ESORFRANKI LIMITED
(Reg No 1994/000732/06)
("the Company")

INFORMATION TECHNOLOGY GOVERNANCE FRAMEWORK

1. Introduction

The need for a well governed IT function is becoming more apparent as business leaders are forced to critically evaluate their cost and value chains in challenging economic environments. Additionally, their compliance, audit, risk and security environments are becoming the focus of attention in a world where regulatory compliance can fundamentally impair or enable the operations of a business.

IT governance is a subset discipline of corporate governance focused on IT systems and their risk and performance management. The rising interest in IT governance is partly due to compliance initiatives, for instance the King III Act, as well as the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization.

A characteristic theme of IT governance discussions is that the IT capability can no longer be a black box to the business. The traditional involvement of board-level executives in IT issues was to defer all key decisions to the company's IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers, and in particular departments such as finance, have the necessary input into the decision making process. This prevents IT from independently making and later being held solely responsible for poor decisions. It also prevents critical users from later finding that the system does not behave or perform as expected.

2. Purpose of this document

The purpose of this document is to provide Esorfranki with an overarching IT governance framework that will assist in ensuring that the IT processes deployed at Esorfranki are managed in controlled and effective manner and is able to support Esorfranki's business goals and objectives.

The following components are expected to be inherent to any IT governance framework and have been used as basis to tailor this document:

- The definition of IT governance;
- An overview of the IT governance framework;
- A list of the IT processes embedded within the IT environment;
- Overview of the roles and responsibilities of key forums or entities as it pertains to IT
- A view of the IT controls framework to be adopted for the IT environment;
- An overview of the policy framework managing the implementation of the IT governance framework; and
- The reporting structures defined for IT.

In the remaining sections of this document, the IT governance framework is defined based on these principles but tailored to the Esorfranki business goals, IT goals and the risk and control maturity of the environment.

2.1. Scope of the document

The following is included to the scope of this document:

- An overview of the IT governance framework deployed or in the process of being deployed within the Esorfranki IT environment;
- A prioritised list of IT process relevant to the Esorfranki IT environment;
- A policy framework that forms a subset of the overall IT governance framework;
- The reporting structure and associated reporting content applicable to the Esorfranki IT environment;
- The policy statements with regard to the update and review of the IT governance framework; and
- The high level roles and responsibilities of the CIO or equivalent staff member based on the risk, control and performance considerations for the IT environment.

2.2. Exclusions of the document

The following is excluded from the scope of this document:

- The IT strategy and related initiatives (this would be included in the IT strategy document);
- The IT tactical or operational plans (these are operational documents that are deployed to support the IT strategy document but are aligned to the IT requirements); and
- The detailed IT policies and procedures governing the IT operations.

3. The definition of IT governance

IT governance is a set of business processes that imposes management and control disciplines on IT activities to help ensure the integrity and protection of IT operations and the achievement of targeted business goals.

IT governance consists of the following key principles:

- An integral part of corporate governance;
- The responsibility of board members and executives;
- A mechanism to deliver value, manage performance, and mitigate risk;
- A method to assign accountability for decisions and performance; and
- Policies, procedures, management committees, performance metrics, and related management techniques working in unison toward common business goals.

4. King III requirements

The King III Code of Conduct was released on 1 September 2009. The revision was necessitated by the Companies Act of 2008 which has incorporated many of the principles contained in King II. The key enhancements in King III are a focus on sustainability, a risk-centric approach to governance and recognition of IT governance as a strategic component of Corporate Governance.

King III requires that the governance of IT is represented on a Board, as well as an Audit Committee level, due to its pervasiveness in business. IT is recognised as an integral part of business and a strategic corporate asset that carries significant risks. IT decisions, accountability, policies, standards, controls, procedures and reporting are required to be far more formalised and embedded in the organisation than ever before.

A proper IT governance framework is essential, as the Board will have to demonstrate how it has fulfilled all of these new responsibilities.

Chapter 5 of the King III Acts contains the following 7 principles that specifically relate to IT:

- Board Responsibility (the Board should be responsible for IT governance)
- Performance & Sustainability (IT should align with the performance & Sustainability objectives of the company);
- IT Governance Framework (The Board should delegate to management the responsibility for the implementation of an IT governance framework)
- IT Investments (The Board should monitor and evaluate IT Investments and expenditure)
- Risk Management (IT should form an integral part of the company's risk management)
- Information Security (The Board should ensure that Information Assets are managed effectively)
- Governance Structure (A risk committee and audit committee should assist the board in carrying out its IT responsibilities)

5. Addressing the King III requirements

As part of the approach for defining and reviewing the IT governance framework, the King III specific requirements have been addressed in the following manner:

Principle	Esorfranki inclusion \ consideration
Board responsibility	• Independent assurance on the effectiveness of the IT internal controls will need to be scoped by the internal audit function and agreed with management. • The implementation plan to be developed for the IT governance framework will be need to consider raising awareness of the framework and it's principles at the appropriate level of management and reporting structures. • The IT internal control framework will be aligned to the IT processes that have been prioritised within the governance framework (this control framework will need to re-assessed when the process priorities change)
Performance & sustainability	• The IT strategy has been informally defined but will need to be formally defined in order to address the "Business Goals" component of the proposed IT governance framework. • The reporting on IT matters to the Board will be aligned to what has been prescribed in the IT governance framework.
IT governance framework	• The CFO is accountable and the CIO or IT manager is responsible for the implementation of the IT governance framework. • The combination of the informal IT operations meetings and the formal Shared Service Centre Steering Committee will serve as the forums to achieve the desired mandate of an IT steering committee. • The CIO or IT manager will be responsible for the management of IT and will use the IT governance framework and its associated roles and responsibilities as a basis for fulfilling that role.
IT investments	• IT investments (both CAPEX and OPEX) will be approved and monitored by the CFO and/or Board based on the relevant delegation of authority. • Reporting on significant IT expenditure will be included in the reporting element of the IT governance framework.
Risk management	• Where significant, the assessment of IT risks will be included as part of the company risk management function. • The CFO will be accountable for ensuring the continuity of IT services whilst the CIO or IT manager will be responsible for the

Principle	Esorfranki inclusion \ consideration
	implementation and provision of the IT continuity services.
Information security	• The CIO or IT manager will be responsible for the implementation, monitoring and updating of the information security policies, procedures and systems. • The classification of information assets will be driven by the CIO or IT manager but responsibility will lie with the individual information asset owners.
Governance structures	• All significant IT risks will be reported to the Audit, Risk and Ethics Committee. • Independent assurance around the IT control environment will need to be reported to the Audit, Risk and Ethics Committee.

6. The approach adopted

A key principle of the IT governance framework is that although the framework structure and components may remain rigid, the priorities defined in the framework will need to be re-assessed from time to time in order to ensure the framework is addressing the key risk, control and performance considerations of the Esorfranki IT environment.

Within this context, the following approach was adopted in developing the IT governance framework for Esorfranki:

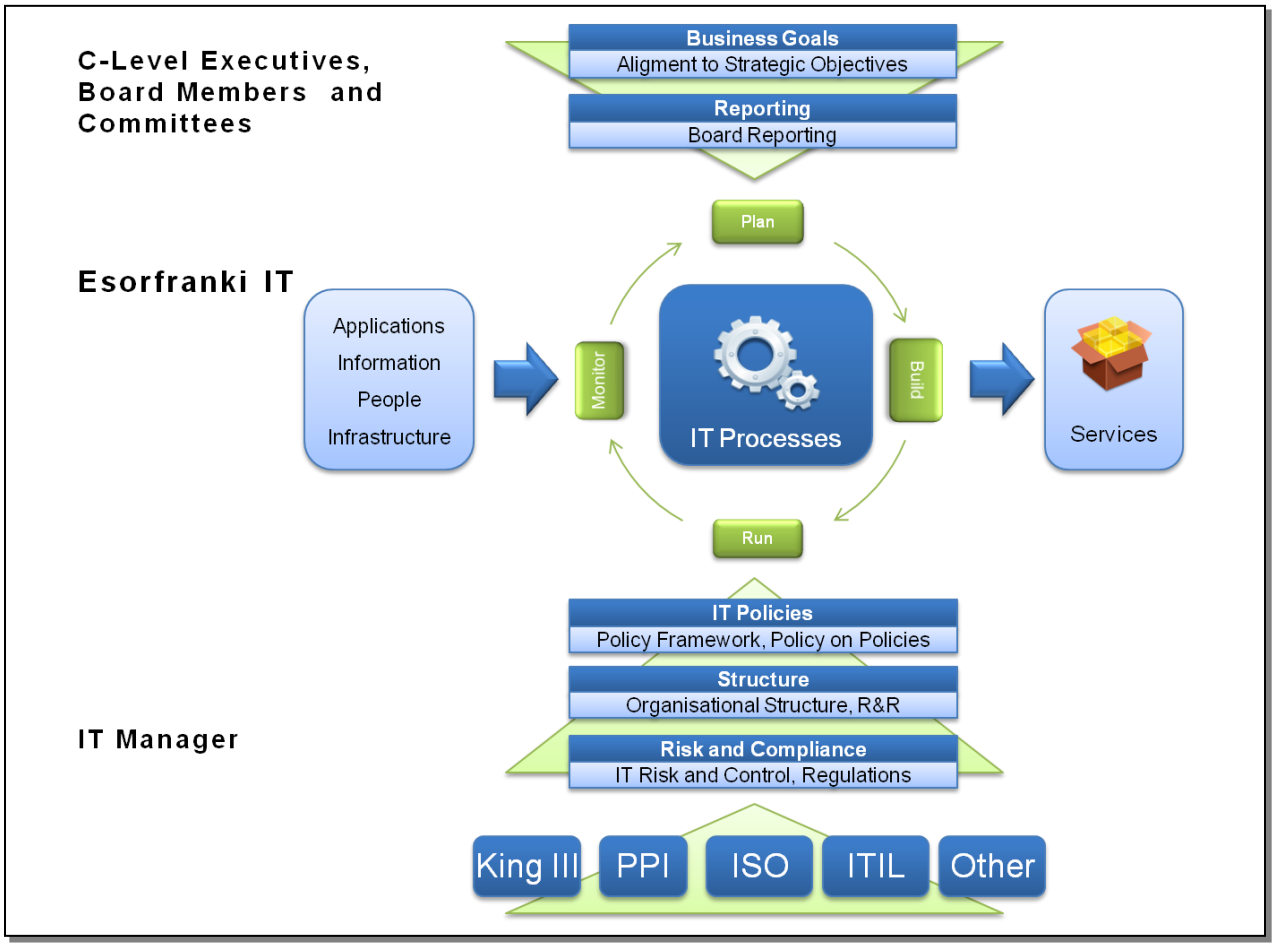
- The current IT environment was assessed based in the following components:
  - The inherent risk relating to use of IT by the key business processes was assessed (e.g. dependence on IT, reliability of the IT systems, level of changes to IT, etc);
  - The IT controls in place to mitigate this risks were considered (e.g. change control procedures, IT strategy documents, IT policies); and
  - The performance requirements for the IT processes that are driven by the keys business goals and objectives of the company were considered.
- The priority of the IT processes was defined based on the risk, control and performance elements defined above; and
- The IT governance framework was defined in terms of processes, reporting, alignment to business goals, risk and compliance, IT policy framework and roles & responsibilities requirements.

The results of this approach are contained in the “IT Governance Framework” presentation completed by Esorfranki management.

7. Esorfranki IT governance framework

7.1. Framework overview

The diagram below is a graphical representation of the IT governance framework adopted by Esorfranki:



An IT governance framework is constituted of various artefacts, such as processes, structures, roles and responsibilities, lifecycles and policies. The Esorfranki IT Governance framework incorporates these fundamental components to ensure a comprehensive, practical framework that is customised to the environment, integrated into the key business objectives, managed across all stakeholders and monitored for compliance and performance.

Below are descriptions of the key components of the Esorfranki IT Governance Framework:

Framework Component	Description	Key Stakeholders
Business goals	The key business goals for Esorfranki were taken into consideration when formulating the framework. This was done to ensure that the strategic direction and operational activities of IT alike were aligned with the	C-Level Executives, Board Members and Committees

Framework Component	Description	Key Stakeholders
	strategy and performance requirements of the overall business.	
Reporting	One of the key outputs of a governance framework is a reporting structure that delivers information on the key control and performance areas to the correct stakeholders.	C-Level Executives, Board Members and Committees
IT Processes	IT governance is driven into the operational areas of Esorfranki through the implementation, formalisation and monitoring of practical, relevant IT processes. These IT processes have been derived based on the control and performance requirements of the organisation and are formulated based on standard practice governance frameworks. These processes are categorised against the four fundamental lifecycle steps of an IT process environment, namely Plan, Build, Run and Monitor. This ensures that their intention is easily understood and can be contextualised in a simple way.	IT Manager or CIO
IT Policies	A well formed IT Policy framework is an important component to drive a common understanding of the IT Governance requirements into the organisation. This assists in ensuring uniform communication and giving a baseline for compliance testing and audits. Additionally, it allows a central point of control to ensure that the governance requirements are up-to-date and well understood.	IT Manager or CIO
	Based on the recommended IT processes and good practice guidelines, an organisational structure and roles and responsibilities will need to be defined to support the execution and reporting of the governance framework. These roles and responsibilities will be aligned where possible with the current structure and suggested roles that currently don't have a custodian will need to be highlighted.	IT Manager or CIO
Risk and Compliance	Management of risk and ongoing monitoring of compliance with external legislative and regulatory standards are critical in ensuring good IT governance. The framework would need to take into account various	IT Manager

Framework Component	Description	Key Stakeholders
	guidelines and standards, such as King III, ISO27002, PoPI and COBIT. Additionally, processes will need to be implemented within the framework to guide continuous assessment of any external requirements to ensure compliance.	

7.2. Business goals

As part of defining which IT process and related internal controls should be prioritised within the IT governance framework the key business goals and objectives of Esorfranki where considered, namely:

- Esorfranki is in the process of standardising business processes across the group;
- There is a strong drive to reduce internal costs (overhead); and
- The provision of sound corporate governance is seen as strategic consideration.

Going forward, the business goals of the organisation need to be considered within the framework as part of the following activities \ components:

- Whenever the IT governance framework is reviewed;
- As part of the reporting structure defined with the IT governance framework;
- As part of the CFO's accountability and the CIO or IT manager responsibility for the strategic alignment of IT;
- As part of the IT processes supporting the IT governance framework (e.g. defining an IT strategic plan, determining technological direction, communicate management aims and direction);

7.3. Policies

The policy component of the framework consists of the following key components:

- A policy framework defining the policy universe to ensure completeness;
- The detailed policies and procedures supporting the policy framework;

The CFO is accountable for both components whilst the CIO or IT manager is responsible for the execution and monitoring of the components.

7.4. IT processes

Based on the approach adopted for defining the IT governance framework the following processes were defined as high priority items:

- Define and manage service levels that are between Esorfranki and its service providers as well as between business and IT within Esorfranki;
- The management of third party service providers;
- Provision of IT governance processes, structures and reporting;

- Ensuring appropriate systems security controls are embedded within company policies;
- A IT strategic plan is defined to ensure alignment to business goals;
- The management of IT resources in terms of succession planning and definition of roles and responsibilities;
- Monitoring and evaluation of IT internal controls; and
- Management of changes within the IT environment.

It is important to note that this list of IT processes are the ones that have been prioritised based on the risk, control and performance elements that were assessed as part of the approach. The accountability and responsibility of all IT processes reside with the Board, CFO, CIO or IT manager (e.g. ensuring the continuity of IT services, managing system data and integrity).

7.5. Structure

The following key entities \ forums \ individuals relate to the reporting elements of the IT governance framework:

Entity	Mandate in terms of IT
Audit, Ethics and Risk Committee	• The review of assurance provided around the IT internal control framework and the related findings. • Assessment of significant IT risk that should be mitigated and\or monitored.
Executive Committee	• Assessment of whether IT is delivering on its mandate in terms assisting in meeting Esorfranki's business objectives. • Monitoring of key changes in IT that could have a significant impact on Esorfranki. • Assessing the IT reporting provided as part of the IT governance framework.
Shared Service Centre Committee	• Review of the ability of IT to support the core business processes within Esorfranki and to identify areas of improvement;
IT Operations Meetings	• Monitoring and evaluation of the day-to-day IT operations with an emphasis on IT services and user demand \ requirements.
CFO	• Accountable for the definition of the IT mandate, goals and objectives as well as the implementation of these within the Esorfranki environment to ensure that they are aligned with the company's strategic objectives; • Responsible for the review of IT budget and expenditure;
CIO or IT manager	• Responsible for the execution of the IT strategy and IT governance framework and the management of the associated IT processes. • Responsible for the management of all third party service providers as part of the delivery of IT services.

Entity	Mandate in terms of IT
	• Responsible for interpreting the business requirements into technical specifications or services. • Responsible for management of the day-to-day IT operations.

8. Review and updating of the IT governance framework

The CFO is accountable to ensure that the accuracy and relevance of the IT governance framework is maintained. The CIO or IT manager is responsible for the execution of the processes required to maintain the accuracy and relevance of the of the IT governance framework.

The following events, triggers and/or principles will be used as a guideline for when the IT governance framework will be reviewed and/or updated:

- The framework should be formally reviewed at least once a year;
- The framework should be formally reviewed in the event there are significant changes to the IT environment (e.g. changes to the key processes, implementation of significant new systems, changes to key service providers);
- Feedback from the monitoring and evaluation activities should be considered when determining when the framework should be reviewed (e.g. internal audit, external audit, management self assessments);

APPROVED BY THE BOARD IN MARCH 2011.