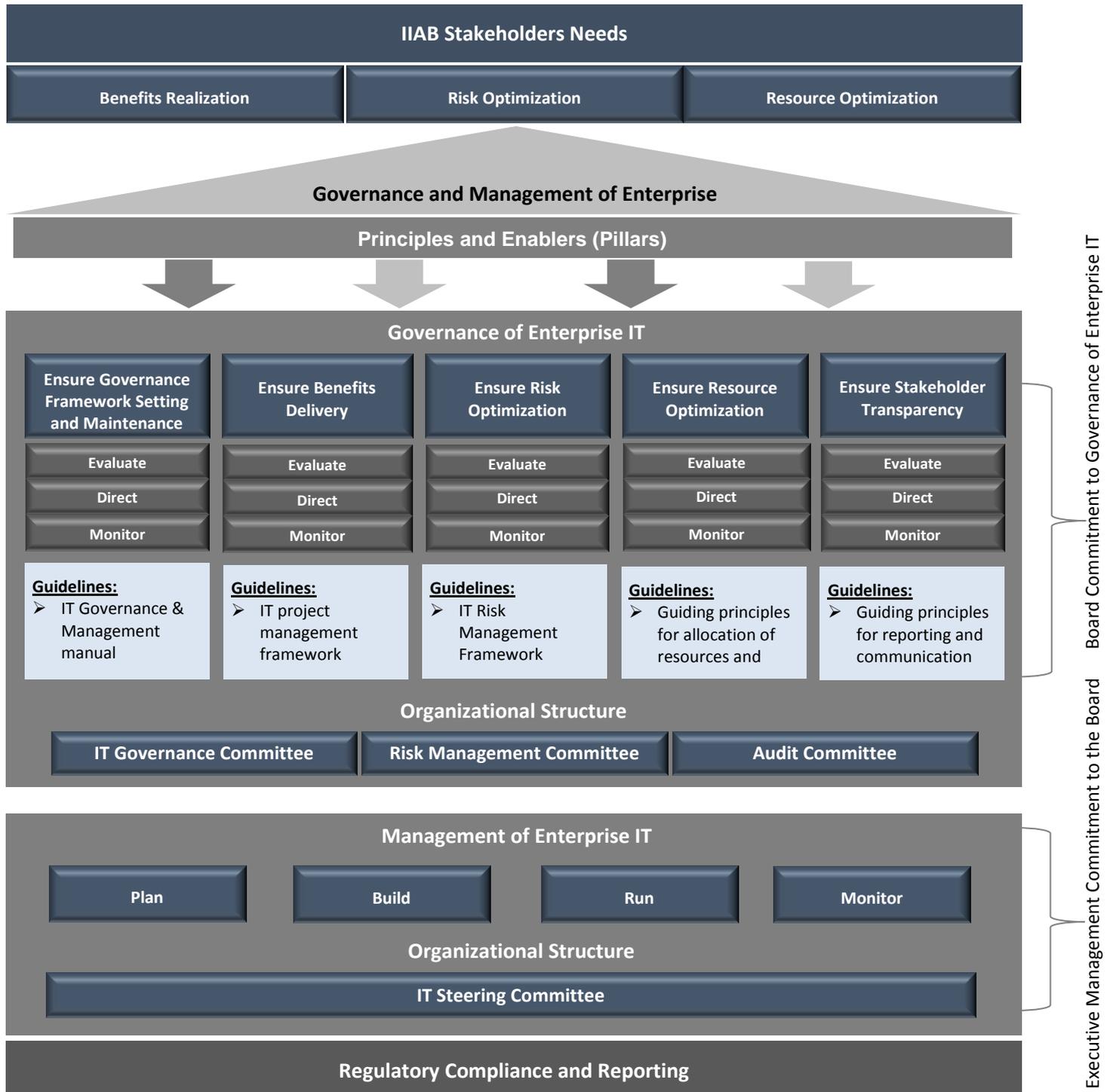The IT Governance and Management framework aims to achieve the following objectives:

1. Align IT goals with business goals.

2. Meet stakeholders' needs by creating a balance between the benefit realization, risk optimization and resources optimization.

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

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

5. Establish technology 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 and operations.

7. Comply with external and internal regulations and requirements.

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

9. Manage third parties/vendors relationships.

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 5.0 framework and principles:


IIAB Stakeholders Needs

| Benefits Realization | Risk Optimization | Resource Optimization |

Governance and Management of Enterprise

Principles and Enablers (Pillars)

Governance of Enterprise IT

Ensure Governance Framework Setting and Maintenance	Ensure Benefits Delivery	Ensure Risk Optimization	Ensure Resource Optimization	Ensure Stakeholder Transparency
Evaluate	Evaluate	Evaluate	Evaluate	Evaluate
Direct	Direct	Direct	Direct	Direct
Monitor	Monitor	Monitor	Monitor	Monitor
Guidelines: ➤ IT Governance & Management manual	**Guidelines:** ➤ IT project management framework	**Guidelines:** ➤ IT Risk Management Framework	**Guidelines:** ➤ Guiding principles for allocation of resources and	**Guidelines:** ➤ Guiding principles for reporting and communication

Organizational Structure

| IT Governance Committee | Risk Management Committee | Audit Committee |

Management of Enterprise IT

| Plan | Build | Run | Monitor |

Organizational Structure

| IT Steering Committee |

Regulatory Compliance and Reporting

Board Commitment to Governance of Enterprise IT

Board Commitment to the Board

Senior Executive Management Commitment to Governance of Enterprise IT

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. 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 Allocation of Resources and Capabilities";
4. Ensure Benefits Delivery by endorsing the "Project Management Framework"; and,
5. Ensure Stakeholder Transparency by endorsing "Guiding Principles for Reporting and Communication".
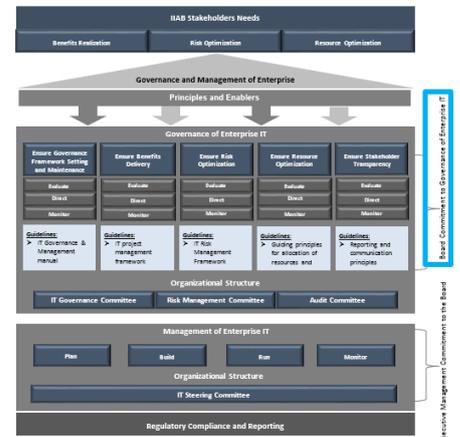
3.2 Organization Structure:

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**

The IT Governance Committee is established to support the Board in enabling the Governance of Enterprise IT practices. The following section includes details on its scope, purpose, members, meeting frequency, objectives and detailed roles and responsibilities.
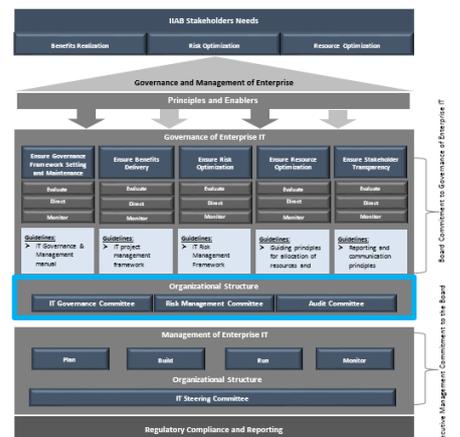
3.3 IT Governance Committee:

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.

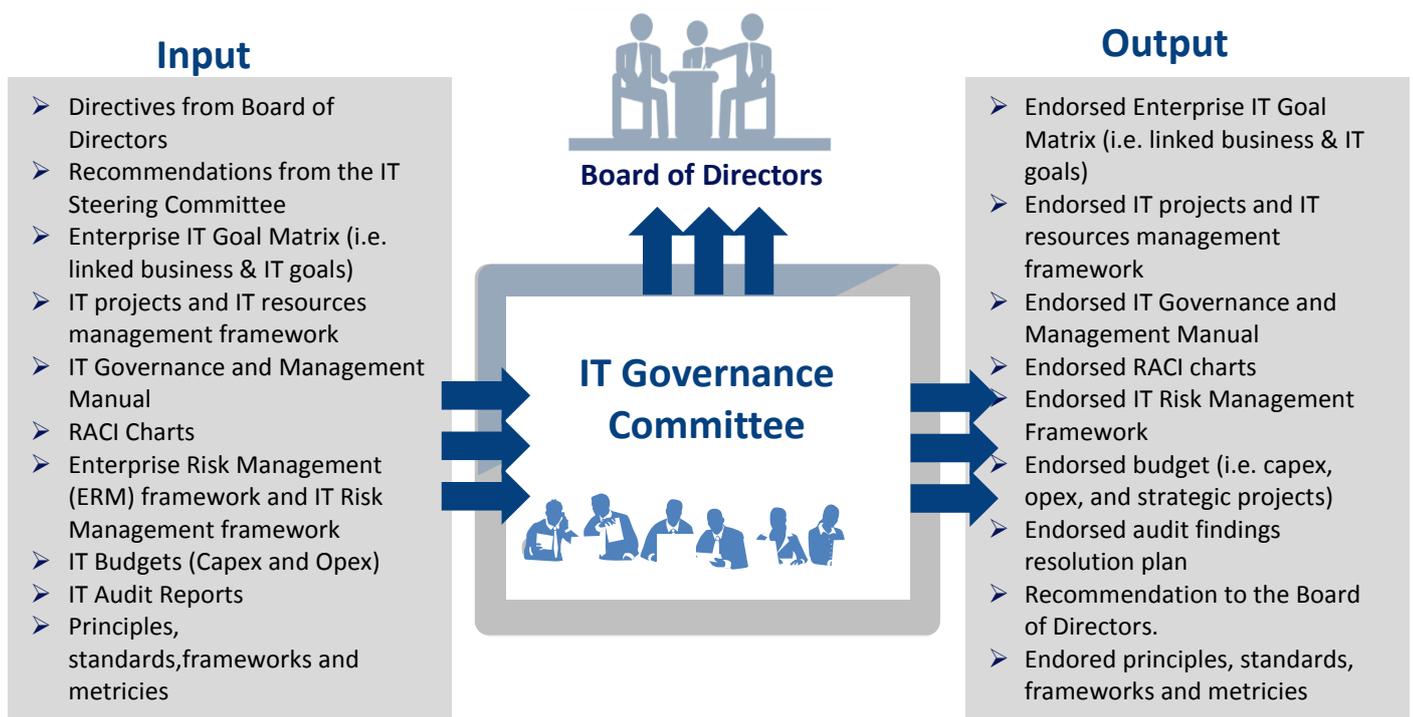**The IT Governance Committee aims to achieve the following objectives:**

1. Ensure Governance Framework Setting and Maintenance;

2. Ensure Risk Optimization;

3. Ensure Resource Optimization;

4. Ensure Benefits Delivery; and,

5. Ensure Stakeholder Transparency.

Roles and Responsibilities:

1. To endorse IT strategic 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 IT Goal Matrix that links business and IT related goals & sub goals.

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

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

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

8. 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.

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

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

11. 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 processes.

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

- IT Human Resources Policy and Competency Matrix covering the IT governance processes 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

- Directives from Board of Directors
- Recommendations from the IT Steering Committee
- Enterprise IT Goal Matrix (i.e. linked business & IT 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 metricies

Board of Directors

IT Governance Committee

Output

- Endorsed Enterprise IT Goal Matrix (i.e. linked business & IT 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 IT 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.
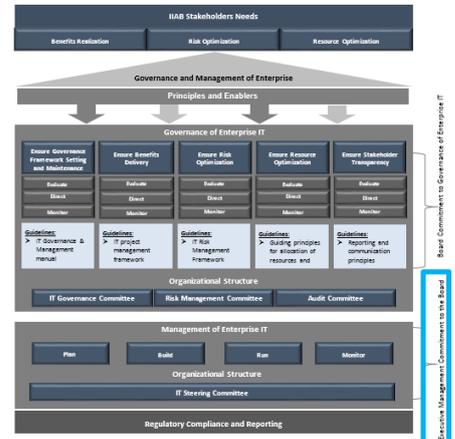
4.2 Organizational Structure:

The IT Steering committee is established to support the IT Governance Committee to enable the Governance of Enterprise IT. The following section includes details on its scope, purpose, members, meeting frequency, objectives and detailed roles and responsibilities.
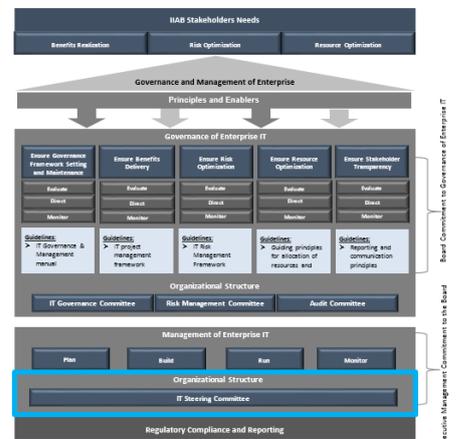
4.3   IT Steering Committee:

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;
➢ Information Security and Business Continuity Manager;
➢ Head of Enterprise Project Management Office & Enterprise Architecture; 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.

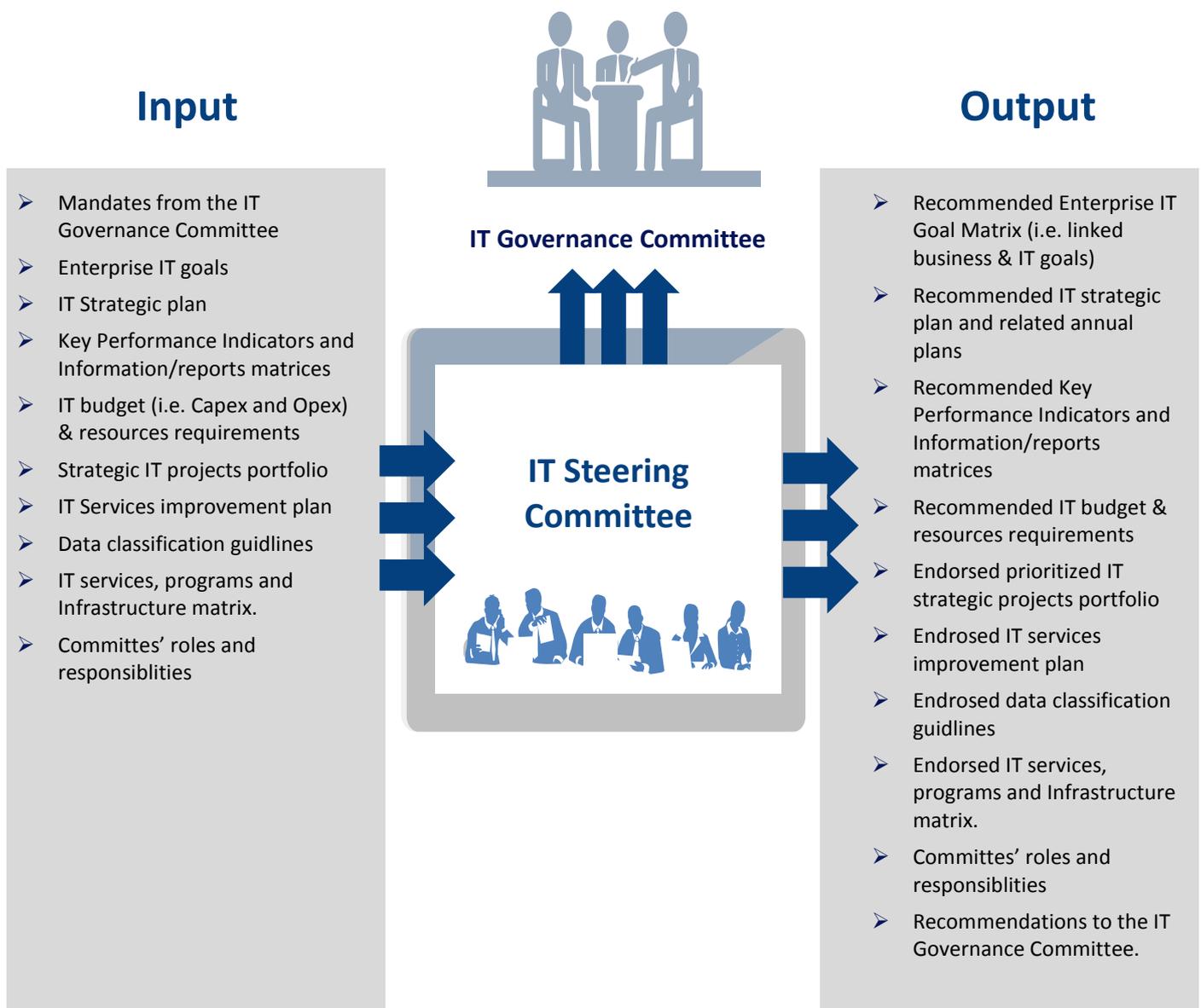**The IT Steering Committee aims to achieve the following objectives:**

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. Ensure IT risk optimization.

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 IT 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 processes' 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 adopted by the bank and CoBIT 5.0 guidelines (CoBIT 5 – Enabling Information).

10. To approve the IT services, programs, and infrastructures matrix required to support the IT Governance and Management processes.

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

IT Governance Committee

IT Steering Committee

Output

- ➢ 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 IT 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**

10

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.

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.
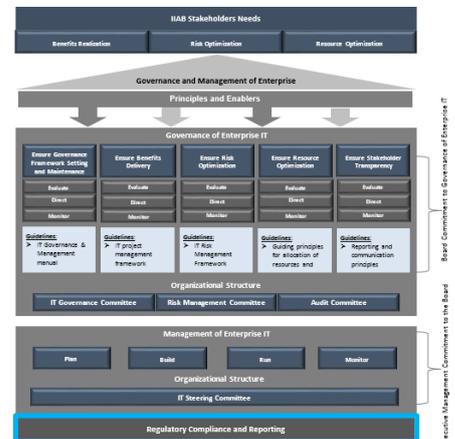
5.2 Reporting:

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).
➢ Ensure that the audit charter scope includes IT Governance and Management processes in line with the CBJ regulation (Regulation No: 65/2016).
➢ 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.

5.2.4 External Audit Reporting

➢ The Bank's external auditor shall perform risk based independent review(s) of the IT Governance and Management processes, 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.
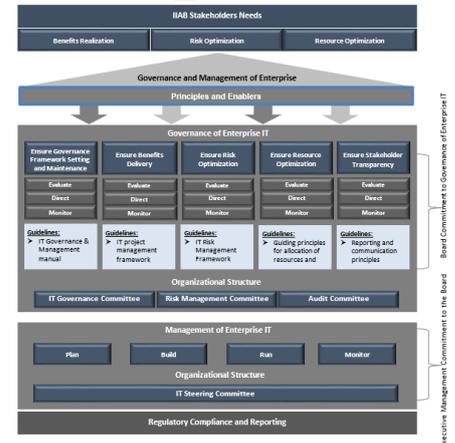
Principles and Enablers

6. Principles & Enablers (Pillars)

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 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 level's roles and responsibilities and related committees.

3. Covering the Bank from end to end which includes requires the commitment of the Board and Senior Executive Management as follows:

    ➢ 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.

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 provisioning and development of 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.

6.2   Enablers (Pillars)

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

Enabler 1: Principles, Policies, and Frameworks

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.

Enabler 2: Processes

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

Enabler 3: Organizational Structures

The Board or mandated committees 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.

Enabler 4: 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.

Enabler 5: Information

The Board or mandated committees shall endorse an 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.

Enabler 6: Services, Infrastructure, and Applications

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

Enabler 7: 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.
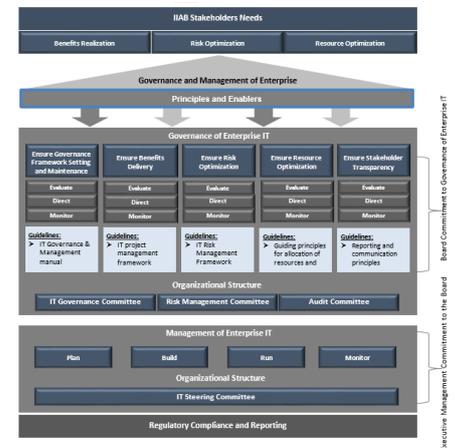
Appendices

Appendix I: Definitions

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

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

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. **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.

5. **Assets:** are defined as any resource or any quality that has value to the bank (e.g. hardware, information, infrastructure, people, resources and outsourced services).

6. **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.

7. **IT Steering Committee:** A group of appointed individuals comprising of the CEO (chair of the committee), deputy CEO, Chief Operating Officer, Chief Risk Officer, 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, and optimize value from IT resources and optimize IT risks.

8. **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 enterprise end-to-end.
   - Applying a single integrated framework.
   - Enabling a holistic approach.
   - Separating governance from management.

9. **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.