A Methodology for Measuring and Monitoring IT Risk

by

Natalie Tansley

Submitted to define the research
area for part fulfilment of the degree

Master Technologiae

in

Business Information Systems

in the

Faculty of Engineering, The Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: **Helen van de Haar**

December 2007

Acknowledgements

Stephen Flowerday, for his guidance and assistance as promoter for this paper during the initial research period.

Helen van der Haar for her guidance and thoroughness as promoter for this paper

Table of Contents

Chapter 1 : A Methodology for Measuring and Monitoring IT Risk

Chapter 2 : IT Governance and its Drivers: Sarbanes-Oxley and Basel II, the Forces of IT Risk Management

Chapter 3 : Standards, Methodologies, Guidelines and Frameworks of CobiT, COSO, ITIL and ISO17799 Internal Control

Chapter 4 : Monitoring and Measuring Internal Control

Chapter 5 : Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC)

Tables

Figures

Chapter 1

A Methodology for Measuring and Monitoring IT Risk

1.1 Introduction

The role of the Information Security Manager has evolved over the past few years from essentially IT focused to that of a business/IT hybrid. At the same time, numerous security codes of practices and methodologies have been developed and published with the intention of providing some level of support or direction for security objectives (Information Security Harmonization, Information Systems Audit and Control Association).

The IT Governance Institute (ITGI) was established in 1998 to advance international thinking and standards in directing and controlling an organization's IT. Effective IT governance helps ensure that IT supports business goals, optimizes business investments in IT and appropriately manages IT related risks and opportunities.

In 2002 an US law, Sarbanes-Oxley was passed to strengthen corporate governance and restore investor confidence (Sarbanes Oxley Tutorial – SOX Compliance Information). Sarbanes-Oxley addresses:

- New standards for corporate boards and audit committees;
- New accountability standards and criminal penalties for corporate managements;
- New independence standards for external auditors;
- The establishment of a Public Company Accounting Oversight Board (PCACB) under the Security and Exchange Commission (SEC) to oversee public accounting firms and issue accounting standards.

Two control frameworks have been widely adopted by organizations, subject to the requirements of the Sarbanes-Oxley Act 2002. These are the Control Objectives for Information and related Technology (CobiT) and the Committee of Sponsoring Organizations (COSO) Internal Control.

CobiT is a comprehensive set of resources that contains the information that organizations need to have in order to adapt to an IT governance and control framework. CobiT helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure (CobiT Executive Summary, IT Governance Institute, 2000).

The COSO framework for internal controls states that internal control is a process, established by an organization's directors, management and other personnel to provide reasonable assurance. (Garrett Hickey, TIU Management Consultants Ltd) The COSO framework was adopted as the standard for internal accounting controls and is viewed as a method to improve the quality of financial reporting.

The main aim of internal control is to identify risks achieving an organization's objectives and to do what is necessary to manage those risks. The setting of goals and objectives is a precondition for internal controls (Standards for Internal Control in the Federal Government, United States General Accounting Office, 1999). If an organization does not have goals and objectives, there is no need for internal control. Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting and compliance goals and objectives. Once the risks to the organization have been identified, a risk analysis should be performed to prioritize those risks. In the same way that managers are responsible for identifying the risks to their operations, they are also responsible for designing, implementing and monitoring the internal controls activities which should address the risks highlighted in the risk analysis process. All five internal control components must be present to conclude that internal control is effective.

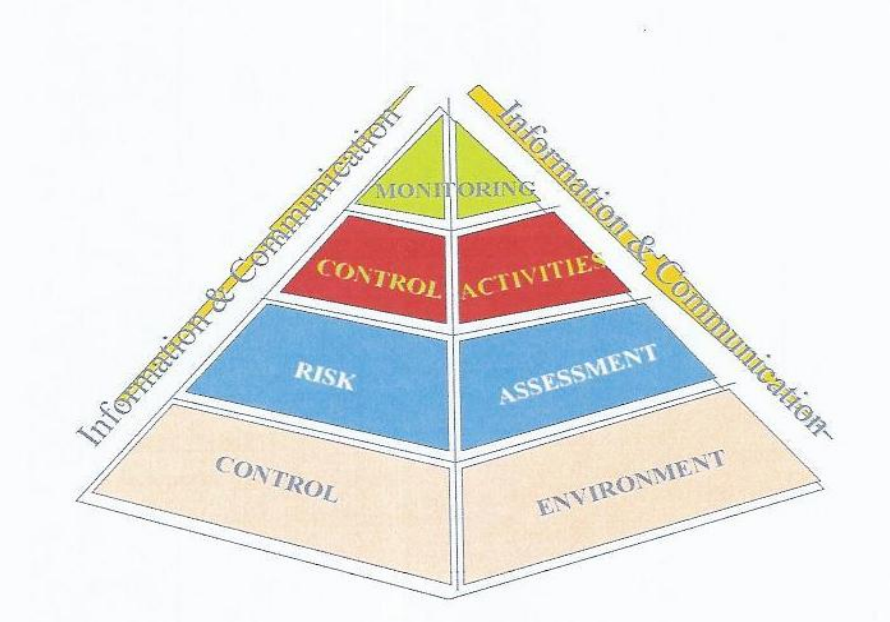

Figure 1 : The Internal Control Process

Internal control is not a single event, but a series of actions and activities that occur on an ongoing basis throughout an organization's operations and should be recognized as an integral part of each business process that management uses to regulate and guide its operations rather than as a separate process within an organization. (Standards for Internal Control in the Federal Government, United States General Accounting Office, 1999).

1.2 Description of Problem Area

One of the most important assets of an organization is its information. The integrity and reliability of that information and the business processes that generate it are crucial to an organization's success.

Accordingly the Common Criteria (1999), "IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration or loss."

Information security is a key aspect of IT governance and it is an important issue for all computer users to understand and address. As computer systems have become

increasingly more commonplace in all walks of life, from home to school and office, unfortunately, so too have the security risks. The widespread use of the Internet, handheld and portable computer devices and mobile and wireless technologies has made access to data and information easy and affordable. On the other hand these developments have provided new opportunities for IT related problems to occur, such as theft of data, malicious attacks using viruses, hacking and even new ways to commit organized crime. These risks, as well as the potential for careless mistakes, can all result in serious financial, reputation and other damages.

According to Dr. Paul Dorey, Director, digital business security, BP, PLC; "Information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it."

Organizations realize investing in IT systems in order to obtain a sustainable competitive advantage is no longer enough. This means that it is naïve for organizations to believe that the implementation of new technologies enables an organization to maintain a competitive advantage over its competitors. In order for an organization to keep up to date with technology advances, organizations must design and create a safe environment in which business processes can function. The environment must maintain confidentiality, availability and assure the integrity of the organization's data and information.

1.2.1 Problem Statement

Business processes need to be managed and modified and internal controls within them are a security solution. One can not manage IT risk exposure unless one measures and monitors progress, only then one can improve on it. It is important to monitor and measure internal controls within the business process to see if they adequately mitigate the IT risks to an acceptable an adequate levels.

A need exists to identity measurement methods in order to determine whether an organization's business processes' internal controls are sufficient or adequate to provide assurances that risk has been addressed.

1.3 Research Objectives

The primary objective of the research is to develop a methodology for monitoring and measuring IT risks, strictly focusing on internal controls. The research delivers a methodology whereby an organization can measure its system of internal controls, providing assurance that the risks are at an acceptable level.

To achieve the primary objective a number of secondary objectives were addressed:

- What are the drivers forcing organizations to better corporate governance in managing risk?
- What is IT risk management, specifically focusing on operational risk.
- What is internal control and specifically focusing on COSO's internal control process.
- Investigation of measurement methods, such as, Balance Scorecards, Critical Success Factors, Maturity Models, Key Performance Indicators and Key Goal Indicators.
- Investigation of various frameworks such as CobiT, COSO and ISO 17799, ITIL and BS 7799 as to how they manage IT risk relating to internal control.

1.3.1 Research Methodology

The research addressed the problem of monitoring and measuring IT risk. The problem was analysed and a methodology is proposed. This involved a literature study of frameworks, methodologies, articles, journals and books as well as a study of the history of measurement methods, such as, Balance Scorecards, Critical Success Factors, Maturity Models, Key Performance Indicators and Key Goal Indicators.

1.4 Layout of the paper

Chapter Two researches IT governance and its drivers; Sarbanes-Oxley and Basel II, the forces of IT risk management. The risk management process and internal control are investigated, focusing specifically on COSO's Internal Control process.

Chapter Three explains internal control further and the standards, methodologies, guidelines and frameworks of CobiT, COSO, ITIL and ISO17799 pertaining to internal control are also investigated.

Chapter Four researches the history of measurement methods available to management which are capable of mitigating an organization's IT risk to an acceptable and adequate level. The measurement methods researched are the Balance Scorecard using Key Performance Indicators, Maturity Models, Critical Success Factors, Key Goal Indicators and the Internal Audit Programme. Chapter Four will also highlight the IT risk methodologies for monitoring and measuring internal controls based on CobiT.

Chapter Five proposes a methodology for measuring and monitoring IT risk's internal control using a process approach. The proposed Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC) consists of the following five processes:

1. Identification of business process goals and objectives using the Balance Scorecard as a tool.

2. Measurement of the status of an organization's internal control system by using the Maturity Model.

3. Understanding of the goals and objectives using the Critical Success Factors identified in the Maturity Model.

4. Identification of Key Performance Indicators, the measures necessary in achieving these objectives and goals.

5. Measurement of the outcome of the Key Performance Indicators against Key Goal Indicators.

1.5 Conclusion

The result of the study conducted in this paper proposes a Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC). The reader of this paper will gain an understanding of IT risk's internal control with regard to measurement, monitoring and evaluation of internal controls.

Effective internal control reduces the possibility of errors and irregularities and needs to be consistently applied and thoroughly understood by an organization's staff for the board and senior management policies to be effectively implemented.

Chapter 2

IT Governance and its Drivers: Sarbanes-Oxley and Basel II, the Forces of IT Risk Management

2.1 Introduction

Critically important to the survival and success of any organization is an effective management of information and related Information Technology (IT). This can arise from any of the following:

- Increasing dependence on information and the systems that deliver this information.
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare.
- Scale and cost of the current and future investments in information and information systems.
- Potential for technologies to dramatically change organizations and business practices, create new opportunities and reduce costs.

There are numerous changes in Information Technology (IT) and its operating environment that highlight the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is encouraging stricter control over information, which has been driven by increasing electronic fraud. The management of IT-related risk is now being understood as a key part of corporate governance (Control Objectives, Control and Audit for Information and Related Technology, IT Governance Institute, June 2007).

Managing operational risk of an organization has become an important task of good risk management. The most important types of operational risk include breakdowns in internal controls and corporate governance. These breakdowns can lead to financial losses through error, fraud, or failure to perform in a timely manner. Other

aspects of operational risk include major failures of information technology, systems or events, such as major fires or other disasters (Operational Risk Management, Basle, September 1998).

2.1.1 Corporate Governance

Basel II and Sarbanes-Oxley (SOX) which is a US law passed in 2002, both strengthen corporate governance and restore investor confidence. SOX is applicable to organizations on the US Stock Exchange and Basel II applies to the financial industry.

Corporate governance is defined as the ethical corporate behaviour by directors or others charged with governance in the creation and preservation of wealth for all stakeholders (Control Objectives, Control and Audit for Information and Related Technology, IT Governance Institute, June 2007). It was introduced to promote a coherent management framework and to ensure the implementation of effective information security programmes in organizations. Organizations with these in place can gain competitive advantages over their competitors. Corporate governance also assists in improving business confidence and enhances investor confidence. All organizations listed on the JSE, banks, financial and insurance institutions, public sector organizations that fall under the Public Finance Management Act and the local government need to comply with corporate governance. The main objectives of corporate governance are (King Report, 2002):

- Discipline – commitment by senior management to adhere to behaviour that is accepted to be correct and proper.
- Transparency – ease with which an outsider can make a meaningful analysis of a company's actions.
- Independence – extent at which mechanisms have been put in place to avoid conflicts of interest that may exist.
- Accountability – groups in a company need to be accountable for their decisions and actions.
- Responsibility – behaviour that allows for corrective action.

- Fairness – the rights of various groups have to be acknowledged and respected.
- Social Responsibility – be aware of social issues and ethical standards.

2.1.2 IT Governance

In the 1990s the use of Information Technology (IT) was not that important. Security requirements such as confidentiality and availability were rated low. Therefore, IT security was managed in an isolated manner. In later years due to the increased use of information technology as the enabling factor in almost every business process, information security became an important business function. This has been further strengthened by increased dependence on the Internet as a business channel and communication medium as well as the need to comply with a number of new data privacy laws in order to establish IT governance (IT Governance Institute. CobiT Third Edition – 6 Volume Set).

Within the corporate governance, IT governance is becoming more and more prominent. IT governance can be defined as a structure of relationships and processes to direct and control an organization in order to achieve its goals by adding value while balancing risks versus return over IT and its processes. IT governance is integral to the success of an organization's governance by assuring efficient and effective measurable improvements in related organizational processes. IT governance provides the structure that links IT processes, IT resources and information to organizational strategies and objectives. IT governance is the responsibility an organization's board of directors and senior management. It is an integral part of corporate governance and consists of leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives (Roussay, 1998, ISACA).

The IT Governance Institute (ITGI) was established in 1998 to advance global thinking and standards in directing and controlling organizations' IT. Effective IT governance ensures that IT supports business goals and optimizes business investments in IT, as well as appropriately managing related risks and opportunities.

As stated earlier IT governance is the responsibility of an organization's board of directors and executive management. Boards have the responsibility to establish mechanisms and monitor operations to ensure their organizations achieve their objectives and comply with the law.

The aim of IT governance is to direct IT endeavours, ensuring that they perform according to the following objectives:

- Alignment of IT with the organization and realisation of the promised benefits;
- Use of IT to enable the organization by exploiting opportunities and maximising benefits;
- Responsible use of IT resources;
- Appropriate management of IT-related risks.

The governance process begins with setting objectives for an organization's IT. Then a continuous loop is established for measuring performance and comparing objectives, which normally results in the redirection of activities and a change of objectives where necessary. Objectives are primarily the responsibility of the board and performance measures are that of management, but they should be developed together so that the objectives are achievable and the performance measures represent the objectives correctly. The IT governance framework can be summarized as illustrated in Figure 2 (IT Governance Institute, 2004).

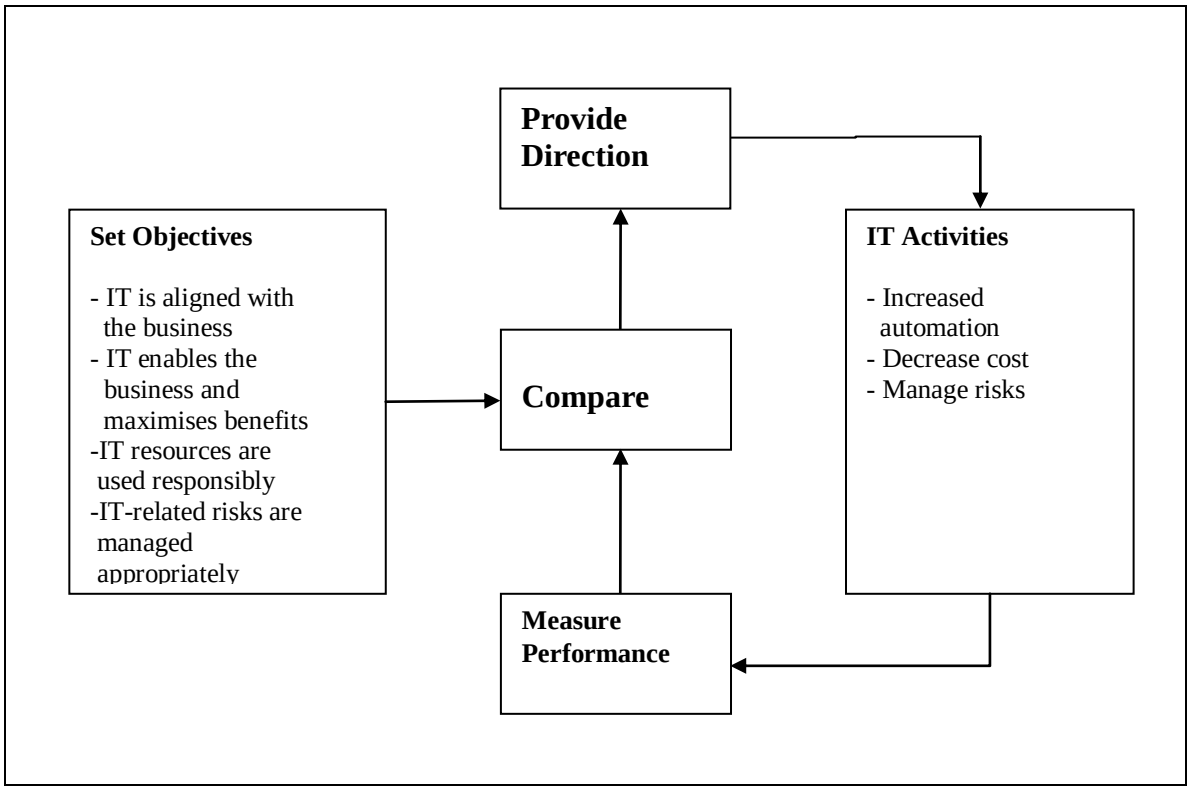

Figure 2 : IT Governance Framework (IT Governance Institute. CobiT Third Edition)

IT governance is mainly concerned with IT's delivery of value to business and mitigation of IT risks. The first is driven by the strategic alignment of IT with the business. The second is driven by embedding accountability into the organization. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

IT governance encourages a number of activities for the board and management, such as becoming informed of the role and impact of IT on the organization, assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance.

2.1.3 The Sarbanes-Oxley Act

The Sarbanes-Oxley (SOX) is a result of a large number of US accounting scandals over a relatively short period of times, beginning with the collapse of Enron in

October 2000. The most prominent area is known as Section 404, which mandates that management establish and report on their control structure. Compliance with Section 404 means implementing a number of information security processes and technologies. Companies are now estimated to spend an average of $3 million each in their compliance efforts.

According to the State of Information Security, 2005, 37% of companies have reported that they have a security strategy in place, however, information security executives are struggling to keep up with security threats and incidents.

SOX is the most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s. Many public companies and the accounting profession have made tremendous progress in meeting the rigorous requirements of this legislation.

Two control frameworks have been widely adopted by organizations subject to the requirements of SOX. These are the Committee of Sponsoring Organizations (COSO) Internal Control Integrated Framework, prepared by the Treadway Commission and released in 1992; and Control Objectives for Information and Related Technology (CobiT), prepared by the US IT Governance Institute. Most companies have turned to CobiT for help in implementing IT controls. CobiT lays out best practices for IT controls, but it is up to each organization to determine which controls make sense for their organization.

2.1.4 New Basel Capital Accord (Basel II)

The complexity of potential risk factors for financial institutions cannot be emphasised enough. Fraud is a risk factor that may result in a financial loss.
The New Basel Capital Accord, more commonly known as Basel II, is about improving risk asset management to avoid financial disasters. Compliance requires all banking institutions to have sufficient assets to offset any risks they may face.

All organizations are exposed to operational risk and the integration of processes, systems and people must be understood and continually monitored to mitigate these

risks. Operational risk is defined by Basel II as: "The risk of direct or indirect loss resulting from in adequate or failed internal processes, people and systems or from external events." Therefore, in order to comply with Basel II, financial institutions will need to have in-depth understanding of all possible risks and their potential impact. This should be an ongoing process and it cannot be regarded as a once-off process.

According to Gartner, compliance with Sarbanes-Oxley and Basel II, is not a software issue but a process one. Financial institutions should gain a complete understanding of their processes, roles and skills employed in the operation of the business through business process modelling (Preparing for the Pain of Basel II, Martin Owen, 2005).

The Basel Committee outlined basic practices in a February 2003 paper, *Sound Practices for the Management and Supervision of Operational Risk*. The paper, together with researchers and risk managers of major banks has helped shape risk management practices for operational risk. Many banks have defined operational risk as any risk not categorized as a market or credit risk, and some have defined it as the risk of loss arising from of human and technical error.

The Basel Committee breaks loss events into seven categories:

i. Internal fraud – loss due to intentional fraud, misappropriating property or circumventing regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party.
ii. External fraud – losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.
iii. Employment practices and workplace safety – losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from discrimination events.
iv. Clients, products and business practice – losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients or from the nature or design of a product.
v. Damage to physical assets – losses arising from loss or damage to physical assets from natural disaster or other events.

vi. Business disruption and systems failures – losses arising from disruption of business or system failures.

vii. Execution, delivery and process management – losses from failed transaction processing or process management from relations with trade counterparts and vendors.

2.2 Risk Management

Risk is the possibility that an event will occur and adversely affect the achievement of objectives. The objective of performing risk management is to enable the organization to accomplish its mission in the following ways (Assessing Risk. Security Risk Management Guide, Microsoft TechNet);

- By better securing the IT systems that store, process or transmit organizational information;
- By enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget;
- By assisting management in authorizing the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organization's mission. Effective risk management must be totally integrated into the System Development Life Cycle (SDLC). An IT systems' SDLC usually has five phases: initiation, development, implementation, operation or maintenance and disposal. An IT system can occupy several of these phases at the same time. Risk management is an iterative process that can be performed during each major phase of the SDLC. The board is responsible for the total process of risk management. Management is accountable to the board for designing, implementing and monitoring the processes of risk management. Management needs to integrate risk management into the day-to-day activities of their organization. The board sets the risk strategy policies in liaison with management and

these policies must be clearly communicated to all employees of the organization. In order to implement a successful risk management programme the following is relied on:

- Senior management's commitment;
- Full support and participation of the IT team;
- Competence of the risk assessment team;
- Awareness and cooperation of the user community;
- Regular evaluation and assessment of the IT-related mission risks.

Risk management encompasses three processes: risk assessment, risk mitigation and evaluation and assessment.

Risk-assessment processes include identification and evaluation of risks and risk impacts and recommendations for risk-reducing measures. Risk identification expects one to know the organization by identifying, classifying and prioritising the information assets. These information assets are targets of various threats and the goal is to protect the assets from the threats. This iterative process begins with identifying all assets, such as people, procedures, data, information, software, hardware and networks. The threats are identified for each information asset and these assets are then listed in order of importance. For each information asset and for each threat it faces, vulnerabilities of each information asset must be identified. The goal of this process is to identify the information assets of the organization that have specific vulnerabilities and list them according to those most needing protection. During this process, a collection of controls in place should also have been identified. At the end of this process a list of information assets and their vulnerabilities should be developed and this list can then be taken into the next process; risk mitigation.

Risk mitigation is a control approach that attempts to reduce the impact caused by exploitation of vulnerability by implementing strategies. Four strategies can be used to mitigate risk: disaster recovery plans, incident response plans, business continuity plans and acceptance. Risk mitigation involves choosing one of the four strategies for

each of the vulnerabilities identified (Stevens, M.W. COCO Enterprise Risk Management),

- A disaster recovery plan is the most common of the mitigation strategies as it includes all the activities in order for an organization to recover from an incident as well as strategies to limit losses before and during the disaster.
- An incident response plan consists of the actions an organization should take while the incident is in progress. The incident response plan focuses on intelligence gathering, information analysis, coordination decision-making and urgent concrete actions.
- A business continuity plan is a long-term plan and encompasses the continuation of business activities when a disaster occurs. It includes planning the steps necessary to ensure the continuation of the organization when the scale of the disaster exceeds the ability of the disaster recovery plan to restore operations.
- Acceptance of risk is the choice to do nothing to protect vulnerability and to accept the outcome of the exploited vulnerability. The following is the only use of acceptance strategy that industry recognises as valid. This happens when the organization determines the level of risk, assesses the probability of attack, estimates the potential damage that could occur from attacks, performs a thorough cost benefit analysis, evaluates controls using each appropriate type of feasibility and decides that the particular information or asset does not warrant the cost of protection.

In most organizations, networks will continually be expanded and updated, their components changed and its software applications replaced or updated with newer versions. Personnel changes and security policies are also most likely to change. These changes ignite new risks, and some risks previously mitigated may become a concern. Thus, risk management is a continuous and evolving activity.

The risk-assessment process should be repeated every three years. This process should be flexible to allow for major changes, such as, to IT systems and processing environments due to changes in policies and new technologies. The risk-management

process should be integrated in the SDLA for IT systems. When doing this an organization's business objectives and/or mission statement are supported. Most organizations have a budget in place to manage every vulnerability through the application of controls therefore each organization needs to define its own level of risk it is willing to take.

2.2.1 Operational Risk

Organizations have always managed operational risk in the past, but there is a need to do so in a more systematic manner in the present climate. In the past, organizations were able to put operational risk and information security in separate departments. Operational risk sat in the audit departments and was reported to the CEO. Information security sat in the IT department and was reported to the CIO.

Currently organizations have been forced through legislation and regulations, such as Basel II (if a bank), and the Turnball Report (if quoted on the London Stock Exchange) or the Sarbanes-Oxley Act (if quoted on the New York Stock Exchange), to have adequate mechanisms for controlling and auditing the flow of information through the organization. If not, the organization will lose money. As a result of this, operational risk and information security have begun to overlap in many organizations.

Operational risks include employee errors, system failures, fires, floods or other losses to physical assets, fraud or other criminal activity. Most operational risks are best managed within the department in which they arise, but overall planning, coordination and monitoring should be provided by a centralized operational risk management department. Operational risks fall into two main categories, risks that occur frequently and with modest loss consequences and risks that occur infrequently but have substantial loss consequences.

Operational risk has gained fresh impetus in the light of Basel II and is a recognised risk management discipline. However, there needs to be a framework of a sound system of internal control, a governance structure and a risk-assessment approach that different management needs can be aligned with and integrated as one.

A variety of techniques is used to control or mitigate operational risk. Internal controls, the major tool for managing operational risk and the internal audit process are seen by most banks as the primary means of doing this. Internal controls are seen as the major tool for managing operational risk (Operational Risk Management, Basel Committee on Banking Supervision, Basle, 1998).

2.3 Internal Control

Internal control is one method used to control or mitigate operational risk and is defined by COSO as a process affected by an entity's board of directors, management or other personnel. It is designed to provide reasonable assurance regarding the achievement of objectives of effectiveness and efficiency in operations, reliability of financial reporting and compliance with applicable laws and regulations. Internal control consists of five interrelated components or standards (Standards for Internal Control in the Federal Government):

i. Control environment – factors include the integrity, ethical values and competence of the entity's people, management's operating style, the way management assigns authority and responsibility and organizes and develops its people.
ii. Risk assessment – every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is the identification and analysis of relevant risks and determining how these risks should be managed.
iii. Control activities – are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of the entity's objectives. Control activities occur throughout an organization at all levels and in all functions.
iv. Information and communication – important information must be identified, captured and communicated in a form and timeframe to enable people to carry out their responsibilities.
v. Monitoring – internal control systems need to be monitored.

Internal control can assist an organization to achieve its performance and profitability targets and prevent the loss of resources. It ensures both reliable financial reporting and organizational compliance with laws and regulations, avoiding damage to its reputation. Everyone in the organization has the responsibility towards internal control as follows (Internal Control Controller's Handbook, January, 2001):

- Management – The Chief Executive Officer (CEO) is ultimately responsible and should direct and lead senior managers in controlling an organization. The senior managers in turn assign responsibilities for the internal control procedures and policies to personnel responsible for that business unit.
- Board of Directors – Management is accountable to the board of directors, which provide governance and guidance. Effective board members should be objective, capable and inquisitive and should have knowledge of the organizational activities.
- Internal Auditors – They play an important role in evaluating and monitoring the effectiveness of the control systems in place.
- Other Personnel – Internal control is the responsibility of everyone in the organization therefore, it should be an explicit part of everyone's job description.

2.4 COSO's Enterprise Risk Management (ERM)

In 2004, COSO released its Enterprise Risk Management Integrated Framework. This framework gives direction to and criteria for improving an organization's ability to manage risk and is fully aligned with COSO's Internal Control Integrated Framework, which is used by most organizations for their reporting under section 404 of Sarbanes Oxley. Section 404 assists organizations to increase their investment in internal control as they make improvements in risk management.

The COSO-based risk assessment has been widely used in the risk management industry for many years, both in financial and non-financial industries. COSO, Enterprise Risk Management aims for a disciplined risk-management environment and can be used as a method of identifying an organization's risk exposure and risk

appetite. The COSO framework requires that an organization establishes a risk appetite, measures actions and decisions against the risk appetite and communicates results to users of the organization's financial information.

ERM is a process conducted by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, which is designed to identify potential events that may affect the entity and manage risks to be within its risk appetite and to provide reasonable assurance regarding the achievement of entity objectives (COSO, Enterprise Risk Management, Martin .W. Stevens, Landskonferanse, 2004).

Enterprise risk management provides a framework for management to effectively deal with uncertainty and its associated risk and opportunity, thereby enhancing its capacity to build value. According to the COSO ERM Framework, enterprise risk management encompasses the following:

- Aligning risk appetite;
- Enhancing risk response;
- Reducing operational surprises;
- Identifying and managing multiple and cross-enterprise risks;
- Seizing opportunities;
- Improving deployment of capital.

The above capabilities of ERM are capable in assisting management to achieve an organization's performance and profitability targets, prevent loss of resources and enhance transparency within the organization.

Table 1 below outlines ERM's process flow in more detail.
(http://www.erm.coso.org/)

Internal Environment Risk Management Philosophy, Risk Culture, Board of Directors, Integrity and Ethical Values, Commitment to Competence, Management's Philosophy and Operating Style, Risk Appetite, Organizational Structure, Assignment of Authority and Responsibility and Human Resource Policies and Practices
Objective Setting Strategic Objectives, Related Objectives, Selected Objectives, Risk Appetite and Risk Tolerance
Event Identification Events, Factors Influencing Strategy and Objectives, Methodologies and Techniques, Event Interdependencies, Event Categories, Risk and Opportunities
Risk Assessment Inherent and Residual Risk, Likelihood and Impact, Methodologies and Techniques and Correlation
Risk Response Identify Risk Responses, Evaluate Possible Risk Responses, Select Response and Portfolio View
Control Activities Integration with Risk Response, Types of Control Activities, General Controls, Application Controls and Entity Specific
Information and Communication Information, Strategic and Integrated Systems and Communication
Monitoring Separate Evaluations and Ongoing Evaluations

Table 1 : ERM's Process Flow

The COSO framework assists organizations by formally organising risk-management responsibilities and activities. If this is done an organization is in a better position to achieve its objectives. Therefore, management will want to ensure that sound risk management processes are in place and functioning.

2.5 Conclusion

CobiT serves as an effective bridge between IT governance and Sarbanes Oxley requirements. CobiT takes the COSO framework and fills in control information that is appropriate for most organizations. CobiT has been developed as a generally applicable and accepted standard for good IT security and control practices and provides a referenced framework for management, users, auditors and security practitioners. CobiT is becoming increasingly popular as a good practice for control over information and IT-related risks.

A manager responsible for information security should be familiar with corporate governance concepts, setting up transparency in operations and adopting a structured framework for analysis and documentation, such as that offered by CobiT (SANS Institute, 2004).

Internal control is a major part of managing an organization. It comprises of the plans, methods and procedures used to meet missions, goals and objectives. Internal control also serves as the first line of defence in safeguarding assets and preventing and detecting errors and fraud. Internal control is a series of actions and activities that occurs throughout an organization's operations on an ongoing basis.

In the following chapter internal control will be explained further and standards, methodologies, guidelines and frameworks of CobiT, COSO, ITIL and ISO17799 pertaining to internal control will be investigated.

Chapter 3

Standards, Methodologies, Guidelines and Frameworks of CobiT, COSO, ITIL and ISO17799 Internal Control

3.1 Introduction

Organizations have recently demonstrated increasing interest in and the adoption of best practices and standards for IT governance. These include the CobiT Framework, ISO 17799 for security and IT Infrastructure Library (ITIL) for service delivery.

According to the King Report, 2002, a board of directors of an organization must ensure that there is effective communication of its strategic plans and ethical code, both internally and externally. The board must see to it that adequate internal control and the management of information systems can cope with the strategic direction in which the organization is heading.

As stated in Chapter 2, internal control is a major part of managing an organization. It comprises the plans, methods and procedures used to meet missions, goals and objectives. Internal control also serves as the first line of defence in safeguarding assets and preventing and detecting errors and fraud. Internal control is not a single event, but a series of actions and activities that occur throughout an organization's operations on an ongoing basis. According to Standards for Internal Control in the Federal Government, United States, internal control should provide reasonable assurance that the objectives of the organization are being met in the following categories:

- Effectiveness and efficiency of operations including the use of the entity's resources;
- Reliability of financial reporting, including reports on budget execution, financial statements and other reports for internal and external use;
- Compliance with applicable laws and regulations.

How can information technology be controlled so that it delivers the information an organization needs? How are risks managed to secure the infrastructure on which organizations are dependent? As with the many issues management faces, these strategic questions needs answers. CobiT, COSO, ITIL and ISO17799 address these issues and answer many of management's questions.

3.2 Internal Control

As highlighted earlier in Chapter 2, internal control consists of policies and procedures designed to provide reasonable assurance that a business entity achieves its objectives and goals. These procedures are often called controls and collectively are referred to as the organization's internal controls. In an organization, goals and objectives are presented in a strategic plan that includes a mission statement. If an organization does not have objectives and goals, then there is no need for internal control, thus setting goals and objectives are preconditions for internal controls.

Several key points need to be highlighted pertaining to internal control. Internal control is a process and is effected by people at every level within an organization. It can provide only reasonable assurance to the achievements of the organization's operations, financial and compliance objectives but will assist in attaining these.

All organizations today need internal control as they are confronted with various types of business risks, both internally and externally. Internal control can limit these risks. An organizations typical business risks can include the following:

- Strategic risks, which affect the overall direction of the organization.
- Financial risks, which involve safeguarding assets.
- Operational risks, which impact the processes that govern daily operations.
- Regulatory risks, which apply to compliance with laws and regulations.
- Reputation risks, which affect the organization's public image.

Good internal control systems should include the following:

- Segregation of duties;
- Reconciliation;
- Authorisation;
- Access Restriction;
- Monitoring and supervision;
- Business interruption recovery;
- Knowledge and training.

The board and management are primarily responsible for implementing internal controls and each department's employees establish, document and maintain them within their departments. Therefore, all employees of an organization are responsible for compliance to the internal controls implemented.

Controls can be classified as either preventive or detective. Preventive controls attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are proper authorization, adequate documentation and physical control over assets. Detective controls attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent one from occurring. Examples of detective controls are reviews, analysis, physical inventories and audits. Both of these controls are essential to an effective internal control system (Standards for Internal Control in the Federal Government, 1999, Internal Control).

Control activities can include the following:

- Approvals, authorisations and verifications (Preventive controls);
- Reconciliations (Detective control);
- Reviews of performance (Detective control);
- Security of assets (Preventive and Detective control);
- Segregation of duties (Preventive control);
- Control over information systems (Preventive and Detective control).

Control of an information system generally has two different categories, general controls and application controls. General controls include, controls over data operations, system software acquisition and maintenance, access security and application system development and maintenance. Application controls include computer edit checks which are programmed steps within application's software. They are designed to help ensure the completeness and accuracy of transaction processing, authorization and validity. General controls are needed to support the functioning of application control and both are needed to ensure a complete and accurate information processing system.

An organization's internal control can, therefore, be summarized as activities which address the organization's risks previously identified from its business objectives and goals. In order for management to achieve its objectives and goals, management needs to effectively balance risks and controls. By doing this reasonable assurance can be attained. As stated in Chapter 2, when an organization does not balance its risks and controls, excessive risks and controls can occur, which can be detrimental to any organization.

3.3 CobiT

CobiT (Control Objectives for Information and related Technology) was developed and promoted by the IT Governance Institute. CobiT is designed to be used for three distinct audiences; management, users and auditors. The main objective of CobiT is the development of clear policies and good practices for security and control in IT.

The four domains identified for high-level classification are:

- Planning and organization - This domain covers strategy and tactics and concerns the identification of the way IT can best contribute to the achievement of the business objectives and applies to top-level management.

- Acquisition and implementation – To realise the IT strategy, IT solutions need to be identified, developed, acquired, implemented and integrated into the business process. This level applies to senior management.

- Delivery and support – This domain is concerned with the actual delivery of required services which range from traditional operations for security and continuity aspects of training. This level applies to middle management.

- Monitoring – All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses management's oversight of an organization's control process and independent assurance provided by internal and external audits. This level applies to the operational level of the organizational structure.

The CobiT framework has 34 IT processes divided into four IT domains as highlighted in Figure 4. Each of the 34 IT processes is broken down into the following, control objectives, control practices, management guidelines and audit guidelines. Each control objective is sub-divided into a list of detailed control objectives. CobiT therefore has 318 detailed control objectives for its 34 IT processes. This structure covers all aspects of information and the technology that supports it. By addressing these 34 control objectives an organization can be assured that an adequate control system is provided for its IT environment.

The IT control practices provide the more detailed "how" and "why" issues needed by management, end users and control professionals to implement highly specific controls, based on an analysis of operational and IT risks.

The CobiT management guidelines provide the vital link between IT control and IT governance. They are action-orientated and provide management direction for bringing the organization's information and related processes under control. The management guidelines include the use of the following measuring tools; maturity models (MMs), critical success factors (CSFs), key goal indicators (KGIs) and key performance indicators (KPIs).

The audit guidelines outline and suggest the assessment activities to be performed corresponding to each 34 IT control objectives and provides helpful guidance on who to interview, what questions to ask, and how to evaluate control, access compliance and substantiate the risk of any identified controls not being met. Audit guidelines provide invaluable guidance for the audit team.

CobiT has been developed as a generally applicable and accepted standard for good IT security and control practices that provide a referenced framework for management, users, auditors and security practitioners. CobiT is becoming increasingly internationally accepted as good practice for control over information, IT and related risks.

Figure 3 on the following page graphically highlights, IT processes defined within CobiT's four domains.

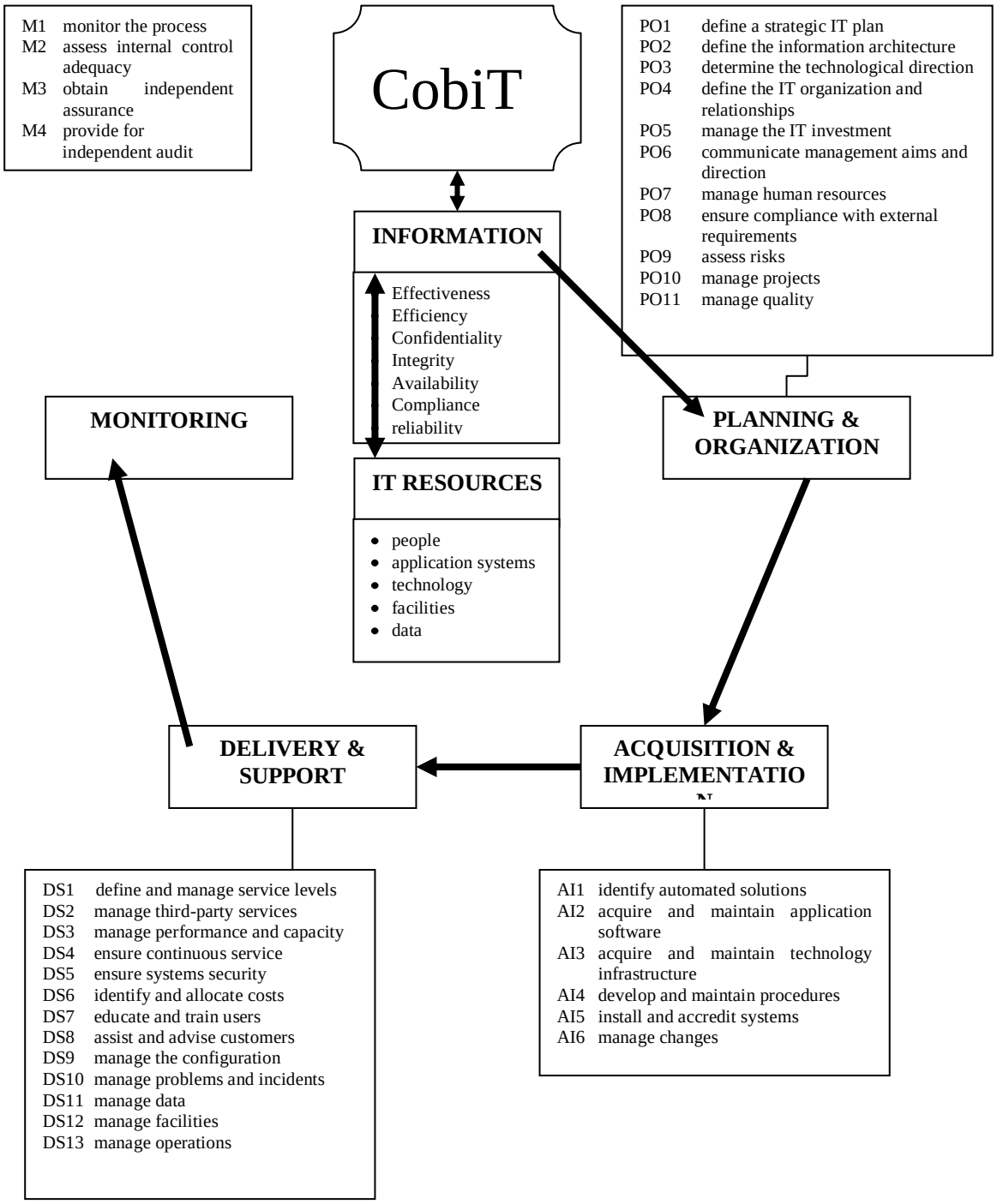

Figure 3 : CobiT, IT processes defined within the four domains

Control in IT is approached by looking at both information that is needed to support the business objectives and by looking at information resulting from the combined application of IT-related resources that need to be managed by IT processes. In order to satisfy business objectives, information needs to conform to certain criteria, which CobiT refers to as business requirements for information. These are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability. The IT resources identified in CobiT are defined as follows:

- People – include staff skills, awareness to plan, organise, acquire, deliver, support and monitor information systems and services.
- Application systems – manual and programmed procedures.
- Technology – hardware, operating systems, database management systems, networking, multimedia, etc.
- Facilities – are all the resources to house and support information systems.
- Data - are internal and external objects, structured and non-structured, graphics, sound, etc.

The main focus of CobiT is the development of clear policies and good security and control in IT for worldwide endorsement by commercial, governmental and professional organizations. Its primary goal is the development of control objectives primarily from the business objectives and needs perspective. This approach is compliant with the COSO perspective, which is first and foremost a management framework for internal controls (CobiT in Academia, IT Governance Institute,2007).

3.4 COSO

The Committee of Sponsoring Organization of the Treadway Commission (COSO) Internal Control – Integrated Framework relates to the effectiveness of internal control over financial reporting. COSO provides a framework of reasonable assurance regarding the achievement of the organization's objectives and internal control over the preparation of published financial statements.

Section 404 of the Sarbanes-Oxley Act of 2002 requires management to annually assess and report on the effectiveness of internal control over financial reporting. COSO recognises section 404 of the Act as a major driver of an organization's evaluation of internal control over financial reporting. COSO urges companies to reduce costs not by reducing the effectiveness of internal control but by recognising that internal control over financial reporting may be achieved by selecting approaches that best fit each organization's circumstances in the most cost-effective manner.

COSO defines formal controls as those which are performed in accordance with policies established by an organization and assist the organization in carrying out its control procedures and training of personnel. Informal controls are difficult to apply on a consistent basis.

COSO further formalizes controls in the context of three models.

- Management reliance only – When management relies on internal controls solely for running the business, controls and supporting documentation are often less formal in part due to greater concentration of decision-making authority, wider spans of control and more direct channels of communication.

- Management assertion – When management is required to assert to a third party on the design and operating effectiveness of internal control, it will need information on the design and operation of internal controls.

- Third-party attestation – When management is required to have a third party, such as external auditors, attest to the design and operating effectiveness of internal control and key processes, the need for formal documentation and evidence of operation increases to allow the third party to review after the fact (COSO-Integrated Framework for Internal Control).

In determining how to deal with the issue of formal versus informal controls, the COSO Task Force made the following decisions:

- There is no correct approach to achieving effective internal control over financial reporting; that is, a control should accomplish the objective set forth in a principle and there are many ways to do that.

- Publicly held companies currently are required to provide evidence that controls are working therefore, this guidance supports implementation of more formal controls when public reporting on internal controls is required.

- The process of understanding and documenting internal control assists companies in mitigating risks.

The COSO framework for internal control states that internal control is a process, established by an organization's directors, management and other personnel to provide reasonable assurance regarding the achievement of the COSO's stated objectives. COSO assigns fundamental principles to the already identified interrelated components of internal control: control environment, risk assessment, control activities, information and communication and monitoring. The fundamental principles address the implementation of effective internal control over financial reporting. Achievement of the principles, listed in Table 2a and 2b, would highlight that controls are in place throughout the organization.

Controls	Principles
Control Environment	1. **Integrity and Ethical Values –** Sound integrity and ethical values, particularly of top management are developed and set the standard of conduct for financial reporting. 2. **Importance of Board of Directors –** The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control. 3. **Management's Philosophy and Operating Style –** Management's philosophy and operating style support achieving effective internal control over financial reporting. 4. **Organizational Structure –** The company's organizational structure supports effective internal control over financial reporting. 5. **Commitment to Financial Reporting Competencies –** The company retains individual competent in financial reporting and related oversight roles. 6. **Authority and Responsibility –** Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting. 7. **Human Resources –** Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Risk Assessment	8. **Important of Financial Reporting Objectives –** A Precondition to risk assessment is the establishment of objectives for reliable financial reporting. 9. **Identification and Analysis of Financial Reporting Risks –** The company identifies and analyses risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed. 10. **Assessment of Fraud Risk** – The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.
Control Activities	11. **Elements of a Control Activity –** Policies and procedures are established and communicated throughout the company, at all levels and across all functions that enable management directives to be carried out. 12. **Control Activities Linked to Risk Assessment** – Actions are taken to address risks to the achievement of financial reporting objectives. 13. **Selection and Development of Control Activities** – Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives. 14. **Information Technology** – Information Technology controls, where applicable are designed and implemented to support the achievement of financial reporting objectives.

Information and Communication	15. **Information Needs** – Information is identified, captured and used at all levels of a company to support the achievement of financial reporting objectives. 16. **Information Control** – Information relevant to financial reporting is identified, captured, processed and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives. 17. **Management Communication** – All personnel, particularly those in roles affecting financial reporting, receive a clear message from top management that both internal control over financial reporting and individual control responsibilities must be taken seriously. 18. **Upstream Communication** – Company personnel have an effective and no retributive method to communicate significant information upstream in a company. 19. **Board Communication** - Communication exists between management and the board of directors so that both have relevant information to fulfil their roles with respect to governance and financial reporting objectives. 20. **Communication with Outside Parties** – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Monitoring	21. **Ongoing Monitoring** – Ongoing monitoring processes enable management to determine whether internal control over financial reporting in present and functioning. 22. **Separate Evaluations** – Separate evaluations of all five internal control components enable management to determine the effectiveness of internal control over financial reporting. 23. **Reporting Deficiencies** – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate.

Table 2a : COSO's Implementation Controls and Principles

In addition to the above principles, COSO has identified three principles relating to the roles that various parties play with regard to internal control over financial reporting, and how these roles translate into specific responsibilities. The roles and responsibilities are directly derived from the 1992 guidance and listed in Table 2b.

Roles and Responsibilities	24. **Management Roles** - Management exercises responsibility and ownership for internal control over financial reporting. 25. **Board and Audit Committees** - The board of directors perform their oversight responsibilities relating to the achievement of effective internal control over financial reporting. 26. **Other Personnel** – All company staff accept responsibility for actions that directly or indirectly impacts financial reporting.

Table 2b : Roles and Responsibilities

COSO presents a common definition of internal control and emphasises that internal controls assist organizations achieve effective and efficient operations, reliable financial reporting and compliance with applicable laws and regulations (COSO, Internal Control – Integrated Framework, October 2005).

3.5 ITIL

The ITIL framework provides an effective foundation for quality IT service management. An organization considering improving their service delivery should start with ITIL. ITIL has rapidly been adopted across the world as the standard for best practice in the provision of IT service.

Organizations are becoming increasingly dependent on IT in order to satisfy their corporate aims and meet their business needs, which has led to an increased requirement for high quality IT services. The ITIL provides the foundation for quality IT Service Management (ITSM). The main focus of ITSM is divided into two areas, service support and service delivery.

3.5.1 ITIL Service Support

ITIL service support is the practice of disciplines that enables IT services to be provided effectively. The service support disciplines are listed below:

- Configuration management is the implementation of a database that contains details of an organization's elements that are used in the provision and management of its IT services.
- Incident and problem management is the resolution and prevention of incidents that affect the normal running of an organization's IT services.
- Change management is the practice of ensuring all changes to configuration items are carried out in a planned and authorised manner.
- Service/Help desks play an important part in the provision of IT services. The two main focuses are incident control and communication.
- Release management is the management of all software configuration items within an organization. It is the management of software development, installation and support of an organization's software products.

3.5.2 ITIL Service Delivery

Service delivery is the management of IT services and involves a number of management practices to ensure that IT services are provided as agreed between the service provider and the customer. Service delivery consists of five disciplines:

- Service level management is the primary management of IT services ensuring that agreed services are delivered when and where they are supposed to be delivered.
- Capacity management is the discipline that ensures IT infrastructure is provided at the right time, in the right volume and at the right price, and ensures that IT is used in the most efficient manner.
- Continuity management is the process by which plans are put in place and managed to ensure that IT services can recover and continue should a serious incident occur.

- Availability management is the practice of identifying levels of IT service availability for use in service level reviews with customers.
- IT financial management is the discipline of ensuring IT infrastructure is obtained at the most effective price (which does not necessarily mean the cheapest) and calculating the cost of providing IT services.

ITIL is a consistent and comprehensive document of best practice for IT service management, in use by many organizations around the world. ITIL can be trusted to provide guidance on the provision of quality IT services needed to support IT (ITIL Service Level Management, 2005).

3.6 ISO 17799

Information security is the protection of information from a wide range of threats which ensures business continuity, minimizes business risk and maximises return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved upon where necessary, to ensure that the specific security and business objectives of an organization are met (ISO/IEC 17799:205, South African National Standard).

ISO/IEC 17799 is a code of practice for information security management and is also known as BS 7799. ISO/IEC 17799 was created by the British Standards Institute together with the input from other international organizations. ISO/IEC 17799 is a combination of best information security practices in general use in many leading international organizations. ISO/IEC 17799 has been accepted as a national standard by many countries and has been translated into more than 15 languages.

ISO/IEC 17799 consists of 11 control clauses, 39 main security categories and 133 controls and one introductory clause introducing risk assessment and treatment. Each of the 11 security control clauses contains a number of main security categories included within each clause, highlighted in brackets as follows:

1. Security policy (1)
2. Organising information security (2)
3. Asset management (2)
4. Human resources security (3)
5. Physical and environmental security (2)
6. Communications and operations management (10)
7. Access control (7)
8. Information systems acquisition, development and maintenance (6)
9. Information security incident management (2)
10. Business continuity management (1)
11. Compliance (3)

Each main security category contains:

- ✓ A control objective stating what is to be achieved;
- ✓ One or more controls that can be applied to achieve the control objective

The control objectives of the international standard are intended to be implemented to meet the requirements identified by the risk-assessment process.

Risk assessment and treatment consists of:

- Assessing the security risks – Risk assessments should identity, quantify and prioritize risks against a criterion for risk acceptance and the objectives of an organization. The results should determine the appropriate management action and the implementation of controls to protect against these risks. Risk assessment should be performed periodically to address changes in the security requirements and in the risk situation.

- Treating the surety risks – An organization needs to determine criteria whether or not risks can be accepted. For each risk identified during the risk-assessment process: a risk-treatment decision needs to be made such as

appropriate controls to reduce the risk, accepting risks, avoiding risks and transferring the associated risk to other parties, e.g., insurers or suppliers.

In applying appropriate controls to risks, these controls should be selected and implemented to meet the requirements identified by the risk assessment. Controls should ensure that risks are reduced to an acceptable level.

According to ISO/IEC 17799, information security controls should be considered at the systems requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions. It should also be kept in mind that no set of controls can achieve complete security and that additional management action should be implemented to monitor, evaluate and improve the efficiency and effectiveness of security controls to support an organization's objectives.

3.7 A Process Approach to Information Security

As per ISO/IEC 17799, 2000, information is defined as an asset which like other important business assets adds value to the organization and consequently needs to be protected. In today's information technological world there is a growing demand for security solutions. Information systems are becoming more vulnerable because of increased complexity and the interconnection of insecure components and networks.

ISO17799, 2000 defines the purpose of information security as to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. An organization can ensure good security by implementing ISO/IEC standards.

ISO27001 is a global standard for Information Security Management System (ISMS) and is the only certifiable standard for ISMS requirements against which organizations are formally certified. The ISO27001 standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

CobiT's referenced framework of 34 IT processes uses a process approach to the development of clear policies and good practices for security and control in IT and is compliant with COSO's management framework for internal controls. COSO clearly states that internal control is a process which is established by an organization's directors, management and other personnel. It provides reasonable assurance to the organization when implementation of COSO's 26 principles are achieved.

Information security management is, therefore, a complete process of securing all the information services and consists of a number of processes such as information security policy, risks analysis, risk management, contingency planning and disaster recovery. As discussed in Chapter 2, risk management is a process comprising of risk assessment, risk mitigation and evaluation and assessment and is the responsibility of the board of directors. In using a process approach to information security compliance, organizations will not only address identified risks but also comply with the law.

3.8 Conclusion

With the increase in government information security requirements, organizations are viewing information security as a regulatory compliance. Threat of fines and penalties to organizations has also increased the implementation of comprehensive information security policies, and many organizations are wanting to comply with international laws and regulations.

An effective and efficient system of internal control is vital to an organization in order for it to achieve its objectives and goals. CobiT and COSO have become acceptable standards for good information technology security and control practices. CobiT and COSO contain many of the same internal control concepts. CobiT is more directed to three distinct audiences, management, users and information systems auditors and COSO is more directed to managers and boards of directors.

How does an organization know that it has sufficient internal controls in place? It cannot manage IT risk exposure unless it measures and monitors progress. It is very important to measure and monitor internal controls to ensure that they mitigate the IT

risks to an acceptable and adequate level. Measurement methods need to be in place in order to measure whether an organization's internal controls are sufficient or adequate to provide assurance that risk has been successfully addressed. Chapter 4 will research the history of measurement methods and discuss the IT risk methodologies for monitoring and measuring internal controls based on CobiT.

Chapter 4

Monitoring and Measuring Internal Control

4.1 Introduction

Information security governance has become an essential part of overall corporate governance activities. To ensure effective governance of an organization's information security activities, business-aligned metrics and measures need to be developed, implemented, monitored and reported to management. This ensures that the risk management and business goals of the organization are being met and the information infrastructure of the organization is secure (Developing Metrics for effective Information Security Governance, John P. Pironti, Information Systems Control Journal, Vol2, 2007).

An internal control procedure may be well designed and correctly implemented initially, but with time it may lose its effectiveness and efficiency due to environmental changes. Therefore periodic checks of an organization's internal control system (ICS) are necessary.

It is imperative that management can determine by certain measurement methods whether the ICS is achieving the objectives of its organization. The problem facing senior management today with regard to controls can be highlighted as follows:

- Do the controls work?
- Are they cost effective?
- Are the controls performed correctly?
- Are there sufficient controls in place?

The objective of this chapter is to research the history of measurement methods and identify methodologies of monitoring and measuring internal controls. In order for management to achieve its organizational goals, it needs to effectively balance risks

and controls. By doing this it can attain reasonable assurance that risks have been addressed.

Internal controls need to be proactive, value-added, cost effective and also monitored over time. As highlighted before the purpose of monitoring is to determine whether internal controls are adequately designed, properly executed and effective. Just as control activities help to ensure that actions to manage risks are carried out, monitoring helps to ensure that control activities and other planned actions which effect internal control, are carried out properly and timeously and that the end result is an effective ICS.

There are a number of measurement methods available to management which are capable of mitigating organization's IT risks to an acceptable and adequate level such as the balance scorecard using key performance indicators (KPIs), the maturity model (MM) and critical success factors (CSFs).

4.2 Using the Balance Scorecard with Key Performance Indicators (KPIs)

The Balance Scorecard developed in the 1990s by Robert S. Kaplan and David P. Nortan is a measurement system that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal business processes and external outcomes and supplies key indicators to management.

Kaplan and Nortan describe the innovation of the Balance Scorecard as follows: "*The Balance Scorecard retains traditional financial measures. But financial measures tell the story of past events, and adequate story for industrial age companies for which investments in long-term capabilities and customer relationships were not critical for success. These financial measures are inadequate, however, for guiding and evaluating the journey information age companies must make to create future value through investment in customers, suppliers, employees, processes, technology and innovation.*" (www.balancescorecard.org/basics)

The main objective of the Balance Scorecard is to reflect the strategy of the organization and indicates how well the organization is performing using both financial and non-financial measures, these measures being the KPIs. The traditional Balance Scorecard is created with the following critical steps:

1. Develop a vision for the organization;
2. Understand the CSFs and an evaluation of risk factors;
3. Identify business objectives;
4. Define adequate performance measures (KPIs);
5. Develop appropriate information systems;
6. Implement the process.

The Balance Scorecard views an organization from four perspectives learning and growth, internal process, customer and financial as highlighted in Figure 4.

For each of the four perspectives, objectives/goals can be established and relevant measures assigned to each objective/goals, which leads to the information needed to measure the achievement of the objectives/goals.

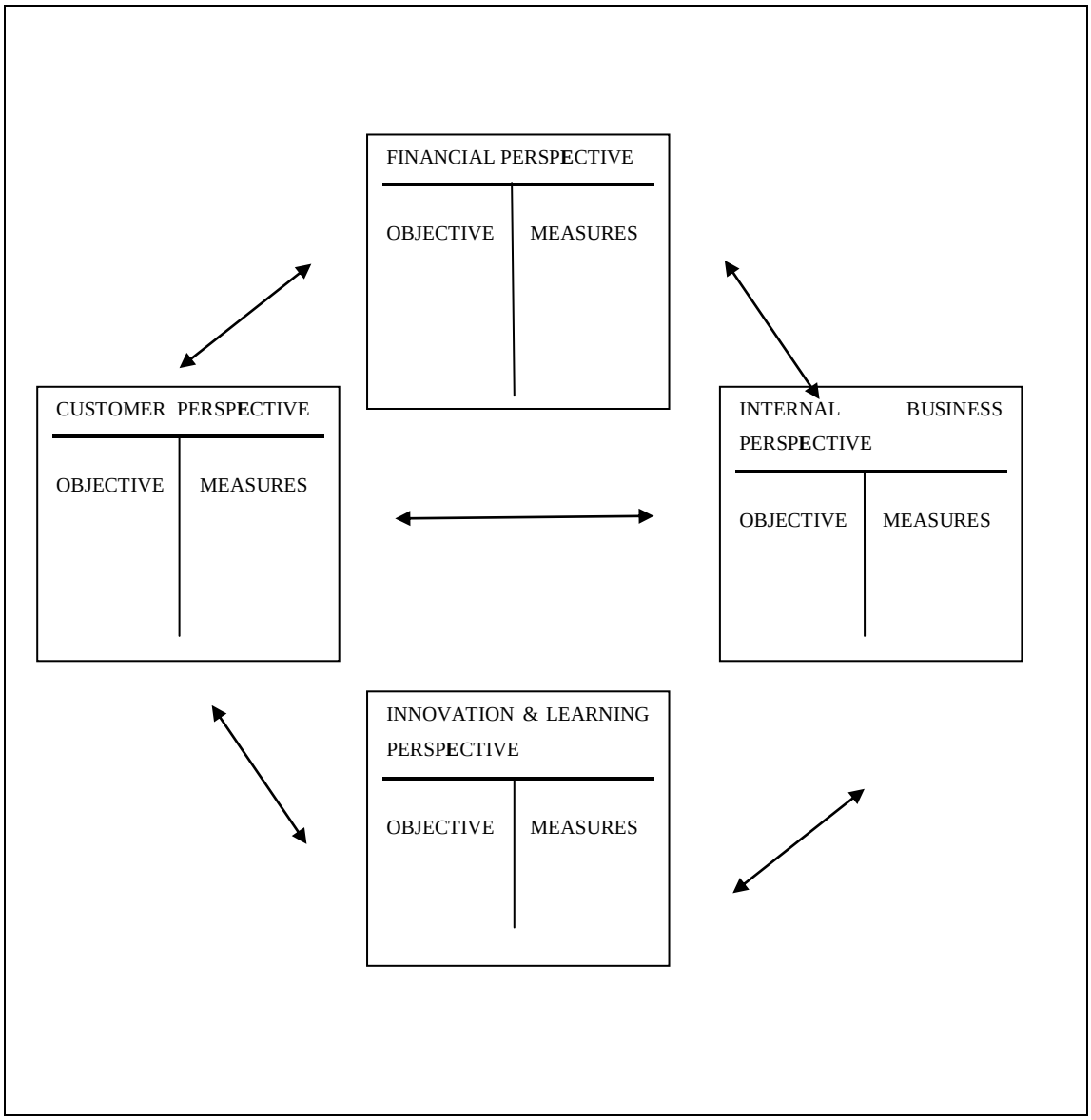

Figure 4 : The Balance Scorecard (Ward and Peppard, Strategic Planning for Information Systems, 3rd edition, 2002)

When an organization uses the Balance Scorecard in risk management, it assists managers to better monitor their organization's performance while controlling and managing risks. Use of a Balance Scorecard also identifies the information required to measure performance against business objectives. The outputs of a Balance Scorecard can be a comprehensive set of information system requirements as it links measures to business objectives. It has been a popular tool for managing and monitoring an organization's performance.

KPIs are one of the most effective tools that can be used to measure the effectiveness of an organization's controls. When designed and implemented correctly KPIs provide an organization with valuable metrics and measures to help determine the effectiveness of its threats and its information security programme (Information System control Journal, Volume 2, 2007).

For each of the four perspectives discussed in the Balance Scorecard, the objectives established needs relevant measures as to how the organization is going to meet them. These measures are referred to as the KPIs and this is the information which is used by the organization to measure its performance.

The use of the Balance Scorecard has become widespread as a performance measurement and management tool. The evaluation of an organization should not be restricted to a traditional financial evaluation, but should be supplemented with measures concerning customer satisfaction, internal processes and learning and growth. Results achieved within these perspectives can ensure future financial results and drive the organization towards its strategic goals while keeping all four perspectives in balance (Information systems control Journal, Volume 2, 2005).

4.3 Using the Maturity Model (MM)

IT management is always on the lookout for a tool to measure progress against a goal or objective. The MM satisfies this need by allowing management to benchmark its goals.

The MM can be used to access the overall IT control environment and describes the stages of maturity that an organization may go though in developing a thorough level of control and quality. The concept of MMs can be traced back to the pioneering work of Philip Crosby. The Software Engineering Institute (SEI) developed the "Capability Maturity Model (CMM)". SEI (2002) and identifies its purpose: "*To provide guidance for improving an organization's processes and the ability to manage the development, acquisition and maintenance of products and services.*
The five stages of the MM process are as follows (Measuring Operational Risk Management Systems under Basel II, Patrick Mc Connel, 2004):

1. Initial – processes are usually ad hoc and chaotic.
2. Managed – processes are planned, performed, measured and controlled.
3. Defined – processes are well characterized and understood and are described in standards, procedures, tools and methods.
4. Quantitatively managed – processes are predictable in that quality and process performance are understood in statistical terms and are managed throughout the life of the processes.
5. Optimising – processes are continually improved based on a quantitative understanding of the common causes of variation inherent in processes.

Organizations usually move through the five stages of maturity from where there is little understanding of a process through increased understanding and measurement to fully understanding a process. In order for any organization to achieve stage five of the MM, would require strong support from senior management, good working relationships, strong leadership, trust and effective communication, as well as a thorough understanding of the business environments. Table 3 highlights an example of a MM showing the status of the internal control environment and the establishment of internal controls in an organization.

MATURITY LEVEL	STATUS OF THE INTERNAL CONTROL ENVIRONMENT	ESTABLISHMENT OF INTERNAL CONTROLS
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/ad hoc	There is some recognition of the need for internal control. The approach to risk and control requirements is ad hoc and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an ad hoc basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and

	Many control weaknesses exist and are not adequately addressed, the impact can be severe. Management's actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed action plan.
3 Defined processes	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there are an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could be severe. Employees are aware of their control responsibilities.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment improvement plan.
4 Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented	IT process critically is regularly defined with full support and agreement from relevant business

4 Managed and measurable continued	evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited tactical use of technology is applied to automate controls.	process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprise risk and control programme provides continuous and effective risk and control issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm the controls are in the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls

	compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analysis. Employees are proactively involved in control improvements.	more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Table 3: Maturity Model (MM) for Internal Control (CobiT 4.0, IT Governance Institute, 2005)

When using the MM approach it is relatively easy for managements to place them on the scale and understand what is involved if they need to improve their performances. With the assistance of the MM scales, professionals can easier explain to managers where IT management's shortcomings exist and set targets for where they need to be in relation to IT governance, security and control.

4.4 Critical Success Factors (CSFs)

CSFs should be set against each objective of the organization. Once this has been done CSFs can then be ranked according to their importance. Only then should the importance of information or systems in achieving the CSFs be considered. Too many CSFs for an objective could highlight that the objective is unachievable. CSFs forces management of an organization to analyse its strengths, weaknesses, opportunities and threats and ensures the correct understanding of its mission and objectives.

The output from the Balanced Scorecard and the CSFs can be combined to provide a more comprehensive set of information security requirements. The Balance

Scorecard links measures (KPIs) to business objectives, while CSFs identify what is critical to achieving the KPIs. This is highlighted in Figure 5.

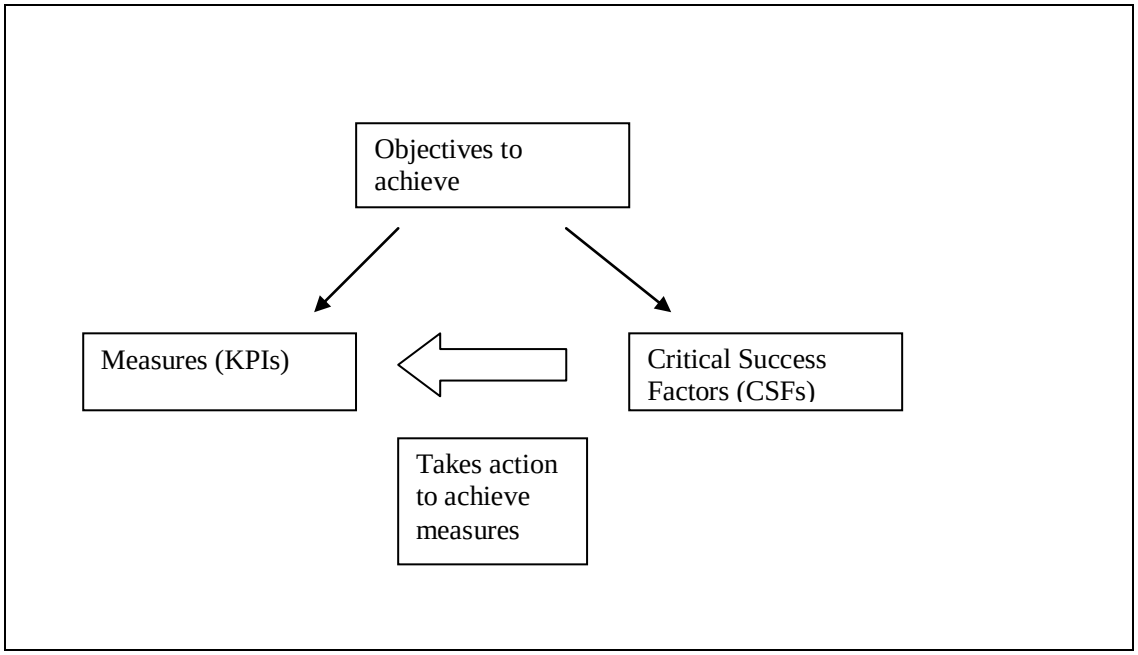

Figure 5 : Critical Success Factors (CSFs)

4.5 The Internal Audit Program

The Sarbanes-Oxley Act of 2002 declares that management is legally responsible for establishing, evaluating and monitoring the effectiveness of internal control over the financial reporting process. These regulations have increased more stringent financial and internal controls within organizations. The regulations require businesses to possess evidence of business strategy and evidence of internal controls to protect valuable assets.

An audit is basically a review of past history. An IS auditor is expected to follow the defined audit process, establish audit criteria, gather meaningful evidence and render an independent opinion about internal controls.

Internal auditing is an independent appraisal function established within an organization to examine and evaluate the adequacy and effectiveness of the organization's internal control system. Internal auditing gives senior management analysis, appraisals, recommendations and information regarding the activities reviewed. Internal auditing reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, economical use of resources and established operational objectives. According to the National Commission on Fraudulent Financial Reporting (Treadway Commission), every public corporation should have an internal audit function.

Internal auditors are the key to an organization's success in today's business world. They provide useful professional advice to all levels of management. Today's auditors have extensive knowledge of computer systems and the Internet. The auditors ensure that policies and procedures are carried out effectively and that risks are kept to a minimum.

According to the IT Governance Institute the general structure of the audit guidelines are as follows:

- provides management with reasonable assurance that control objectives are being met;
- where there are significant control weaknesses, to substantiate the resulting risks;
- advise management on corrective actions.

The generally accepted structure of the audit process is:

- identification and documentation;
- evaluation;
- compliance testing;
- substantive testing.

The IT process is, therefore, audited by:

- obtaining an understanding of business requirements related risks and relevant control measures;
- evaluating the appropriateness of stated controls;
- assessing compliance by testing whether the stated controls are working as prescribed, consistently and continuously;
- substantiating the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources.

4.6 Monitoring and Measuring Internal Control in CobiT

All IT processes need to be regularly assessed for compliance with control requirements. CobiT's IT domain, Monitor and Evaluate, addresses performance management, monitoring internal control, regulatory compliance and providing governance. Management has a role to ensure that internal controls are effectively in

place. This domain is listed below in Figure 6 highlighting the four control objectives.

Monitor and Evaluate	
ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

Figure 6: CobiT's domain Monitor and Evaluate

This domain deals with the organization's strategy in assessing the needs of the company whether or not the current IT system meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of the IT system in its ability to meet business objectives and the organization's control processes by internal and external auditors.

CobiTs' Monitor and Evaluate domain's four control objectives are explained further in 4.6.1 to 4 (CobiT 4.0, IT Governance Institute, 2007).

4.6.1 ME1 Monitor and Evaluate IT Processes

This process includes defining relevant performance indicators, a systematic and timely reporting of performance and prompt action on deviation. Monitoring is needed to make sure that the correct actions are taken and are in line with the set policies and procedures. The process focuses on the monitoring and reporting process metrics and identifying and implementing the performance improvements actions.

This process is measured by:

- the satisfaction of management and the governance entity with the performance reporting;
- number of improvement actions driven by monitoring activities;
- percent of critical processes monitored.

4.6.2 ME2 Monitor and Evaluate Internal Control

This process includes the monitoring and reporting of control exceptions, results of self assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

This process is measured by:

- number of major internal control breaches;
- number of control improvement initiatives;
- number and coverage of control self-assessments.

4.6.3 ME3 Ensure Regulatory Compliance

Effective regulatory oversight requires the establishment of an independent review process to ensure compliance with laws and regulations. This process includes defining an audit charter, audit independence, professional ethics and standards, planning performance of audit work and reporting and follow-up of audit activities. The purpose of this process is to provide positive assurance related to IT compliance with laws and regulations.

This process is measured by:

- cost of IT non-compliance, including settlements and fines;
- average time lag between identification of external compliance issues and resolution;
- frequency of compliance reviews.

4.6.4 ME4 Provide IT Governance

Establishing an effective governance framework includes defining organizational structures, processes, leadership roles and responsibilities to ensure that enterprise IT investments are aligned to and delivered in accordance with enterprise strategies and objectives.

This process is measured by:

- frequency of board reporting on IT stakeholders;
- frequency of reporting from IT to board;
- frequency of independent reviews of IT compliance.

4.7 CobiT's Management Guidelines

As stated earlier in Chapter 3, the management guidelines provide the vital link between IT control and IT governance. The management guidelines include the use of the following measuring tools; MMs, CSFs, KGIs and KPIs. CobiT, therefore, delivers an improved framework to meet management's need for control and measurability of IT by providing management tools to assess and measure the organization's IT environment against the 34 IT processes CobiT identifies. CobiT's Management Guidelines address the following types of management concerns:

- performance management – What are the indicators of good performance?
- IT Control profiling – What are the critical success factors for control?
- awareness – What are the risks of not achieving our objectives?

- benchmarking – How do we measure and compare?

In answering the above requirements of determining and monitoring the appropriate IT security and control, MMs, KPIs and CSFs are used. CobiT uses the Balance Scorecard to assist in focusing on performance management. Using the Balance Scorecard approach helps in defining KPIs to identify and measure outcomes of processes and KPIs to assess how well processes are performing by measuring the enablers of the process. IT has become the major enabler of business, therefore, the relationship between business goals with their measures and IT with its goals and measures is important. This relationship is illustrated in Figure 7.

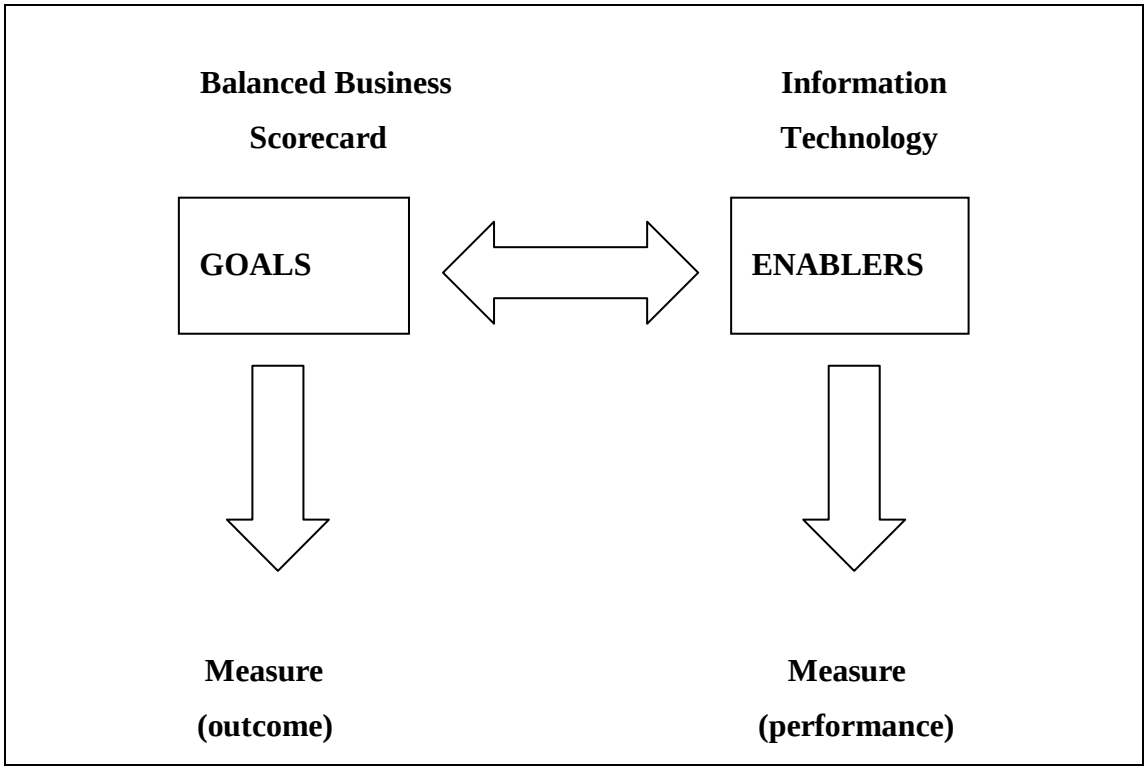

Figure 7 : Relationship between Business Goals and Information Technology

The measures will assist management in monitoring their IT organization by answering the following questions (CobiT 4.0, IT Governance Institute, 2007):

1. What is the management concern? (Make sure that the organization's needs are fulfilled.)

2. Where is it measured? (On the Balance Scorecard as a Key Goal Indicator, representing an outcome of the business process.)

3. What is the IT concern? (These are the CSFs for the organization.)

4. Where is that measured? (On the Balance Scorecard as a KGIs representing the outcome for IT.)

5. What else needs to be measured? (Whether the outcome is positively influenced by a number of CSFs that need to be measured against KPIs of how well IT is doing.)

4.7.1 Maturity Model (MM)

According to CobiT 4.0, the approach to MMs for control over IT processes consists of developing a scoring method for an organization in order it to be to be able to grade itself from non-existent to optimised (from 0 to 5) for each of the 34 IT processes. The method used for scoring on the MM was discussed in section 4.2.

By using the MM management can map from where the organization is today to where the organization should be in the future. Organizations need to achieve a competitive level of IT security and control today and this can be done by benchmarking and measuring progress against the organization's objectives or goals. MMs are action-orientated guidelines for management and if used correctly can maintain control over the organization's information and related processes and technology.

According to CobiT 4.0, IT Governance Institute, 2007 MMs:

- refer to business requirements and the enabling aspects at the different maturity levels;
- are a scale that lends itself to pragmatic comparison;
- are a scale where the difference can be made measurable in an easy manner;
- are recognisable as a "profile" of the enterprise relative to IT governance, security and control;
- help setting "As-Is" and "To-Be" positions relative to IT governance, security and control maturity;
- lend themselves to do gap analysis to determine what needs to be done to achieve a chosen level;
- avoid, where possible, discrete levels that create thresholds that are difficult to cross;
- increasingly apply CSFs;
- are not industry specific, nor always applicable the type of business defines what is appropriate.

4.7.2 Critical Success Factors (CSFs)

CSFs provides management with guidance for implementing control over IT and its processes. CSFs are the important things to do in order for the IT process to achieve its goals. Developing CSFs can be defined by examining the objectives and monitoring guidelines of the IT Governance Framework. The IT Governance Framework is the responsibility of the executives to setup.

According to CobiT 4.0, IT Governance Institute, 2007, CSFs are:

- essential enablers focused on the process or supporting environment;
- a thing or a condition that is required for optimal success or an activity recommended for optimal success;
- the most important actions to do to increase the probability of success of the process;
- either strategic, technological, organizational or procedural in nature;

- focused on obtaining, maintaining and leveraging capability and skills;
- expressed in terms of the process, not necessarily the business.

4.7.3 Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs)

KGIs are often defined as a target to achieve and are a measure of "what" has to be accomplished. KPIs are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of the enablers of that IT process. According to the Balance Scorecard principle, the relationship between KGIs and KPIs are that KGIs measure the outcome of the goals accomplished by the Balance Scorecard and the KPIs measure the performance of the enablers which make it possible for the goals to be achieved, with IT being the major enabler of the business. This is depicted in Figure 8.

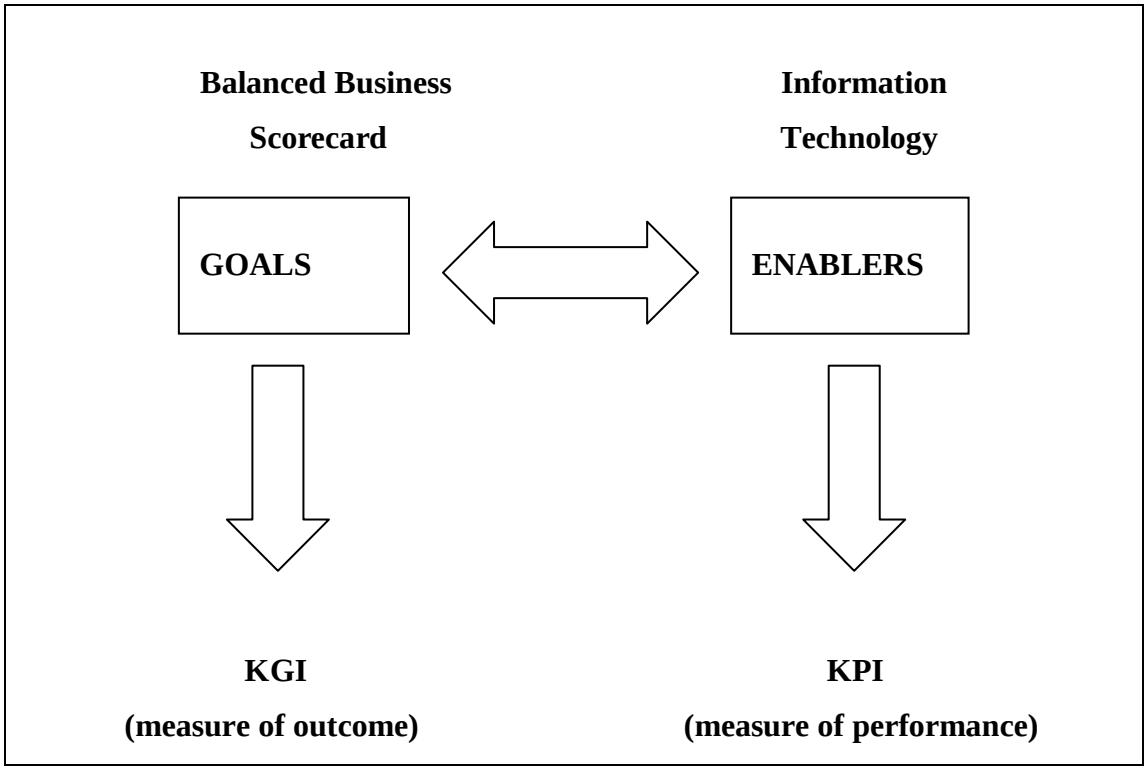

Figure 8 : Comparison of KGIs and KPIs according to Balance Scorecard principles

KPIs therefore, measure the performance of the enabler as to give an indication of how the business goals will be achieved. KGIs are business driven and usually

provide the measures needed to support the financial and customer perspective of the organization's Balance Scorecard. KPIs focus on the other two perspectives of the Balance Scorecard, internal business and innovation perspective.

According to CobiT 4.0, IT Governance Institute, 2007, KGIs are:

- a representation of the process goal, i.e., a measure of "what" or a target to achieve;
- immediate indicators of the successful completion of the process or indirect indicators of the value the process delivered to the business;
- possible description of a measure of the impact of not reaching the process goal;
- focused on the customer and financial perspectives of the Balanced Scorecard;
- IT orientated but business driven;
- expressed in precise, measurable terms, wherever possible.

According to CobiT 4.0, IT Governance Institute, 2007, KPIs are:

- a measure of how well the process is performing;
- predictions of the probability of success or failure in the future;
- are process orientated but IT driven;
- focus on the process and learning perspectives of the Balanced Scorecard;
- are expressed in precisely measurable terms;
- will help in improving the IT process when measures are acted upon.

4.8 CobiT's Audit Guidelines

CobiT's Audit Guidelines outline activities to be performed on each of the 34 high-level control objectives. The control objectives are supported by the audit guidelines which enable auditors and managers the review of specific IT processes against the audit guidelines.

CobiT's Audit Guidelines provide the auditors with assistance in preparing their audit plans for reviewing the organization's IT processes. Each of the audit guidelines consist of a statement pertaining to the following:

- a general understanding of the process;
- points to be considered in evaluating controls and assessing compliance;
- guidance on substantiating the risks associated with the specific IT process.

CobiT's Audit Guidelines use an audit framework that builds on CobiT requirements of (Audit Guidelines, IT Governance Institute, 2000).

- presentation in a level approach;
- business objective's orientation;
- process driven;
- focusing on resources that need to be managed and information criteria that are required.

Figure 9 highlights the structure for audit guidelines application according to the Auditor Guidelines, CobiT, IT Governance Institute, 2000.

Level 1 General IT Audit Approach	. CobiT Framework . Audit Process Requirements . Control Observations . Generic Audit Guidelines
Level 2 Process Audit Guidelines	. Detailed Audit Guidelines
Level 3 Audit Attention Points to Complement Detailed Control Objectives	. Local Conditions ➢ sector specific criteria ➢ industry standards ➢ platform specific elements ➢ detailed control techniques used

Figure 9 : Detailed Structure for Audit Guidelines Application (Audit Guidelines, CobiT, IT Governance Institute, 2000)

At the conclusion of the audit, the auditor should have performed sufficient tests on the processes to conclude whether a given control objective is being achieved. If this is not the case, further tests or actions need to be taken. The following are possible problems which the auditor could identify:

- no control measures are in place;
- control measures are evaluated as not being satisfactory;
- control measures have not been consistently applied .

4.9 Conclusion

According to CobiT 4.0, (IT Governance Institute, 2007) *"CSFs are the most important things you need to do based on the choices made in the MM, whilst monitoring through KPIs whether you will likely reach the goals set by the KGIs."*

CobiT's use of measuring methods can ensure that risk management and business goals of the organization are met. CobiT also ensures management that the internal control system is successful. Therefore, with the use of CobiT an effective governance of an organization's Information Security Activities is guaranteed.
CobiT also makes excellent use of earlier researched measurement methods such as; the Balance Scorecard, KGIs, KPIs, the MM and Internal Audit Program to mitigate an organization's IT risks to an acceptable level.

In this current age of increasing electronic business technology dependence, organizations need to be able to demonstrate and attain increasing levels of security and control. Every organization needs to understand their own performance and must be able to measure their progress. Benchmarking and measuring progress against the organization's strategy is one way of achieving a competitive level of IT security and control.

CobiT 4.0 provides the management tools the organization needs and ensures that IT is aligned with the business strategy. The management tools provided being CSFs, MMs, KPIs, KGIs and the internal audit.

Chapter 5

Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC).

5.1 Introduction

Section 404 of the Sarbanes-Oxley Act of 2002 requires management to annually assess and report on the effectiveness of the organization's internal control system.

Most organizations today are confronted with many different business risks, internally and externally. Having an internal control process in place can limit these risks. Today most organizations should have an internal control process in place to mitigate IT risks to an acceptable and adequate level.

M.W Stevens states in the NFRF, COSO Enterprise Risk Management, 2004, that internal control is a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievements of objectives in the following areas:

- effectiveness and efficiency of operations;
- reliability of financial reporting;
- compliance with applicable laws and regulations.

As discussed in Chapter 3, COSO's framework states that internal control is a process which is established by an organization's directors and management. The Oxford English Dictionary defines a process as *a continuous and regular action or succession of actions, taking place or carried out in a definite manner and leading to the accomplishment of some result, a continuous operation or series of operations.*
ISO9001: 2000, clause 3.4.1, defines a process as *"a set of interrelated or interacting activities that transform inputs into outputs".*

For an organization to achieve its objectives, internal controls need to be in place. If an organization does not have objectives, internal control will not be needed. It is

important that management can determine by measurement whether the Internal Control System is achieving the objectives. The internal control procedure may be well designed and implemented but over time it may lose its effectiveness. Therefore, periodic measurement of an organization's Internal Control System is necessary. An organization cannot manage its IT risk exposure unless it measures and monitors its progress, only then can it improve upon it.

When an organization uses a process approach it is noticeable that the quality of one process affects the quality of the next. The most important point of the process approach is that output from one process usually becomes the input to the next process, thereby affecting the next process. If the concept of a process approach is applied appropriately it can lead to adding value within an organization.

5.2 Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC)

As discussed in Chapter 3, CobiT is in accordance with IT Governance and addresses 318 detailed control objectives over the 34 IT processes in its framework (IT Governance Institute. CobiT Third Edition).

CobiT is an authoritive, up-to-date, international set of generally accepted IT control objectives and control practices for daily use by business and IT managers. CobiT is structured and organised to provide a powerful control model as well as having the following scope, It:

- focuses on information having integrity, being secure and available;
- is management orientated;
- supports corporate and IT governance;
- serves as a criteria for evaluation;
- is process-oriented;
- is controls-based;
- is measurement driven.

The CobiT management guidelines provide the vital link between IT control and IT governance. The management guidelines include the use of the following measuring tools, Maturity Models (MMs), Critical Success Factors (CSFs), Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs).

Measuring, monitoring and evaluating internal control involves the following: (Internal Control, Comptroller's Handbook, January 2001):

- identifying the internal control objectives relevant to the organization;
- reviewing pertinent policies, procedures and documentation;
- discussing controls with relevant personnel;
- observing the control environment;
- sharing findings, concerns and recommendations with the board and senior management;
- determining that the organization has taken timely corrective action on noted deficiencies, specific weaknesses and made recommendations, which should be fully documented, on how to correct them.

As noted in Chapter 2, the COSO Framework for Internal Control states, that internal control is a process and consists of five interrelated components or standards: control environment, risk assessment, control activities, information and communication and monitoring. When measuring and monitoring the Internal Control System, a methodology is necessary.

In developing a methodology for measuring and monitoring IT risk's internal control, a process approach will be adopted as each process of the methodology affects the next process.

As discussed in Chapter 2 and 3, the risk-management process comprises of four primary phases: assessing risk, conducting decision support, implementing controls and measuring program effectiveness. This process provides a path for organising limited resources to manage risk across the organization. The outcome of the process is a cost-effective control environment that drives and measures risk to an acceptable

level. Once the risk-management process has identified and prioritized risks to the organization, it must begin the process of identifying appropriate risk mitigation strategies. These strategies also need to be monitored and measured to ensure that identified risks have been addressed appropriately.

The main aim of the internal control process is to identify risks to the achievement of the organization's objectives and to do what is necessary to manage these risks. The board and senior management are responsible for identifying the risks to their operations and they are also responsible for designing, implementing and monitoring the internal control activities which should address the risks highlighted in the organization's risk-analysis process.

According to the IT Governance Institute, effective IT governance helps ensure that IT supports business goals, optimizes business investments in IT and appropriately manages IT-related risk and opportunities. CobiT is a comprehensive set of resources that assists organizations to adapt to IT governance.

The following proposed methodology for measuring and monitoring IT Risk's Internal Control (MMMITIC) is based on CobiT's control framework. And in using CobiT's framework IT governance can be assured.

The proposed MMMITIC consists of five processes:

1. Identify business process goals and objectives using the Balance Scorecard as a tool.

2. Measure the status of the organization's internal control system by using the Maturity Model.

3. Understand the goals and objectives using the Critical Success Factors identified on the Maturity Model.

4. Identity Key Performance Indicators, the measure necessary in achieving the objectives and goals.

5. Measure the outcome of the Key Performance Indicators against the Key Goal Indicators.

The five processes are depicted in Figure 10.

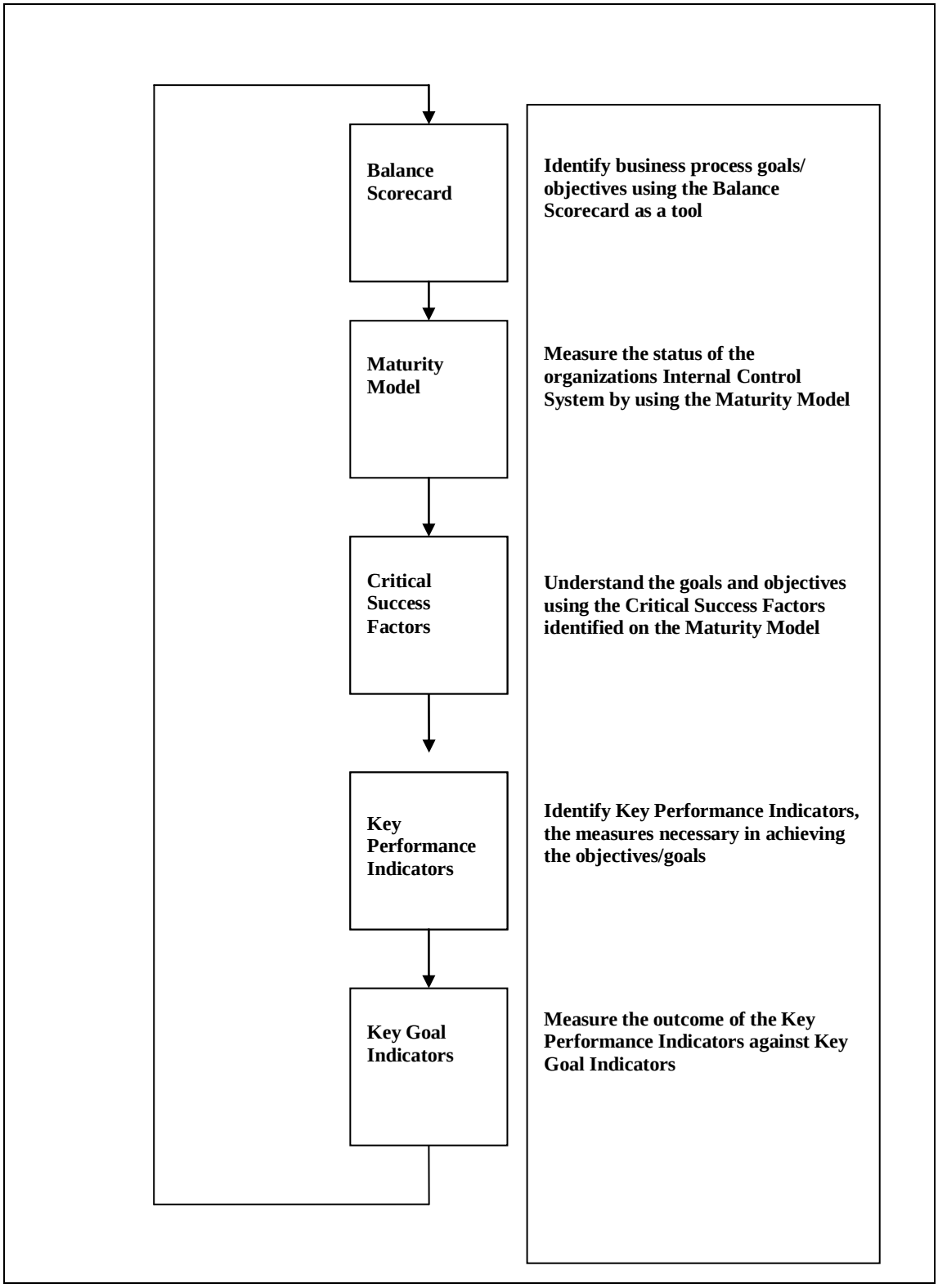

Figure 10 : Methodology for Measuring and Monitoring IT Risk's Internal Control (MMMITIC)

5.2.1 Identity business goals and objectives using the Balance Scorecard

If performance measurement is to have any real meaningful impact, a more balanced set of objectives, goals and measures are required. It is important that management can determine by measurement whether the Internal Control System is achieving the goals and objectives of the organization's business processes. The measurement tool, the Balance Scorecard enables management to do this.

Using the Balance Scorecard as a measurement tool provides feedback on the business processes and supplies KPIs to management. The Balance Scorecard is a measurement tool which provides clarity of an organization's vision and strategy. The Balance Scorecard allows the organization to be viewed from four perspectives learning and growth, internal process, customer and financial perspectives. For each of the four perspectives, objectives and goals are established. When using the Balance Scorecard as a measuring tool, the organization's business goals and objectives are achievable. It assists the manager to better monitor the organizations performance while controlling and managing risks. Use of the Balance Scorecard also identifies the information required to measure the performance of achieving the goals and objectives of the organization's business processes.

The output of the Balance Scorecard will give a comprehensive set of Information Security requirements as it links the measures (KPIs) to the business objectives and goals.

5.2.2 Measure the status of the organization's internal control system by using the Maturity Model (MM)

The MM can be used to measure the organization's internal control system in relation to IT Governance and control. The MM identifies what needs to be done to achieve a chosen level and can be measurable in an easy manner.

The MM can assist management in determining the stages and expectation levels of internal control and compare them against industry norms. It also allows management

to measure progress against the organization's objectives and goals identified in the Balance Scorecard.

The MM is a tool which accesses the overall IT control environment and appraises the organization's maturity level. When using the MM as a measurement tool, management will get a thorough understanding of the organization's processes and establish priorities for improvements. This should place management in a position of knowing whether or not they need to improve their performance.

The MM will therefore, set targets for where the organization needs to be in relation to IT governance, security and control. The targets, which are set by the MM are the CSFs. If the CSFs can be achieved the organization should meet a competitive level of IT security and control (IT Governance Forum, Information System Control, Paris, 2001).

5.2.3 Understand the goals and objectives using Critical Success Factors (CSFs)

CSFs are the most important factors that contribute to the IT process achieving its goals and objectives and ensure a successful competitive level of IT security and control. These are areas of activity that should receive constant and careful attention from management. Performance in each area should be continually measured. CSFs can be short, medium or long-term factors that an organization must focus on in order to meet the objectives and goals. CSFs are set against each objective and goal identified in the Balance Scorecard and CSFs can be weighted according to priority.

Using CSFs forces an organization to analyse its strengths, weaknesses, opportunities and threats. CSFs ensure, a thorough understanding of the organization's goals and objectives and identifies the actions necessary to support each of them.

5.2.4 Identify Key Performance Indicators (KPI's) of IT processes to measure whether the IT control process is meeting the objectives

The Balance Scorecard has identified the objectives and goals and using the CSFs has ensured a thorough understanding of these objectives and goals. It is now necessary to identify the measures necessary to meet each of the objectives and goals.

The KPIs are a tool that can be used to measure the effectiveness of the organization's controls. The objectives and goals identified in the Balance Scorecard need measures of how the organization is going to meet them; these measures are the KPIs. Using the KPIs as tool of measurement will predict the probability of success or failure. KPIs focus on the process and learning factors of the Balanced Scorecard and should assist in improving the IT process.

5.2.5 Measure the outcome against the Key Goal Indicators (KGI's)

When using the Balanced Scorecard approach the goal is measured (KGIs) as well as the drivers/enablers (KPIs) that make it possible to achieve the goal. The KGIs focus more on customer and financial aspects of the Balanced Scorecard.

Therefore, KGIs measure the outcome of what is needed to achieve the objectives. Targets are set against each objective which needs to be achieved and the KPIs are the enablers to achieve the KGIs. The Balance Scorecard links the measures (KPIs) to the business objectives. Therefore, the KPIs are the action that needs to take place to achieve the organization's target level of performance.

5.3 Conclusion

The board of directors and senior management have the responsibility of exercising IT governance within their organizations. If implemented correctly IT governance should provide the following:

- strategic direction for the organization;

- ensuring that the business objectives are achieved;
- ascertaining that risks are managed appropriately;
- verifying that the organization's resources are used responsibly.

Organizations require a structured approach to manage and control IT, including having a clear understanding of the business objectives, having appropriate frameworks of control, employing the fundamentals of IT governance and building mechanisms which provide adequate assurance that IT governance objectives are addressed.

CobiT provides a framework for IT governance as it helps build the gaps between business risks, control needs and technical issues. It also provides good practices across a domain and process framework and presents activities in a manageable and logical structure. CobiT starts from the business requirements, incorporates major international standards and has become the *de facto* standard for overall control of IT.

Effective internal control is the foundation of safe and sound business. Effective internal control reduces the possibility of errors and irregularities and assists in their timely detection when they do occur. The board of directors and senior management cannot delegate their responsibilities for establishing, maintaining and generating an effective system of internal control. The board should ensure that senior management regularly verifies the integrity of the organization's internal control. Internal control also needs to be consistently applied and thoroughly understood by the organization's staff if the board and senior management policies are to be effectively implemented (Assessing Risk, Security Risk Management Guide, Microsoft TechNet).

Bibliography

1. Assessing Risk. Security Risk Management Guide, Microsoft TechNet. Accessed June 2007. http://www.microsoft.com

2. Axelrod, C.W. (2007). Achieving Privacy Through Security Measures. Information Systems Control Journal, Information Security, 2, pp. 56-60

3. Axelrod, C.W. (2007). The Dynamics of Privacy Risk. Information Systems Control Journal, Information Security, 1, pp. 51-55

4. Central Washington University – Internal Auditor's Office: Internal Controls (2005). Accessed May 2007.http://www.cwe.edu/~auditor/accounting.html

5. Cerrullo, V.C. (2005). How the new standards and regulations affect an auditors assessment of compliance with Internal Controls. Accessed June 2007. http://www.isaca.org

6. CobiT 4.1 Information Technology Control Objectives & Control Practices.

7. CobiT source for best practices, Network Magazine, May 2004, pp 5-6. Accessed July 2007. http://www.networkmagazineindia.com/

8. Accessed July 2007.http://www.isaca.org

9. Combs, M.R. (1995). Information Systems for Business Management.

10. Comptroller of the Currency Administrator of National Banks, Internal Control: Comptroller's Handbook, January 2001. Accessed January 2007. http://www.treas.gov/handbook/

11. COSO, Internal Control-Integrated Framework. Accessed September 2006. http://www.coso.org

12. Dhillon, G. (1997). Managing Information System Security.

13. Effy, O. (2002). Management Information Systems. (Third Edition).

14. Enterprise Risk Management. (2005). Accessed January 2007. http://www.coso.org/publications.htm

15. Fabian, R. (2007). Interdependence of CobiT and ITIL. Information Systems Control Journal, Information Security, 1, pp. 32

16. Fox, C. & Zonneveld, P. IT Control Objectives for Sarbanes-Oxley.

17. Handscombe, K. (2007). Continuous Auditing from a Practical Perspective. Information Systems Control Journal, Information Security, 2, pp. 51-55

18. IT Control Objectives for Sarbanes-Oxley.(2005). Accessed June 2007. http://www.isaca.org

19. IT Governance Institute. Cobit Third Edition – 6 Volume Set.

20. ITIL Service Level Management. (2005). Accessed February 2007. http://www.itil-itsm-world.com/

21. ISO/IEC 17799:205, South African National Standards

22. Jenster,P. & Hussey, D. (2001). Company Analysis. Determining Strategic Capability.

23. King Report on Corporate Governance, 2002. Accessed April 2006. http://www.corporatecompliance.org/

24. Lainhart, J.W. (2001). CobiT Management Guidelines. IT Governance Forum. Accessed June 2007. http://www.isaca.org

25. Lambeth, J.L. (2007). Using CobiT as a tool to lead Enterprise IT organizations. Information Systems Control Journal, Information Security, 1, pp. 28-29

26. Olivier, M.S. (1999). Information Technology Research: *A practical Guide*. Johannesburg, South Africa.

27. Operational Risk and Information security need to Co-exist for effective Risk Management. (2005). Accessed March 2007. http://www.continuitycentral.com/feature0189.htm

28. Pfleeger, C.P.(1996). Security in Computing. (Second Edition).

29. Pironti, J.P. (2007). Developing Metrics for effective Information Security Governance. Information Systems Control Journal, Information Security, 2, pp. 33-37

30. Processor Editorial Article. (2005). Accessed June 2007. http://www.processor.com

31. Sarbanes Oxley Tutorial – SOX Compliance Information(2005). Accessed October 2006. http://www.sixsigmatutorial.com/SOX/sarbanes-oxley.aspx

32. Sayana, S.A. (2002). The IS Audit Process. Accessed July 2007. http://www.isaca.org

33. Singleton, T.W. (2007). What every IT Auditor should know about Auditing Information Security. Information Systems Control Journal, Information Security, 2, pp. 20-21

34. Smith, H.S. & Fingar, P. (2002). Business Process Management. *The third wave. The Breakthrough that redefines competitive advantage for the next fifty years.*

35. Standards for Internal Control in the Federal Government, (1999)). Internal Control. Accessed June 2007. http://www.isaca.org

36. Stevens, M.W. (2004). COSO, Enterprise Risk Management. Accessed September 2006. http://www.erm.coso.org/

37. Von Solms, R. & Flowerday, S. (2005). Continuous Auditing: Verifying information integrity and providing assurances for financial reports.

38. Von Solms, R. & Flowerday, S. (2005). Real-Time Information Integrity: System integrity, Data Integrity and Continuous Assurances.

39. Ward, J. & Peppard, J. (2002). Strategic Planning for Information Systems. (Third Edition)

40. Whiteman, M.E. & Mattord, H. (2003). Principles of Information Security.