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

This document is furnished “as is” without warranty of any kind. All warranties on this document are hereby disclaimed, including the warranties of merchantability and fitness for a particular purpose.

The information contained in this book could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication.

Trademarks and service marks

King III is a trademark of the Institute of Directors in South Africa. Control Objectives for Information and related Technology (CobiT®) and ISACA® are trademarks of ISACA and the IT Governance Institute. ITIL is a trademark of the Office of Government Commerce in the UK. COSO is a trademark of the Committee of Sponsoring Organisations of the Treadway Commission.

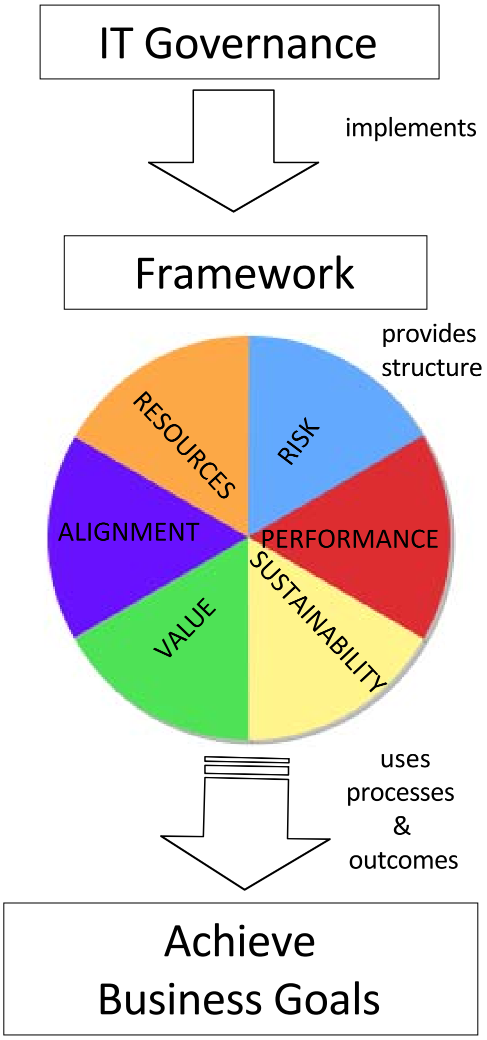
CONTENTS

Preface

A 2007 survey[1] commissioned by ISACA® found that while many IT functions had gone beyond being concerned only about the day to day operational activities and were addressing regulatory compliance requirements such as risk management and internal controls, less than fifteen percent were emphasising good governance and are able to effectively manage the delivery of value to the stakeholders.

In most organisations the goals and business benefits of IT are not defined upfront and CIOs do not have the mechanisms in place to be able to manage and measure the success of their IT function contributing to the creation of real value.

What Does This Book Contain?



The primary objective of this book is to show how IT Governance and the King III requirements are aligned and to describe the impacts of these on the board, CIO and IT organisation. The diagram shows the IT Governance topics covered by this book. Existing IT Governance models and standards have been referenced to assist clarification of concepts.

Who Should Read It?

An understanding of the integrated nature of IT governance and corporate governance, the scope of IT governance and the key activities will be of value to everyone participating in the management of IT and defining, developing, delivering, monitoring and evaluating IT services and solutions.

Board members wishing to better understand and apply the King III principles.

CIOs looking to institutionalise discipline and build capability, plan, prioritise and measure the performance of IT. It will enable them to clarify role descriptions, assign responsibilities and plan improvements.

IT management tasked with establishing governance mechanisms.

Auditors, compliance personnel and risk managers interested in IT governance.

This page intentionally left blank.

1. Introduction

IN EXERCISING THEIR DUTY OF CARE, DIRECTORS SHOULD ENSURE THAT PRUDENT AND REASONABLE STEPS HAVE BEEN TAKEN REGARDING IT GOVERNANCE.

1.1 Why is IT Governance important?

For the first time the King Committee on Corporate Governance has addressed the issue of corporate governance for information technology. In doing so 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.

Information technology is a big ticket item for most companies and can consume considerable resources with little real value being created. Few organisations have not experienced the disappointment of a failed IT project or dissatisfaction from poorly delivered services and support. Many organisations are all too familiar with the ever increasing cost of information technology not being matched with ever more effective IT solutions. Equally true is the tremendous impact information technology has had in enabling businesses to grow, reduce costs and improve performance.

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 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. In addition to ensuring that the risks and costs associated with IT are properly controlled, they are required to measure and manage IT performance and report the results to the board.

The ambiguity in the roles, responsibilities and reporting lines of risk managers, compliance officers and auditors has also been clarified in King III. For example, Internal Audit should not share the same reporting lines with Risk Management and these functions should not report to one another.

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 governance is the responsibility of the board and an integral part of corporate governance. It is about the governance of management processes (and decisions) relating to the information and communication services used by an organisation.

Governance differs from management in that it is about those activities that have an impact on achieving the organisation’s strategic goals. This involves evaluating and directing the use of IT to support the organization and monitoring the use of IT to achieve plans. Of concern is management's ability to direct and control the company's IT activities so as to sustain and extend the organisation’s strategies and objectives.

The challenge is to address stakeholder expectations when multiple business units "own" and "use" the same set of services (i.e. “shared services”) and where most applications are "owned" by individual business units that control the budget for design, development, and support (i.e. “federated system development”).

The first step towards better governance is to establish accountability. This requires an examination of the roles and responsibilities within the processes used for decision-making that can impact on the achievement of strategic goals.

The board provides leadership and delegates responsibility to the CIO to implement the organisational structure and processes to leverage IT resources and drive alignment, deliver value, manage risk, optimise resources and manage performance. People who are accountable for good governance are responsible for making the changes, when necessary, to deliver the performance expected by the Business.

Processes are defined to organise IT activities in a manner that is intended to be efficient and effective. Processes exist at various layers within the organisation and are influenced by the organisational structure and leadership provided. Implementing IT governance is iterative and occurs at the strategic, tactical and operational levels in line with stakeholder priorities.

Capability is developed to better govern people (i.e. roles), process and technology and requires the managing of outcomes consistent with measurable preconditions. The purpose is to institutionalise discipline and maturity in IT processes so as to gain greater control and economies in achieving the enterprise’s strategic goals.

Typical outcomes of IT governance are:

- Strategic alignment with corporate objectives and the company’s performance and sustainability goals
- Value delivery through the 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 How must King III be implemented?

In keeping with the countries of the Common Wealth and European Union, King III has not followed the US statutory regime of 'comply or else' for which there are legal sanctions for non-compliance. The King Committee on Corporate Governance recognised that the cost of compliance can be unreasonably burdensome and therefore has preferred the 'apply or explain' approach.

This means that where the collective wisdom of the board believes that following a recommendation of King III would not be in the best interests of the company, it can apply another practice to that recommended and give the reasons for applying the alternative. Paramount is what is in the best interest of the company, subject always to proper consideration for the legitimate interests of all stakeholders.

This implies that the implementation of King III must be appropriate and applicable to the IT organisation's size, role and legal obligations. Commonsense must prevail and suitable structures, processes and governance mechanisms deployed to achieve the organisation's strategies and objectives.

1.5 Good Governance and the Law

Corporate governance is the system by which organisations are directed and controlled and involves the establishment of organisational structures, processes and governance mechanisms.

The Companies Act requires that directors and management must discharge their fiduciary duties and act with care, skill and diligence.

In assessing the standard of appropriate conduct, a court will take into account all relevant circumstances, including what is regarded as the normal or usual practice in the particular situation.

1.6 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

IT GOVERNANCE IS THE RESPONSIBILITY OF THE BOARD

2.1 Board and Management Responsibilities

The board should specify the decision rights and accountability framework to encourage the desirable culture in the use of IT.

The board may appoint an IT steering committee with relevant representation from business and IT to assist with its governance of IT. A risk committee and audit committee should assist the board in carrying out its IT responsibilities. The CEO should appoint a suitably qualified and experienced person responsible for the management of IT, often called the chief information officer (CIO).

Typically, oversight bodies are established with clear terms of reference and appropriate membership from the business. The exact nature of the oversight authorities will vary between organisations. In larger organisations these oversight authorities may have accountability for:

- Governance, Strategy, Investment and Performance
- Service Management
- Solution Delivery
- Third-Party Management
- Architecture, Technical Support and Operations
- Risk, Compliance and Internal Controls
- Security and Business Continuity.

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. In deciding on delegating responsibility, the board should give consideration to the company's reliance on:

- cost-effective, uninterrupted, secure, smoothly operating technology systems
- competitive advantage through systems that provide new value-added services and products
- responsiveness to customers
- capital expenditure and corporate cost of strategic transformation
- innovation and large-scale expenditure on new technology.

2.2 Integral part of overall Corporate Governance

IT governance is not an isolated discipline but it is an integral part of overall corporate governance. The difference between IT governance and corporate governance is the resources being leveraged to achieve business objectives.

2.3 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.

King III requires ethical leadership from the board based on responsibility, accountability, fairness and transparency. Each director should discharge the moral duties of conscience, competence, commitment, courage and inclusivity of all stakeholders.

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 to management
- Determine and communicate levels of risk tolerance/appetite
- Oversee the development of the information security strategy and delegate its implementation to IT management
- Assign accountability for the organisational changes needed for IT to succeed.

2.4 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
- Use the risk and audit committees to assist the board fulfil its responsibilities
- Ensure that prudent and reasonable steps have been taken in regard to IT
- governance
- 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
- Ensure that information assets are managed effectively
- Protect information and intellectual property
- Ensure personal information is treated by the company as an important business asset
- Ensure information records provide adequate evidence of business activity
- 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
- Obtain project assurance from independent experts that IT management apply all basic elements of appropriate project management principles to all IT projects.
- Question the delivery of proper value in proportion to the investments made
- Ensure that the company's risk management includes IT risks

- Measure and evaluate the amount spent on and the value received from IT
- Assess the learning being retained from experiences (post implementation reviews, process refinement, improvements in capability)
- Assess the sharing and re-use being achieved
- Obtain independent assurance of the governance and controls supporting outsourced services.

2.5 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. Governance Framework

An IT governance framework assists those at the highest level of organisations ensure that IT use contributes positively to the performance of the organization and conforms with the company's obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of IT

3.1 Developing an IT Governance Framework

An IT governance framework comprises definitions, principles and a model for governing IT. The board should govern IT through three main tasks:

a) **Evaluate** the current and future use of IT, including strategies, proposals and supply arrangements (internal, external, or both).
b) **Direct** preparation and implementation of plans and policies to ensure that use of IT meets business objectives.
c) **Monitor** the performance of IT against plans and business objectives; and, that the use of IT conforms to internal policies and conforms to external obligations (regulatory, legislation, common law, contractual).

The risk of directors not fulfilling their obligations is mitigated by giving due attention to the model in properly applying the principles.

In evaluating the use of IT, the board should consider:

- the external or internal pressures acting upon the business, such as technological change, economic and social trends, and political influences.
- the current and future business needs such as maintaining competitive advantage,
- the specific objectives of the IT strategies and proposals they are evaluating.

Directors should assign responsibility for, and direct preparation and implementation of a management system of policies, processes, and structures that support IT governance.

Directors should ensure that the transition of projects to operational status is properly planned and managed, taking into account impacts on business and operational practices as well as existing IT systems and infrastructure.

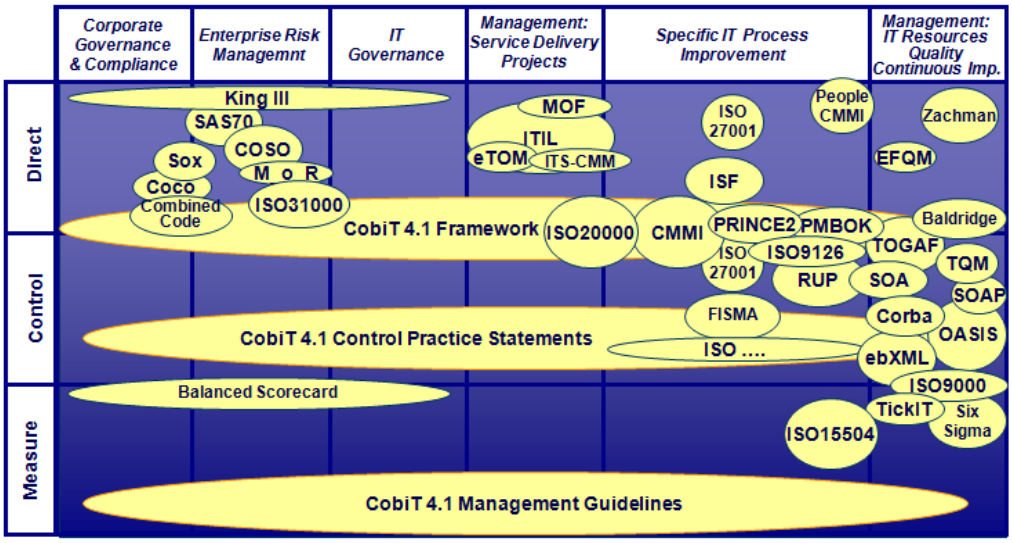
Directors should encourage a culture of good governance of IT in their organization by requiring managers to provide timely information, to comply with direction and to conform to the principles of good governance.

In deciding on an appropriate governance framework, the board should consider whether the selected framework:

- broadly covers all areas of IT activity
- presents IT activities in a manageable and logical structure
- is generally accepted as containing good practices
- is business-orientated and capable of linking IT activities to business goals
- provides management with control objectives suitable to uncover IT issues
- fits with and supports risk management
- incorporates a baseline of internal controls for IT managers to implement

- guides management in aligning IT initiatives with real business needs
- contains performance measures to judge success and failures
- assists with assurance activities that confirm the achievement of business objectives and undesirable events are prevented, detected and corrected
- assists companies to comply with continually increasing regulatory requirements.

Whilst there are a number of management frameworks, models and standards available, CobiT (Control Objectives for Information and related Technology from ISACA) is the most widely adopted framework for implementing IT governance.



3.2 IT Governance Framework to deliver Value and manage Risk

For the IT governance framework to add value or manage risk it must:

- Establish a link to the business requirements
- Make performance against business requirements transparent
- Organise IT's activities into a generally accepted process model
- Be focused on both the process and the outcomes to be achieved
- Identify the major IT resources to be leveraged
- Define the management control objectives to be considered
- Provide a common language.

Governance occurs at the strategic, tactical and operational levels through the assignment of decision-making authority and accountability to encourage desirable behaviour in the use of IT. Governance structures differ between companies and are influenced by the size of the organisation, extent of business unit autonomy and empowerment of individual process owners with decision-rights.

Good governance depends on those with decision-making authority having the required knowledge and understanding of the decision-making process.

IT Governance Charter

An organisational charter provides the terms of reference for the IT organisation. It ensures that those with responsibility for actions also have the authority to perform those actions.

The IT Governance Charter outlines the decision-making rights and accountability framework for IT governance that will enable the desirable culture in the use of IT within the company by requiring IT management to provide timely information, to comply with direction and to conform to the principles of good governance.

3.3 Organisational Structure

A suitable organisation structure with relevant representation from the business and IT, appropriate for the size needed to adequately manage the IT organisation is to be implemented.

A top-down, layered approach to IT governance is required with team leaders reporting to and receiving direction from their managers, with managers reporting up to the executive, and the executive to the board of directors.

To be effective, business strategy and goals have to be cascaded down into the IT organisation and used as the basis for measuring performance. Each layer of governance contributes to the fulfilment of the business strategy achievement of corporate goals.

The typical organisational structure for IT governance comprises the board, an IT steering committee, a CIO and IT management with delegated responsibility to execute the IT governance framework, implemented to add value and minimise risk, including business continuity. Additional oversight authorities and ad hoc project steering committees are used to include business leaders to oversee specific services and projects.

A risk committee and an audit committee assist the board in carrying out its responsibilities and therefore should receive regular reports from IT management.

3.4 Processes

Process serves as the foundation for the definition of a management system. Process descriptions are used to capture and document details about ownership, scope, responsibilities, measurements, structured working practices and interfaces.

Processes describe the life-cycle of activities (with feedback loops) and enable the development and implementation of a lean, sustainable capability to achieve the outcomes (business goals) desired.

Processes ensure a stable, controlled, repeatable service that can be objectively measured against deliverables and outcomes achieved.

3.5 Governance Mechanisms

A broad range of governance mechanisms are often used including strategies, goals, policies, steering committees, oversight authorities, processes, procedures, roles, job descriptions, plans, schedules, contracts, proposals, authorisations, standards and scorecards with a view to deliver value and minimise risk (e.g. business continuity).

The board should monitor that those given responsibility to deploy governance mechanisms acknowledge and understand their responsibilities. The board should monitor the performance of those given responsibility in the governance of IT.

3.6 Governance of Information

To satisfy business objectives, information needs to conform to the business requirements that:

- information is relevant and pertinent to the business process, and is delivered in a timely, correct, consistent and usable manner
- Information is provided through the optimal (most productive and economical) use of resources
- sensitive information is protected from unauthorised disclosure
- Information is accurate and complete, and its validity is in accordance with business values and expectations
- information is available when required by the business process now and in the future as a result of deploying the necessary resources and associated capabilities
- information provided complies with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies
- information provided is appropriate for management to operate the entity and exercise its fiduciary and governance responsibilities.

3.7 Developing an Accountability Framework (decision rights)

Decision-making must occur as a part of a process with clearly defined roles and accountabilities. Abdication of responsibility in this process leads to undisciplined decisions made by whoever has sufficient political clout.

When assigning decision-making authority:

- start by articulating the decision that needs to be made, then
- determine the steps that must be carried out to reach a decision
- identify who should provide input, and what activities are required to obtain such input, and how

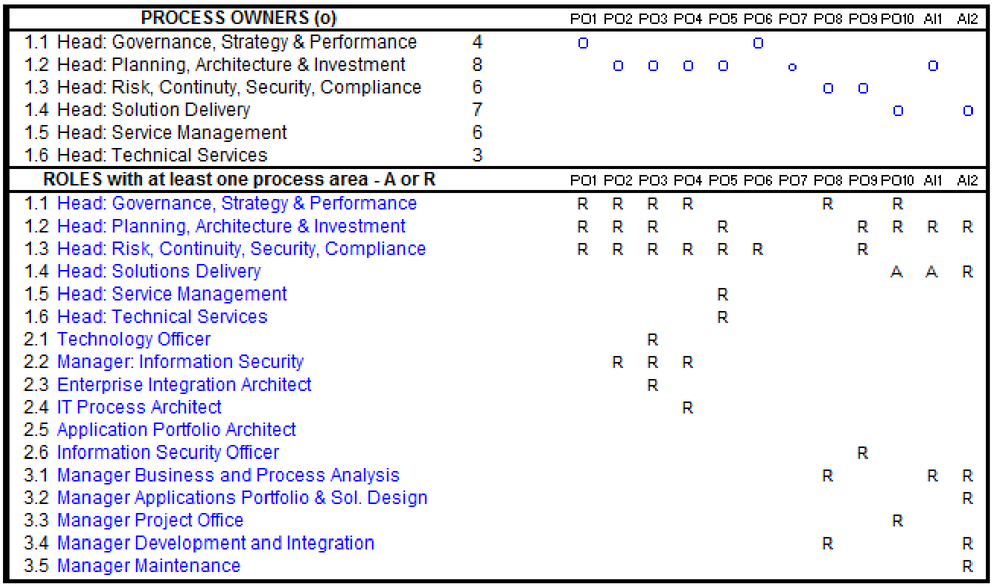
- determine who will decide, ensuring that the decision makers are equipped with the information to make a fact-based decision.

Popular sources of good practices for information technology such as ITIL, CobiT and ISO 20000 all recommend a process-orientated approach to establishing accountability for the achievement of predefined goals. In a process-orientated approach the roles needed to perform the process are identified and assigned responsibilities to perform parts of the defined process in the manner required to deliver the outcome expected. The roles performing the activities with the process are typically described as being either “Accountable”, “Responsible”, “Concur” and “Informed” (RACI) for or about the activity performed.

A key feature of the process-orientated approach is the identification of process owners. These individuals have the necessary authority (decision rights) to build and execute the process. They also have the authority to take remedial action.

The illustration below shows the managers who have been assigned **O**wnership and the managers have been assigned **R**esponsibility. One process owner may be assisted by a number of roles within the process. Ideally the role descriptions and personal performance measures for each role are based on the activities they perform in the process.

A Framework for the delegation of Authority in IT



PROCESS OWNERS (o)		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2
1.1 Head: Governance, Strategy & Performance	4	o					o						
1.2 Head: Planning, Architecture & Investment	8		o	o	o	o		o				o	
1.3 Head: Risk, Continuty, Security, Compliance	6								o	o			
1.4 Head: Solution Delivery	7										o		o
1.5 Head: Service Management	6												
1.6 Head: Technical Services	3												
ROLES with at least one process area - A or R		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2
1.1 Head: Governance, Strategy & Performance		R	R	R	R				R		R		
1.2 Head: Planning, Architecture & Investment		R	R	R		R				R	R	R	R
1.3 Head: Risk, Continuity, Security, Compliance		R	R	R	R	R	R			R			
1.4 Head: Solutions Delivery											A	A	R
1.5 Head: Service Management						R							
1.6 Head: Technical Services						R							
2.1 Technology Officer				R									
2.2 Manager: Information Security			R	R	R								
2.3 Enterprise Integration Architect				R									
2.4 IT Process Architect					R								
2.5 Application Portfolio Architect													
2.6 Information Security Officer										R			
3.1 Manager Business and Process Analysis									R			R	R
3.2 Manager Applications Portfolio & Sol. Design													R
3.3 Manager Project Office											R		
3.4 Manager Development and Integration									R				R
3.5 Manager Maintenance													R

More granular assignment of responsibilities and decision rights is achieved through the preparation of detailed process workflow charts. First the scope of each process is defined and then all the key activities within the process are identified. Next, the various organisational roles and individual roles within the process are identified. Finally, the roles are assigned their respective RACI responsibilities and decision-rights. The result is greater clarity about the accountability assigned to each role together with details about their decision rights and the collaboration expected between these roles – a framework of authorities.

Decisions now occur as a part of a process with clearly defined roles and accountabilities for the outcomes achieved.

3.8 Implementing an IT Internal Controls Framework

King III requires the board to ensure that an IT control framework is adopted and implemented, and that the board receives independent assurance of its effectiveness.

An IT controls framework comprises Accounting controls (“General” controls, “Application” controls and “User” controls) and Administrative controls. General controls are found in the infrastructure, technology and system software. Application controls are specific to business processes. User controls are the manual checks performed by staff.

Administrative controls represent the wider concerns of management, particularly with regard to efficiency and effectiveness of administration, and increased profitability.

Within applications there are:

- Inherent Controls - hard coded into the system and should not be changed.
- Configurable Controls - designed into the system, configured during installation and must be maintained during normal operation.
- Business Process/Manual Controls - utilised to support and extend the above controls to achieve a satisfactory environment that is efficient and effective.

The role of an internal control is to be preventative, detective or corrective regarding a particular risk. Controls are made sustainable through incorporation in the operational process. The selection of controls is risk-based. Ideally, a minimum set of controls is selected by determining which are most effective and have the broadest span of control.

COSO (Committee of Sponsoring Organisations of the Treadway Commission) is the suggested internal control framework to be used for compliance with Sarbanes-Oxley in the USA. It is usually complemented with an IT specific control framework - CobiT.

The condition of controls depends on the organisational structure, written policies, systemisation, evidence of controls operating and the competence and integrity of the people involved.

3.9 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
- Take responsibility for the implementation and monitoring of IT governance within the company
- Seek leadership from the board, obtain direction and an understanding of the ethics and values that will influence and guide practices and behaviour within IT to achieve sustainable performance
- Implement an Accountability framework to assign decision-making rights
- Implement a suitable organisational structure and define terms of reference
- Be a bridge between IT and the business
- Ensure transparency through regular reporting to the board
- Implement IT processes and governance mechanisms
- Implement IT frameworks, policies, procedures and standards
- Enable IT to add value to the business and mitigate risks
- Incorporate IT into the business processes in a secure, sustainable manner
- Develop and implement an IT governance charter and policies
- Encourage the desirable use of IT by requiring managers to provide timely information, comply with the direction given and to conform to the principles of good governance
- Implement an ethical IT governance and management culture
- Create an awareness of the maturity levels of governance
- Build management skills and competencies to govern and promote a common language
- Incorporate IT governance in corporate governance
- Adopt and implement an IT control framework
- Implement processes to ensure that reporting to the board is complete, timely, relevant, accurate and accessible
- Obtain assurance on the effectiveness of the IT control framework
- Sustain and enhance the company's strategic objectives
- Implement a strategic IT planning process that is integrated with the business strategy development process
- Enable the improvement of the company's performance and sustainability
- Integrate IT plans with the business plans
- Define, maintain and validate the IT value proposition
- Align IT operations with business operations
- Align IT activities with environmental sustainability objectives
- Implement a robust process to identify and exploit, where appropriate, opportunities to improve performance and sustainability of the company in line with triple bottom line objectives
- Include relevant representation from the business in oversight structures
- Have regard for the legislative requirements that apply to IT
- Understand business requirements and long-term strategy
- Have a strategic approach and facilitate the integration of IT into business strategic thinking
- Translate business requirements into efficient and effective IT solutions
- Exercise care and skill over the design, development, implementation and maintenance of sustainable 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
- Measure and manage the amount spent on and the value received from technology
- Protect information and intellectual property
- Conduct post-implementation reviews to learn from each implementation
- Promote sharing and re-use of IT assets
- Ensure all parties in the chain from supply to disposal of IT services and goods apply good governance principles
- Monitor and enforce good governance across all suppliers
- 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
- Design, implement and monitor the IT risk management plan
- Maintain an IT risk register, including IT legal risks
- Comply with applicable laws and regulations
- Perform continual risk assessments
- Select and use an appropriate framework for managing risk (e.g. COSO)
- Consider and implement appropriate risk responses
- Implement an IT controls framework
- Minimise risks
- Manage information assets effectively
- Ensure the integrity and availability of information and information systems in a timely manner
- Implement information records management and ensure information assets are identified, classified, retained, stored, archived, protected and made available when required for business and legal purposes
- Establish a business continuity programme for the company's information and successful execution of the business' activities
- Identify all personal information processed by the company and treat this as an important business asset, including being processed in accordance with applicable laws
- Implement an information security strategy
- 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
- Consider using IT to aid the company's risk management, compliance and audit efforts.

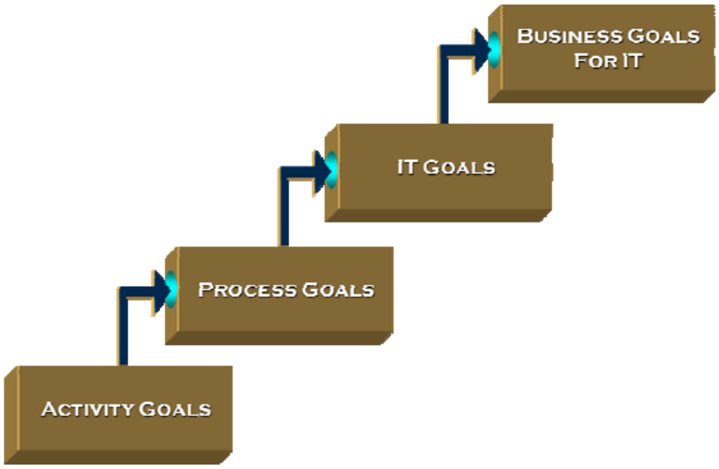
4. Strategic Alignment

THE BOARD SHOULD ENSURE THAT IT IS ALIGNED WITH BUSINESS OBJECTIVES, INCLUDING ECONOMIC, SOCIAL AND ENVIRONMENTAL SUSTAINABILITY

4.1 Alignment with Corporate Objectives

Corporate objectives are attained through the effective and efficient management of IT resources. This assists management understand "what is the outcome expected", "what does success look like" and "who will recognise this success".
It enables IT management to align IT activities with the performance and sustainability objectives of the company".

Business goals are cascaded to IT goals, process goals and activity goals. This might appear to be straight forward, but is made difficult when there isn't agreement between the business leaders as to what priority should be given to the business goals.



4.2 Integration of Strategic IT Planning with the Company's Strategic and Business Objectives

King III states that the board should ensure that IT achieves, sustains and extends the company's strategic objectives. Management is to implement a strategic IT planning process that is integrated with the business strategy development process, and:-

- IT plans are integrated with the business plans
- IT operations are aligned with business operations
- The IT function, roles and reporting lines are structured to reflect the integration of IT with the business operations
- IT contributes towards the company's objectives in an effective and efficient manner
- The IT contribution towards the attainment of the company's objectives is monitored and measured
- The IT value proposition has been defined, maintained and validated
- The effect of IT on the environment is considered

- There is a process in place to identify and exploit opportunities where IT can create value and assist the company to gain competitive advantage for the company
- The IT steering committee contains both business and IT representation
- A business-oriented CIO is appointed
- The CIO has an understanding of the business strategy
- The CIO has access to the board and executive management
- IT investment and expenditure supports the business objectives
- The role of IT in achieving strategic business objectives is clear
- IT spend is measured and managed to deliver value to the business
- IT assurance is addressed as an integral part of the normal assurance activities
- IT risk is addressed as an integral part of the normal risk management activities
- IT compliance with legal requirements is addressed as an integral part of the normal compliance activities
- IT risks are understood and managed from a business strategic perspective.

Every company’s approach to IT governance should be based on business needs and the reliance on IT to drive, enable, support and improve the company’s ability to attain its strategic performance and sustainability objectives.

4.3 Direction from the Top

In keeping with other sources of good practices for corporate governance, King III requires the board to translate its leadership into clear statements of direction that management of the company can follow. Direction can be communicated in many different ways. Corporate objectives, business goals and policy statements are some of the media used to communicate the board’s intent.

An example would be the policy defined by the CIO for board approval as to the nature, extent and accountability for implementing information security. The CIO can preauthorise services proposed for a future date within the policy framework set by the CIO and approved by the board.

4.4 Define, maintain and validate the IT value proposition

The value proposition of IT is determined by clarifying the role of IT in achieving business strategies.

The generic value chain model represents a useful tool for analysing how individual organisations create value. Within value chain analysis, there are two generic strategies an organisation can pursue to achieve a competitive advantage by:

- Creating a low-cost competitive advantage by reducing the cost of an individual value chain activity or reconfiguring the value chain.

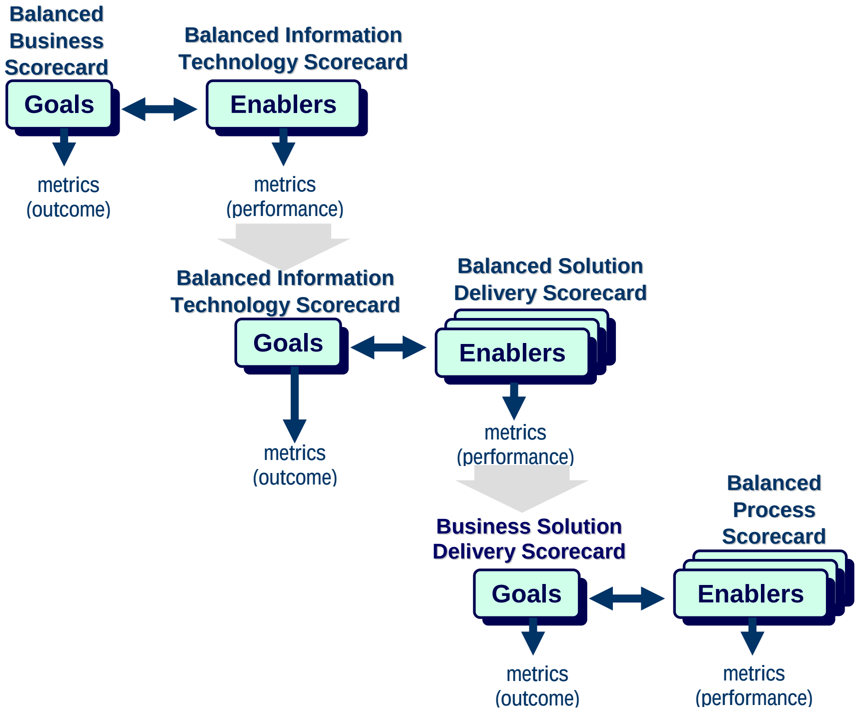
- Creating a value-added competitive advantage by increasing the value of an individual chain activity or reconfiguring the value chain.

The IT organisation adds business value by enabling a company to differentiate its value chain from each of its competitors' value chains. In some organisations IT adds value to "Inbound Logistics" through supply chain integration. In others, IT may add value through "Customer Support". Often IT adds more value to the company in some parts of the value chain and less in others.

It makes sense that IT activities are prioritised in areas where there is greater contribution of value.

4.5 Aligning IT Operations with Business Operations

IT activity goals are to be aligned with IT process goals, which in turn are aligned to IT organisational goals and business goals. Conversely, business goals cascaded down to the activity level within IT providing substance to the requirement of aligning IT with strategic goals.


Balanced Business Scorecard
Goals
metrics (outcome)
Balanced Information Technology Scorecard
Enablers
metrics (performance)
Balanced Information Technology Scorecard
Goals
metrics (outcome)
Balanced Solution Delivery Scorecard
Enablers
metrics (performance)
Business Solution Delivery Scorecard
Goals
metrics (outcome)
Balanced Process Scorecard
Enablers
metrics (performance)

4.6 Sustainability

Tomorrow's Company in the United Kingdom developed the concept of three corporate sins, namely:

- *sloth*, being a loss of flair when enterprise gives way to administration
- *greed*, when executives might make a short-term decision because it has greater impact on their share options than a decision that might create longer term prosperity for the company

- *fear*, where executives become subservient to investors and ignore the drive for sustainability and enterprise.

For CIOs and IT management sustainability is about maintaining the capability to perform as expected. Without investment, capability within IT is certain to diminish over time and dependency would grow on external solution providers. Without the necessary skills the company will not be able to exploit business opportunities that may come their way in the future.

Nurturing, protecting, capturing, retaining and developing human capital is a vital ingredient in the sustainable economic performance of any enterprise. The ongoing challenge is for the enterprise to benefit from staff members' latent potential.
.

4.7 Improve Performance and Sustainability

King III states that IT management is to implement a robust process to identify and exploit, where appropriate, opportunities to improve performance and sustainability of the company in line with triple bottom line objectives.

Process orientation, with an element of self-analysis, provides for continuous improvement often described as the Deming cycle of "Plan-Do-Check-Act". This provides the iterative characteristic required for a process to sustain and extend its performance and sustainability.

4.8 Concern for the Environment

Aligning IT activities with environmental sustainability objectives requires management to consider the environmental aspects and significant Impacts of IT and IT activities, including:

- Energy saving
  - Data centre facilities design
  - Data centre heat recycling
  - Advanced cooling technologies
  - Processor design and server efficiency
  - Energy management for the office environment
  - Integrated energy management for the software environment
  - Combined heat and power
  - Use of modelling and monitoring software

- Avoidance of wasteful expenditure
  - Recycling of infrastructure
  - Reusable code and services
  - Paperless reporting
  - Optimised software programs
  - Overly complex and tightly integrated solutions
  - Unnecessarily large infrastructure
  - Unnecessary data storage
  - Excessive security and disaster recovery planning.

- Avoidance of unnecessary CO2 emissions
    - Disposal of inefficient technology
    - Purchase greener energy
    - Purchase from companies known to be greener
    - Excessive data redundancy
    - Excessive feature
    - Records management
    - Avoiding travel and transport.

Direction from the board will ensure that green IT initiatives are aligned with the company's overall strategy and its corporate social responsibility programme. Green IT principles would be based on the environmental policy established by the board. These principles provide decision makers with predefined preferences when alternative options are available.

EXECUTING ON THE VALUE PROPOSITION OF IT

5.1 Value Delivery

"Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT". - CobiT

King III acknowledges that companies create employment and wealth through their business endeavours. They expect a return commensurate to the risk they are prepared to take in doing business. The board should ensure that the purpose and value drivers of the company are included in the strategy whilst taking into consideration the legitimate interests and expectations of all stakeholders.

The board is responsible for ensuring that IT resources facilitate the achievement of the company's strategic objectives and that IT should add value by enabling the company's performance and sustainability.

The board should ensure that the expected return on investment from IT projects is delivered and that the information and intellectual property contained in the information systems are protected. This can be achieved by:

- clarifying the role of IT in achieving business strategies;
- measuring and managing the amount spent on and the value received from IT;
- assigning accountability for organisational changes required to benefit IT capabilities;
- learning from each implementation, becoming more adept at sharing and reusing IT assets.

The value of an IT investment depends entirely on whether or not it makes the people doing the work, more efficient and effective.

Spending money simply to improve a system's performance is meaningless; spending money on a system to improve the organization's performance is useful. Therefore, the value of an information system should be measured and managed by people focusing on business processes and practices, not the system itself.

In order to deliver value to the business, an IT governance framework should have relevant organisational structures, IT processes and measurements. The framework should also be applicable and appropriate. There is no sense in doing more than is absolutely necessary to achieve the company's objectives.

Balanced scorecards are popular tools for proving the value of IT. Most balanced scorecards address four perspectives: financial contribution, customer, internal process excellence and future orientation (i.e. sustainability). Balanced scorecards are cascaded down from the business' balanced scorecard to IT process balanced scorecards, establishing a link with the activities creating the value proposition for IT.

6. Risk Management

RISK MANAGEMENT SHOULD SEEK TO PROVIDE INTERVENTIONS THAT OPTIMISE THE BALANCE BETWEEN RISK AND REWARD WITHIN THE COMPANY

6.1 IT Governance and Risk Management

Each day companies face considerable risk that grows in significance when using information technology. There are regular opportunities for information technology failures to disrupt business and prevent the achievement of operational and strategic objectives. Some of the causes are:

- Error
- Poor quality of service
- High-rate of obsolescence
- High-level of development
- High-level of dependence on vendors, service providers and consultants
- Wasteful expenditure, unnecessary features
- Inadequate architecture, limited interoperability and poor scalability
- Unproven, brittle and poorly designed technology
- Limited capability to implement and support solutions and end users
- Monolithic, inflexible applications with complex integration
- Multiple contractual, regulatory and legislated compliance requirements.

King III requires that IT risks form part of the company's risk management. IT management should regularly demonstrate to the board that the company has adequate "business resilience" arrangements in place to recover from disaster.

The King III principles for risk management are:

- The board is responsible for the governance of risk
- The board should determine the levels of risk tolerance
- The risk committee or audit committee should assist the board in carrying out its risk responsibilities
- The board should delegate to management the responsibility to design, implement and monitor the risk management plan
- The board should ensure that risk assessments are performed on a continual basis
- The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks
- The board should ensure that management considers and implements appropriate risk responses
- The board should ensure continual risk monitoring by management
- The board should receive assurance regarding the effectiveness of the risk management process
- The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

6.2 Responsibility for Risk Management

The board is responsible for the process of risk management. The board may task a risk committee to oversee risk management.

Line management has responsibility to manage risk and this should be reflected in individual letters of appointment, key performance areas and reward systems. Risk management is to be embedded in its operations, decision-making processes and the execution of strategy.

6.3 Risk Appetite

It's the board's role to set a risk appetite or tolerance level for the company. This should be determined in accordance with the company's strategic objectives.

The CIO should use this risk appetite as the basis for implementing a risk management process across the IT function and to establish an IT risk management plan.

6.4 Risk Identification

As is the case with COSO, King III requires risk identification to be directed in the context of the company's purpose and to focus on strategic and operational risks.

Risk identification should not rely solely on the perceptions of a select group of managers. A thorough approach to risk identification is required. Consideration should be given to reputation risk and IT legal risks.

6.5 Risk Quantification and Response

King III states that the board should ensure that key risks are quantified and are responded to appropriately. The board is to decide which risks are significant.

It may be sufficient to classify risk as high, moderate or low. It is important that the board and the management develop a clear, shared understanding of the risks that are acceptable or likely to become unacceptable and then decide how they will manage the risks and control strategies.

The board should ensure that risks are validated with relevant stakeholders to confirm the:

- accuracy and validity of risk information recorded
- assumptions made in assessment of the risk information provided
- the need for any additional data or information on the effectiveness of the control environment.

Risks evaluated should be prioritised and ranked to focus risk response measures on those risks outside the board's risk tolerance limits.

Whilst King III states that management must identify and consider the possible risk response options, past experience shows that CIOs and IT management have spent little time managing the risks inherent in information technology.

6.6 Risk Management Plan

King III requires the use of a risk management plan to achieve risk management objectives. It states that the board is to adopt a risk management plan.

The CIO is to ensure that IT management design the processes of risk management based on the board's appetite for risk, the company's defined risk philosophy and the company's short- and long-term strategies. The risk management plan should include an implementation plan, which should be monitored as a medium-term project and have scheduled reviews.

The plan should outline the resources, tasks and responsibilities for introducing and developing the risk management processes and activities into the company. When designing the implementation plan, management should determine the sequence of implementation, document roles and responsibilities, determine the target dates for implementation and decide on the frequency and format of reporting against milestones.

The risk management plan should state the company's objectives on risk optimisation, how risk management should support its business strategy and how regulatory requirements should be managed. Risk management processes should be incorporated into budgeting and business planning activities.

6.7 Risk Assessment using a Generally Recognised Methodology

COSO is the risk assessment methodology frequently quoted in discussions about the Sarbanes-Oxley Act in the US. An alternative is ISO 31000, the international standard for risk management. Regardless of the risk assessment methodology, almost always it is the CobiT framework that is actually used within IT.

This process-orientated model focuses the risk assessment on the activities and processes that produce the information, the information, and the impact information has on the business. A process-orientated model like CobiT provides management with a framework that assists with understanding the scope of risk assessment and helps avoid gaps when conducting the risk assessments.

6.8 Risk Assessment Outputs

King III states that risk assessments are to be performed on an ongoing basis with the outputs of risk assessments providing the board and management with a realistic perspective of the material risks facing the company.

6.9 Risk Register

King III states that the board should receive and review a register of the company's key risks. It is important that the risk information presented to the board includes a profile of aggregated risks, correlated risks and risk concentrations.

IT management are therefore required to provide a balanced assessment of the significant risks and the effectiveness of internal control in managing those risks.

Any significant control failings or weaknesses identified should be discussed in the reports, including the effect that they have had, or may have had, on the company, and the actions being taken to rectify them. It is essential that management communicates openly with the board on matters relating to risks and controls.

6.10 Reputational, Sustainability and Ethics Risk Assessment

In assessing risk, management are required by King III to address the broader issues of company reputation, sustainability and ethics.

6.11 Alignment of IT with business objectives and sustainability

The pervasive nature of IT makes it an integral part of the business that is fundamental to support, sustain and grow the business. Consequently, King III requires companies to implement IT governance, splitting responsibility between the board and management.

The board is to "specify the decision rights and accountability framework to encourage the desirable culture in the use of IT". Board members are to take an active role in IT strategy and governance.

Board level oversight for IT activities is usually based on the strategic importance of IT:

- How much does the company rely on cost-effective, uninterrupted, secure, smoothly operating technology systems?
- How much does the company rely on IT for its competitive edge through systems that provide new value-added services and products, its responsiveness to customers?

At a time of major investment in information technology, with 50% or more of capital expenditure and 15% or more of operation costs spent on IT, the board is expected to be fully informed and able to exercise the necessary oversight. If it is technology that is promising a major transformation of the company's business processes the board must take full accountability and be responsible for the decisions made.

King III has identified information security as an important aspect of IT governance. Weaknesses in information technology solutions continue to exist and be exploited by a growing number of criminals. To the extent the threats are real, companies need to invest in ever increasing levels of information security. Just how far does a company needs to go depends on the risk appetite of the board and the direction provided. Without adequate information security companies may not be able to fully exploit business opportunities available from exploiting information technology in innovative ways.

6.12 Business Continuity

Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in the event of a disaster affecting IT.

6.13 Information Management

Management is to ensure the integrity and availability of information and information systems in a timely manner. They must attend to record retention and compliance with security and privacy requirements.

6.14 Data Privacy

The board should ensure that resources are deployed to manage personal information and to ensure compliance with the applicable laws.

6.15 Information Security

Resources should be deployed to develop, implement and manage an appropriate Information Security Management System. The board should delegate responsibility for the management of these resources to IT Management.

6.16 The use of technology to aid the management of risk and compliance

Consideration should be given to the suitability, economy and effectiveness of using technology at various stages of the processes to manage risk and compliance.

7. Managing IT Resources

OPTIMISING KNOWLEDGE, IT INFRASTRUCTURE AND RELATIONSHIPS

7.1 Resource Management

The effective and efficient management of IT resources is central to the King III definition of IT governance. The board should ensure that the company treats its economic, social and environmental resources responsibly and that this performance should be reported on in an "integrated report".

Directors have a fiduciary duty to act in the best interest of the company. This requires the board to direct management to focus on ensuring the optimal use of available resources, including knowledge, infrastructure and partnerships.

King III states that board responsibilities include:

- monitoring and evaluating the extent to which IT actually sustains and enhances the company's strategic objectives
- monitoring and evaluating the acquisition and use of IT resources to ensure that they support business requirements
- monitoring and evaluating the acquisition and appropriate use of technology, process and people
- overseeing IT investment to ensure that IT expenditure is in proportion to the delivery of business value
- Ensuring good governance principles apply to all parties that provide IT resources. This includes suppliers of hardware, software, skills and IT services
- Remaining accountable for ensuring that effective IT governance is in place where a resource has been "outsourced".

Management is expected to leverage knowledge and skill, capture the lessons learnt and build capability in people. Human resources are crucial to a company's sustainability.

Regardless of whether IT assets are on or off the balance sheet, it is the ability of the company to control and make the most of critical capabilities that matters most. Whilst outsourcing is now common practice the board should be concerned about issues of:

- Governance of outsourced services
- Compliance in an outsourced environment
- Company's capability to outsource.
- Capability of service providers to provide contracted services.
- Considerable additional risks from outsourcing – compliance, staff turnover, control of costs
- Nature of third-party contracts (outsourced services or lease agreements for equipment and the hiring of staff)
- Adequacy of service level agreements
- Pricing and charging practices
- What capability is required at termination of the outsourcing contract?

8. Managing Performance

PROPER IT GOVERNANCE ASSISTS THE BOARD ENSURE THAT IT USE CONTRIBUTES POSITIVELY TO THE PERFORMANCE OF THE ORGANISATION.

8.1 IT Governance and Performance Management

Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance, service delivery and the achievement of expected outcomes.

IT performance must be assessed on an ongoing basis against the agreed-upon outcomes of the IT Organisation. This includes measurement of internal control, regulatory compliance and governance.

Performance measurement must also include a review of remedial action where performance is not as expected. Independent assurance about the effectiveness of an implemented internal control framework as well as the performance of the IT organisation should be considered.

IT Management should report to the Board about IT:

- achieving its objectives
- being resilient and agile to adapt to changing strategic needs
- judiciously managed risks
- recognising and acting on business opportunities.

Performance management underpins IT governance by proving the value proposition and measuring the performance of IT. Performance measurement necessitates consideration of:

- Outcomes expected by stakeholders - key goal indicators
- Measurement of the enablers used to achieve these outcomes
- Management's control of activities critical to the success of the enablers.

IT goals and measures must flow directly from strategic goals. IT managers and staff should not develop performance management systems that optimise operational customer results without considering a company-wide perspective.

IT goals and measures in support of individual operational customers must meet IT department or unit objectives. In turn, IT department or unit objectives must map directly to both programme and company-wide strategic directions or goals. The result is that IT goals and measures track in a seamless fashion back to the company's business objectives and corporate goals.

Any outsourced IT services remain the responsibility of the Board and external assurance regarding the governance must be obtained. The audit committee must include these assurance tasks within the normal assurance activities.

IT projects may require reviews by independent experts to ensure that appropriate project management principles are applied.

8.2 Approach to Performance Measurement

Capability measures provide insight into the processes used to deliver the required outcome. Surprising for many companies is that their level of capability is largely dependent on people for their success. Some have basic processes defined to manage risk. More efficient organisations will have well-defined processes that are efficient and effective.

Institutionalisation is a critical aspect of process improvement and is an important concept within each level of organisational maturity. It implies that processes are ingrained in the way work is performed.

A managed process is institutionalised by doing the following:

- Assigning responsibility and authority for performing the process
- Adhering to organisational policies
- Following established plans and process descriptions
- Providing adequate resources (including funding, people, methods and tools)
- Training the people performing and supporting the process
- Placing designated work products under appropriate levels of configuration management
- Identifying and involving relevant stakeholders
- Monitoring and controlling the performance of the process against the plans for performing the process and taking corrective actions
- Objectively evaluating the process, its work products, and its services for adherence to the process descriptions, objectives, and standards, and addressing non-compliance
- Reviewing the activities, status, and results of the process with higher-level management, and taking corrective action.

Performance measures can only be successful if they measure not only the outcomes of the governance activities but also the relevance and effectiveness of the applied governance framework, processes and measurements.

9. Risk and Audit Committees

RISK AND AUDIT COMMITTEES SHOULD ASSIST THE BOARD IN CARRYING OUT ITS IT RESPONSIBILITIES

9.1 Risk Committee

IT management of any company, regardless of size, should be fully committed to the goal of supporting and maintaining an effective risk committee.

The risk committee should fully understand the company's overall exposure to IT risks from a strategic and business perspective. The risk committee is to obtain assurance that all significant risks are managed in an appropriate manner.

9.2 Audit Committee

IT management of any company, regardless of size, should be fully committed to the goal of supporting and maintaining an effective audit committee.

King III views the audit committee as a critical component in ensuring the integrity of integrated reporting and financial controls, the proper identification and management of financial risks and the integrity of the reporting practices.

The audit committee generally oversees the company's reporting and assurance functions on behalf of the board, and serves as a link between the board and these functions. The audit committee should be responsible for monitoring the integrity and completeness of the company's financial reporting and compliance with other regulatory requirements. It may also review aspects of risk and sustainability issues where it is mandated to do so by the board.

King III requires management to at least annually conduct a formal documented review of the design, implementation and effectiveness of the company's system of internal financial controls by conducting suitable testing and report back to the audit committee. This enables the audit committee to perform its responsibilities to oversee the integrity of the company's financial information. (External auditor attestation on internal financial controls is not a requirement.).

As information technology often provides the company's system of internal controls, the CIO and IT management are therefore required to conduct suitable tests and report back to the audit committee.

Understanding and measuring IT risks helps members of the audit committee understand the company's overall exposure to IT risks from a business perspective. Areas that are not appropriately governed (e.g. outsourcing and ERP implementations) expose the company to higher levels of risk. The audit committee should obtain appropriate assurance that controls are adequate to address the risks in these areas.

10. Managing Information

THE BOARD IS TO ENSURE INFORMATION ASSETS ARE MANAGED EFFECTIVELY

10.1 Information Management

Management is to manage information assets effectively, ensuring the integrity and availability of information and information systems in a timely manner. Suitable processes should be in place to manage information throughout the life cycle.

Information records providing evidence of business activity are important information assets that need to be identified, classified, retained, stored, archived, protected and made available when required for business and legal purposes.

10.2 Information Privacy

All personal information processed by the company is to be identified and treated as an important business asset, including being processed in accordance with applicable laws.

10.3 Information Security

The board should ensure that an information security management system is implemented according to an applicable information security framework. The board should oversee the development of the information security strategy and delegate its implementation to IT management.

Management are to implement the information security strategy and an information security management system in accordance with an appropriate information security framework.

11. Compliance

PROPER IT GOVERNANCE ASSISTS DIRECTORS IN ASSURING CONFORMANCE WITH OBLIGATIONS (REGULATORY, LEGISLATION, COMMON LAW, CONTRACTUAL) CONCERNING THE ACCEPTABLE USE OF IT

11.1 Compliance with obligations

Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.

It is the Boards responsibility that all relevant IT laws are adhered to. The Board should consider any standards, guidelines or practices that would be relevant to the IT organisation.

King III states that the board is responsible for the company's compliance with laws and regulations and should ensure that the company implements an effective compliance framework and processes.

11.2 A Single, Holistic Approach to Compliance

Often IT management is required to address multiple compliance requirements. In the US, one government agency reported that it was subjected to 28 compliance audits in the space of two years.

With the ever-increasing number of regulators, regulations, legislation and contractual obligations, management need to find a practical way to deal with compliance. Frequently multiple compliance requirements target the same set of risks and controls.

The most effective way to achieve compliance with external regulators and internal requirements is to adopt a process-orientated approach, starting with a single, generally accepted baseline of controls to which additional regulatory and statutory required controls are added.

Management should consider how IT can be used to assist the company in managing its compliance obligations.

11.3 Compliance must be made sustainable

Sustainability comes through controls being:

- Enabled through documented processes
- Supported by the capability of people
- Made effective through automation
- Regularly monitored.

12. GLOSSARY

Accountability Framework

Defines the nature and scope of responsibilities, identification of key results, performance expectations, and the monitoring and reporting strategies.

Charter

A charter is the grant of authority or rights, stating that the granter formally recognizes the prerogative of the recipient to exercise the rights specified.

Control

A process implemented in an organization to help in achieving specific goals.

Delegation of Authority

Delegation requires *specific detail* about what has been delegated (specificity) and *specific responsibility* to control what has been delegated (accountability).

Framework

A framework is a basic conceptual structure used to solve or address complex issues.

Governance Framework

An IT governance framework comprises definitions, principles and a model for governing IT.

Management

The system of controls and processes required to achieve the strategic objectives set by the organisation's governing body. Management is subject to the policy guidance and monitoring set through corporate governance.

Mechanism

A set of rules designed to bring about a certain outcome.

Model

The practical implementation of a framework.

IT Governance model of the cycle of Evaluate-Direct-Monitor. The text following Figure 1 explains the elements and relationships depicted.

Policy

Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organization.

Policy statements are used by management to exert major influence on the organisation’s resource allocation and on specific issues, including technology.

A statement of commitment to a broad requirement, often used in an organization to instruct personnel as to a required outcome.

Principle

A rule used to choose among solutions to a problem. A normative rule or code of conduct. Principles express preferred behaviour to guide decision making. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented – as these aspects are dependent on the nature of the organization implementing the principles. Directors should require that these principles are applied.

Procedure

Procedures describe how a policy is implemented. An organisation needs to be efficient in the tasks that are carried out internally. The organisation therefore should see to the development of *rules* and *procedures* that prescribe the preferred manner in which things are to be done in the organisation, as well as a means of *monitoring* the application of these rules.

Process

A structured set of activities that achieve a specific purpose.

Process Owner

Person who is accountable for ensuring the process is performed in a manner suitable to achieve the required outcome, and make changes to the process, when necessary.

Role

A set of responsibilities defined in a process and assigned to an individual or team.

Risk Management Plan

A risk management plan is a document prepared by a project manager to foresee risks, to estimate the effectiveness, and to create response plans to mitigate them.

Segregation of Duties

The allocation of tasks to individuals must take account of the potential risk of mistakes and fraud. Segregation should:

- increase the need for collusion
- reduce the opportunities for concealment of fraud or incompetence.

Strategy

An organization's overall plan of development, describing the effective use of resources in support of the organization in its future activities. It involves setting objectives and proposing initiatives for action.

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