EXECUTIVE OVERVIEW

IT GOVERNANCE

ALIGNED TO

KING III

Simon Liell-Cock
Julio Graham
Peter Hill
CISA CISM CGEIT

IT Governance Network
South Africa USA UK Switzerland
www.itgovernance.co.za
info@itgovernance.com
0825588732

7 September 2009
Version 1.00

Notices

Trademarks and service marks

CONTENTS

This page intentionally left blank.

1. Overview

1.1 Why is IT Governance important?

The third Report on Governance in South Africa has addressed the pervasive nature of information technology, its importance as part of the business strategy and the significant additional risks it introduces.
King III states that "the board should be responsible for IT governance". It is expected that through effective and responsible leadership information technology will be used to sustain and extend the company's business strategy and corporate objectives.

1.2 Who is affected?

The role and responsibilities of company directors, chief information officers and IT managers regarding information technology is clarified. The King III report states that the board is expected to provide leadership, ensure proper value delivery and effectively manage IT risks. Company executives are to become involved in IT steering and similar oversight committees.
The role of the Chief Information Officer will depend on the size of the company and the seniority of this position within the organisation. CIOs are expected to be the bridge between IT and the business and they can expect to be regular attendees of audit and risk committees. Where the CIO has received delegated responsibilities from the board, the CIO will be expected to take responsibility for the implementation and execution of IT governance.
IT management is expected to implement structures, processes and governance mechanisms for the effective and efficient management of information resources to facilitate the achievement of corporate objectives.

1.3 What is the focus of IT Governance?

IT governance is defined in the glossary to the King III Code of Governance as "the effective and efficient management of IT resources to facilitate the achievement of corporate objectives". It is about the governance of management processes (and decisions) relating to the information and communication services used by an organisation.
Typical outcomes of IT governance are:

- Strategic alignment with corporate objectives and the company's performance and sustainability goals
- Value delivery, optimisation of IT expenditure and proving the value of IT
- Risk management in support of the company's strategic and business objectives
- Resource management to optimise organisational knowledge and investments in IT resources
- Performance management to ensure that the company achieves its objectives, can be aligned with changes in strategic needs, judiciously manages IT risks and enables opportunities to be identified and acted on.

1.4 Application of the Code

King III applies to all entities regardless of the manner and form of incorporation or establishment. The 'apply or explain' basis allows every organisation to apply all the principles of the code as it best meets the objectives of the entity and to focus on the substance rather than the form of application. Effective date is March 1, 2010.

2. Board Responsibilities

2.1

Board and Management Responsibilities

The need for board level oversight of IT activities depends on the strategic importance of IT to the company and the organisational maturity of its IT management processes.

2.2 Leadership and Direction

Leaders are required to articulate the company's goals and vision, drive, guide and inspire. They direct company strategies and operations with a view to achieving sustainable economic, social and environmental performance.

The board is to:

- Place IT on the board agenda
- Clarify business strategies and objectives, and the role of IT in achieving them
- Delegate responsibility for implementing an IT governance framework
- Determine and communicate levels of risk tolerance/appetite
- Assign accountability for the organisational changes needed for IT to succeed.

2.3 Monitor and Evaluate

The board is to:

- Ensure that IT is aligned with corporate objectives
- Monitor and evaluate the extent to which IT actually sustains and enhances the company's strategic objectives
- Monitor and evaluate the acquisition and appropriate use of technology, process and people
- Ensure that an internal control framework has been adopted, implemented and is effective
- Use the risk and audit committees to assist the board fulfil its responsibilities
- Obtain project assurance from independent experts that IT management apply all basic elements of appropriate project management principles to all IT projects.
- Obtain independent assurance of the governance and controls supporting outsourced services.
- Monitor the application of King III governance principles by all parties, at all levels (starting with the board), at all stages of business operations, across organisational boundaries (including third parties) and for the acquisition and disposal of IT goods and services.

2.4 IT Reporting to the Board

Management should increase transparency and provide the board with complete, timely, relevant, accurate and accessible information about:

- The likelihood of IT achieving its objectives?
- IT's resilience to learn and adapt?
- The judicious management of the inherent risks from using IT, including disaster recovery?
- How well IT has recognised opportunities and acted on them?

The board should take steps to ensure that resources are in place to ensure that comprehensive IT reporting is in place, both to the board by management and by the board in the integrated report.

3. CIO Responsibilities

3.1 The Role and Responsibilities: Chief Information Officers

The board is to appoint a suitably qualified and experienced individual as the chief information officer who is expected to:

- Interact regularly on matters of IT governance with the board, or appropriate board committee, or both
- Understand the accountability and responsibility of IT
- Implement an IT Governance framework to deliver value and manage risk
- Implement an Accountability framework to assign decision-making rights
- Implement a suitable organisational structure and define terms of reference
- Incorporate IT into the business processes in a secure, sustainable manner
- Implement an ethical IT governance and management culture
- Implement an IT control framework
- Obtain assurance on the effectiveness of the IT control framework
- Implement processes to ensure that reporting to the board is complete, timely, relevant, accurate and accessible
- Implement a strategic IT planning process that is integrated with the business strategy development process
- Integrate IT plans with the business plans
- Define, maintain and validate the IT value proposition
- Align IT activities with environmental sustainability objectives
- Include relevant representation from the business in oversight structures
- Have regard for the legislative requirements that apply to IT
- Translate business requirements into efficient and effective IT solutions
- Support the business and governance requirements in a timely and accurate manner through the acquisition of people, process and technology
- Optimise resources usage, leverage knowledge
- Ensure that the business value proposition is proportional to the level of investment
- Deliver the expected return from IT investments
- Protect information and intellectual property
- Promote sharing and re-use of IT assets
- Monitor and enforce good governance principles across all parties in the chain from supply to disposal of IT services and goods
- Obtain independent assurance that outsourced service providers have applied the principles of IT governance
- Obtain independent assurance of the effectiveness of the IT controls framework implemented by service providers
- Obtain independent assurance that the basic elements of appropriate project management principles are applied to all IT projects
- Regularly demonstrate to the board that the company has adequate business resilience arrangements in the event of a disaster affecting IT
- Implement a risk management process based on the boards risk appetite
- Select and use an appropriate framework for managing risk (e.g. COSO)
- Comply with applicable laws and regulations
- Implement an IT controls framework
- Manage information assets effectively
- Implement an information security management system in accordance with an appropriate information security framework
- Provide the Audit and Risk Committees with relevant information about IT risks and the controls in place
- Measure, manage and communicate IT performance
- Report to the IT Steering Committee on IT performance.

Simon Liell-Cock
Julio Graham
Peter Hill
CISA CISM CGEIT

IT Governance Network
South Africa USA UK Switzerland
www.itgovernance.co.za
info@itgovernance.com
0825588732