A MODEL FOR INFORMATION SECURITY CONTROL AUDIT FOR SMALL TO MEDIUM-SIZED ORGANISATIONS

NATASHA DEYSEL

2009

A MODEL FOR INFORMATION SECURITY CONTROL AUDIT FOR SMALL TO MID-SIZED ORGANISATIONS

By

Natasha Deysel

Submitted in partial fulfilment of the requirements for the degree of Masters in Business Information Systems in the Faculty of Engineering, the Built Environment and Information Technology at the Nelson Mandela Metropolitan University

January 2009

Promoter: M Gerber

Table of Contents

ABSTRACT

Organisations are increasingly dependent on their information. Compromise to this information in terms of loss, inaccuracy or competitors gaining unauthorised access could have devastating consequences for the organisation. Therefore, information security governance has become a major concern for all organisations, large and small. Information security governance is based on a set of policies and internal controls by which organisations direct and manage their information security. An effective information security governance programme should be based on a recognised framework, such as the Control Objectives for Information and related Technology (COBIT). COBIT focuses on what control objectives must be achieved in order to effectively manage the information technology environment. It has become very clear that if a company is serious about information security governance, it needs to apply the COBIT framework that deals with information security. The problem in some medium-sized organisations is that they do not realise the importance of information security governance and are either unaware of the risks or choose to ignore these risks as they do not have the expertise or resources available to provide them with assurance that they have the right information security controls in place to protect their organisation against threats.

Keywords

Information Security, Information Security Governance, ISO/IEC 27002, COBIT, COBIT Framework, Information Security Auditing

Chapter 1: INTRODUCTION

Information and the systems that handle it are critical in the operation of virtually all organisations. Access to reliable information has become an indispensable component of conducting business. In a growing number of organisations, information **is** the business (IT Governance Institute, 2006).

As organisations strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, often requiring the deployment of more information systems, which results in more information being stored. Whilst managers become ever more dependent on these systems, the information becomes ever more vulnerable to a widening array of risks that could threaten the very existence of their enterprises. This is forcing managements to face difficult decisions about how to address information security effectively (IT Governance Institute, 2006).

1.1. Background

The objective of information security is to protect sensitive and valuable information from potential loss, inaccessibility, alteration or wrongful disclosure. The security objective is usually considered met when:

- Information systems are available and usable when required (*availability*);
- Data and information are disclosed only to those who have a right to know them (*confidentiality*);
- Data and information are protected against unauthorized modification (*integrity*) (IT Governance Institute, 2001).

Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability (IT Governance Institute, 2006).

Corporate governance can be described as a set of policies and internal controls by which organisations, irrespective of size or form, are directed and managed. Information Technology (IT) governance is a subset of an organisation's overall (corporate) governance programme (Corporate Governance Task Force, 2004).

IT governance is a structure of relationships and processes that direct and control an enterprise in order for it to achieve its goals by adding value while balancing risk versus return over IT and its processes. Many companies worldwide are establishing environments for IT governance (von Solms, 2005).

1.2. Description of Focus Area

Companies are realising that it is preferable to follow some type of internationally recognised reference framework rather than doing it *ad hoc* (von Solms, 2005). One of the most commonly used frameworks is the Control Objectives for Information and related Technology (COBIT).

COBIT focuses on what is required to achieve adequate management and control of IT, and is positioned at a high level. It is aligned and harmonised with other, more detailed, IT standards and best practices and acts as an integrator of these different guidance materials, summarising key objects under one umbrella framework that also links to governance and business requirements (IT Governance Institute, 2005). COBIT supports IT governance by providing a framework to ensure that (IT Governance Institute, 2005):

- IT is aligned with the business;

- IT enables the business and maximises benefits;
- IT resources are used responsibly;
- IT risks are managed appropriately;
- IT objectives are monitored against performance measurements.

COBIT provides a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: plan and organise, acquire and implement, deliver and support, and monitor and evaluate. This structure covers all aspects of information and the technology that supports it. Although COBIT is an internationally accepted reference framework and has proven to be an adequate IT management tool for many organisations, there are, however, some indirect problem areas.

1.3. Description of Problem Area

COBIT focuses on what is required to achieve adequate management and control of IT. Information security governance forms part of COBIT. Therefore, this research treatise will only focus on all of COBIT's information security-related control objectives.

The advantage of using COBIT is that it can be used by any company, large, medium or small, regardless of the industry the company is in. It is most likely that small to medium-sized organisations will require IT professionals to guide them through the implementation process of COBIT. It is also very likely that most small to medium-sized organisations are not informed of the benefits of using COBIT. They do not realise the disastrous consequence of not having any or limited preventative measures or recovery procedures in place should a disaster occur, which might compromise a company's most valuable asset, its information. Therefore, information security governance is critical to every company, large or small.

It has become very clear that if a company is serious about information security governance, it needs to apply the COBIT framework that deals with information security. The framework instils confidence in the company that it is using best practices that have been adopted by many companies around the world and that their value has been proven.

The problem area is very evident in small to medium-sized organisations. Often, organisations do not realise the importance of information security governance and are either unaware of the risks that could ruin a company, or they choose to ignore these risks as they do not have the expertise or resources available to help mitigate them.

1.4. Problem Statement

Small to medium-sized organisations do not realise the importance of information security governance, which includes the implementation of information security control objectives and audit guidelines, which will provide them with assurance that the desired IT goals and objectives are being met and key controls are being addressed.

1.5. Research Objectives

PRIMARY OBJECTIVE

The primary objective is to provide small to medium-sized organisations with an Information Security Control Audit Model (ISCAM), based on the COBIT framework. The model will be supported by a self-help Information Security Control Audit Tool (ISCAT) to assist these companies in ensuring that the most effective information security controls are implemented and that audit guidelines are consistently applied.

This tool needs to be in a language that can be understood by people who do not have an IT background; therefore, enabling a small to medium-sized

organisation to implement an information security governance programme itself.

SECONDARY OBJECTIVE

The secondary objective is to test the effectiveness of the tool in order to demonstrate its benefits, which are summarised as follows:

- It is a comprehensive tool, based on COBIT, an internationally recognised IT management framework;
- It provides regular assurance that business assets, particularly information, are properly protected from internal and external threats;
- It is a self-help tool, which is easy to use and can be implemented by personnel with limited IT background;
- It is specific to small to medium-sized organisations, and therefore, more focussed.

1.6. Research Methodology

The treatise commenced with a literature survey. Literature regarding information security, IT governance, the *Control Objectives for Information and related Technology* (COBIT) framework, which includes the control objectives in relation to the processes in IT, the control practices and audit and management guidelines, were gathered. A detailed literature study will be performed on these topics.

The use of reasoning techniques will be used to extract the information on security-related control objectives from the COBIT framework and will specifically focus on the audit guidelines of these control objectives to develop the ISCAM for small to medium-sized organisations, as they have

been identified as requiring a simplified, self-help guide to implementing and monitoring information security controls.

Therefore, an easy-to-use, self-help tool will be presented in the form of a prototype that will be developed to support the ISCAM. Finally, the effectiveness of this tool will be evaluated by conducting a case study.

1.7. Project Plan

Figure 1.1 details the timeline for this project.

				'08												'09
	Task	Start Date	End Date	J	F	M	A	M	J	J	A	S	O	N	D	J
1	Literature study	25/01	08/03	-	-	-										
2	Finalizing research problem	08/03	25/03			-										
3	Plan research design	26/03	08/04			-	-									
4	Project proposal	09/04	31/05				-									
5	Chapter 1	01/06	09/06						-							
6	Further literature studies	10/06	16/06						-							
7	Chapter 2 & 3	17/06	23/06						-							
8	Analyse literature work	24/06	07/07						-	-						
9	Design solution	08/07	21/07							-						
10	Chapter 4	22/07	18/08							-	-					
11	Chapter 5	19/08	15/09								-	-				
12	Chapter 6	16/09	20/10									-	-			
13	Complete references, etc.	21/10	03/11										-	-		
14	Write academic paper	04/11	24/11											-		
15	Review chapters	25/11	15/12											-		
16	Finalize treatise	16/12	22/12											-		
17	Proof reading	23/12	30/12											-	-	
18	Corrections	31/12	08/01												-	-
19	Bind	09/01	18/01													-
20	Handing in	19/01	19/01													-

Figure 1.1: Project Timeline

1.8. Preliminary List of Chapters

The preliminary list of chapters is as follows:

Chapter 1 provides a brief introduction to the project, stating the problem and the framework in which the project will be conducted.

Chapter 2 describes information security governance.

Chapter 3 describes the COBIT framework, specifically highlighting the information security control objectives within it.

Chapter 4 describes the development of the ISCAM, which will be based on the audit guidelines of the information security control objectives extracted from the COBIT framework. This model will be designed specifically for small to medium-sized organisations. This chapter will also involve the development of a tool, in the form of a prototype, based on the ISCAM. The objective of this tool will be to simplify the information security control audit process for small to medium-sized organisations.

Chapter 5 includes the findings of a case study which will be performed to demonstrate the effectiveness of the ISCAM tool.

Chapter 6 summarises the findings and identifies further research areas.

Figure 1.2 graphically illustrates the relationship between these chapters.

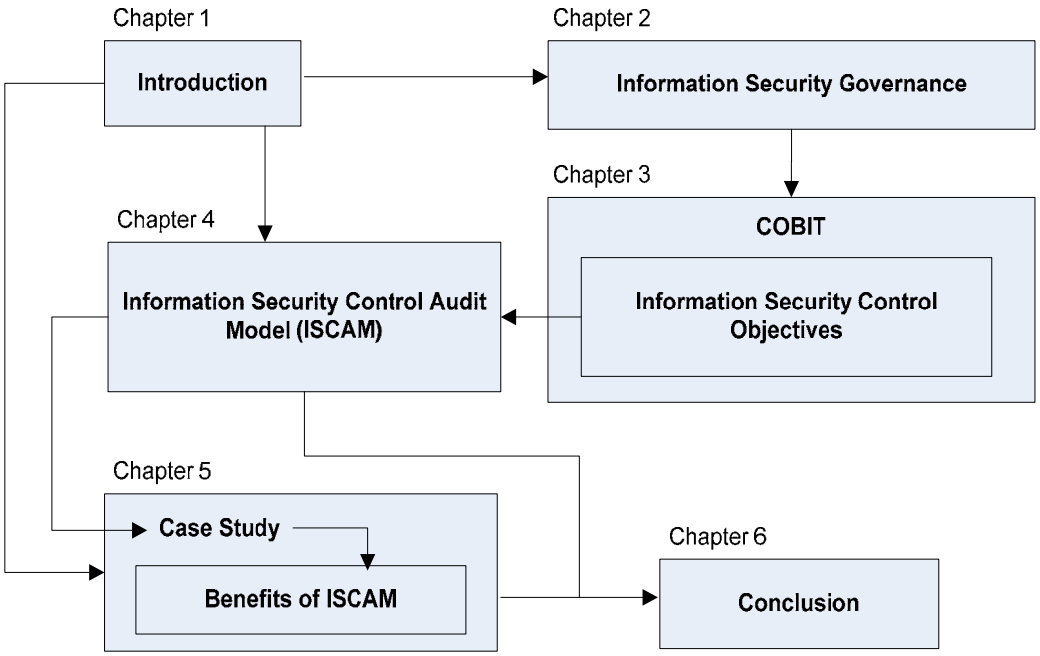


Figure 1.2: Chapter Layout

Chapter 2: INFORMATION SECURITY GOVERNANCE

2.1 Introduction

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, denial-of-services attacks and even new ways to commit organised crime. These risks, as well as the potential for careless mistakes, can all result in serious financial, reputational and other damages.

Therefore, an organisation's executive management has a responsibility to provide a secure information systems environment. Furthermore, organisations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognising the benefits that can accrue from having secure ones. Thus, as dependence on information systems increases, so too does the criticality of information security, bringing with it the need for effective information security governance (IT Governance Institute, 2001).

The objectives of this chapter are to explain what information security and information security governance are, why they are so important, what the benefits are and how to ensure that they are effective.

2.2 What is Information Security?

This section will summarise what information security is and its importance.

Information security is the protection of information and the systems and hardware that use, store and transmit that information. Information has been defined as data with meaning, relevance and purpose. Information is the basis for knowledge. Putting information together in such a way that it can be used to accomplish something useful is knowledge. Knowledge is, in turn, captured, transported and stored as organised information. Information and the knowledge based on it have increasingly become recognised as information assets, i.e., business-critical assets, without which most organisations would simply cease to function. It is a business enabler, requiring organisation to provide adequate protection for this vital resource.

Therefore, the objectives of information security are to protect the interests of those relying on information and the systems and communications that deliver it from harm resulting from failures of availability, confidentiality and integrity. Therefore, the information security objectives are usually considered met when (IT Governance Institute, 2001):

- Information systems are available and usable when required (*availability*);

- Data and information are disclosed only to those who have a right to know them (*confidentiality*);

- Data and information are protected against unauthorised modification (*integrity*).

The relative priority and significance of availability, confidentiality, integrity and trust vary according to the value and type of information and the context in which that information is used. The amount of protection required depends on how likely a security risk is to occur and how big an impact it would have if it did.

This risk management process involves the identification of vulnerabilities in an organisation’s information systems and the taking of carefully reasoned

steps to assure the confidentiality, integrity and availability of all the components in them. Once the vulnerabilities are identified and ranked, the organisation must choose a strategy to control the risk resulting from these vulnerabilities. Once a control strategy has been implemented, the effectiveness of controls should be monitored and measured.

By monitoring the effectiveness of these security controls, the organisation is always making changes to keep pace with the ever-changing technological world we live in, as state-of-the-art security measures today may be obsolete tomorrow.

Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability (IT Governance Institute, 2006).

2.3 What is Information Security Governance?

This section will explain what information security governance is and what is involved in an information security governance programme (IT Governance Institute, 2008).

Information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Whilst senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organisational resources.

To exercise effective enterprise and information security governance, boards and senior executives must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to direct the implementation of an information security programme, how

to evaluate their own status with regard to an existing security programme and how to decide the strategy and objectives of an effective security programme.

Information security governance consists of the leadership, organisational structures and processes that safeguard information. Critical to the success of these structures and processes is effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues. The five basic outcomes of information security governance should include (IT Governance Institute, 2008):

- Strategic alignment of information security with business strategy to support organisational objectives;

- Risk management, by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level;

- Resource management, by utilising information security knowledge and infrastructure efficiently and effectively;

- Performance measurement, by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved;

- Value delivery, by optimising information security investments in support of organisational objectives.

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organisation's management — including boards of directors, senior executives and all managers — does not establish and reinforce the business need for effective enterprise security, the organisation's desired state of security will not be

articulated, achieved or sustained. To achieve a sustainable capability, organisations must make enterprise security the responsibility of leaders at a governance level, not of other organisational roles that lack the authority, accountability and resources to act and enforce compliance.

Gaps in the information security governance programme are usually caused by the following:

- Lack of a comprehensive and maintainable risk and threat management process;
- New vulnerabilities resulting from the widespread use of new technologies;
- Lack of maintenance to assure all patches are promptly made;
- Increased networking and mobile working;
- Lack of security awareness;
- Insufficient discipline when applying controls;
- New and determined efforts of hackers, fraudsters, criminals and even terrorists;
- Changing legislative, legal and regulatory security requirements.

Thus, information security governance requires senior management commitment, a security-aware culture, promotion of good security practices, constant risk identification to keep pace with the ever-changing technological environment and compliance with policies. To emphasize the importance of information security governance even further, the next section will explore this topic in more detail.

2.4 Why is Information Security Governance Important?

A key goal of information security governance is to reduce adverse impacts on an organisation to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that organisations face as a result of information inaccuracy and loss, or the absence of due care in its protection.

Information security governance is important because (IT Governance Institute, 2006):

- Information security covers all information processes, be it physical or electronic, regardless of whether they involve people and technology or relationships with trading partners, customers and third parties;

- Information security addresses information protection, confidentiality, availability and integrity throughout the life cycle of the information and its uses within an organisation;

- Given the dramatic rise of information crimes, including phishing and other cyber attacks, few today would contend that improved security is not a requirement. With new worms and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues;

- Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organisations are concerned with other risks pertaining to the privacy of personal information and an organisation's need to

protect the confidentiality of information, whilst encouraging electronic business;

- The systems and processes that handle information have become pervasive throughout enterprises. Organisations may survive the loss of other assets, including facilities, equipment and people, but few can continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data. The risks, benefits and opportunities these resources present have made information security governance a critical facet of overall governance.

This section has emphasised the importance of information security governance, but besides these points, there are also a number of critical success factors an organisation must consider.

2.5 What are the Critical Success Factors for an Information Security Governance Programme?

The following factors are often critical to the successful implementation of an information security governance programme within an organisation (IT Governance Institute, 2003):

- Information security policy, objectives, and activities that reflect business objectives;

- An approach and framework to implanting, maintaining, monitoring and improving information security that is consistent with the organisation culture;

- Visible support and commitment from all levels of management;

- A good understanding of the information security requirements, risk assessment and risk management;

- Effective marketing of information security to all managers, employees and other parties to achieve awareness;

- Distribution of guidance on information security policy and standards to all managers, employees and other parties;

- Provision to fund information security management activities;

- Providing appropriate awareness, training and education;

- Establishing an effective information security incident-management process;

- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

This section has listed the critical success factors of an information security governance programme. There are also a number of benefits that can emerge from such an information security governance programme.

2.6 What are the Benefits of Information Security Governance?

Information security governance generates significant benefits, which are highlighted as follow (IT Governance Institute, 2001):

- An increase in share value for organisations that practice good governance;

- Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels;

- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care;

- The structure and framework to optimise allocation of limited security resources;

- Assurance of effective information security policy and policy compliance;

- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information;

- A level of assurance that critical decisions are not based on faulty information;

- Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery and regulatory responses.

The benefits add significant value to an organisation by:

- Improving trust in customer relationships;

- Protecting the organisation’s reputation;

- Decreasing the likelihood of violations of privacy;

- Providing greater confidence when interacting with trading partners;

- Enabling new and better ways to process electronic transactions;

- Reducing operational costs by providing predictable outcomes - mitigating risk factors that may interrupt the process.

The above-mentioned benefits emphasise the need for an effective information security governance programme. Therefore, the next section details how to ensure such a programme.

2.7 How is Effective Information Security Governance Ensured?

In the previous sections, the importance and benefits of an effective information security governance programme were discussed. The critical question is: How does one implement a successful and effective information security governance programme?

To achieve effective information security governance, management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

According to Horton, Le Grand, Murray, Ozier and Parker (2000), an information security governance framework generally consists of:

- An information security risk management methodology;

- A comprehensive security strategy explicitly linked with business and IT objectives;

- An effective security organisational structure;

- A security strategy that talks about the value of information both protected and delivered;

- Security policies that address each aspect of strategy, control and regulation;

- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy;

- Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk;

- A process to ensure continued evaluation and update of security policies, standards, procedures and risks.

This kind of framework, in turn, provides the basis for the development of a cost-effective information security programme that supports an organisation's goals and provides an acceptable level of predictability for operations by limiting the impacts of adverse events.

The overall objective of the programme is to provide assurance that information assets are protected in accordance with their value or the risk their compromise poses to an organisation. The framework generates a set of activities that supports fulfilment of this objective.

This section has described what an effective information security governance programme should consist of and that it must reference to an already developed framework to ensure that it is based on international standards.

The next section will evaluate COBIT and ISO 27002 as possible reference frameworks that can be used as a foundation to achieve the information security objectives of an organisation.

2.8 The Evaluation of COBIT and ISO 27002

This section will give a brief overview of both COBIT and ISO 27002 and describes which one was used throughout the rest of this paper (von Solms, 2005).

COBIT

COBIT (Control Objectives for Information and related Technology) positions itself as 'the tool for information technology governance'. COBIT is, therefore, not exclusive to information security – it addresses IT governance and refers, amongst many other issues, to information security.

The upside of using COBIT as an information security governance framework is that information security is 'integrated' into a larger or wider IT governance framework. Even if COBIT is used only for information security governance, it still provides the rest of the framework if the company later decides to base the rest of its IT governance also on COBIT. The then existing information security governance framework will then fit seamlessly into the wider framework defined by COBIT.

The downside of using COBIT for information security governance is that it is not always very detailed in terms of 'how' to implement the information security controls. The detailed control objectives within the COBIT framework are more directed to the 'what' must be done. Therefore COBIT is preferred by IT Auditors and IT risk mangers as the framework of choice, because it assists them to evaluate the internal controls to identify what controls are either weak or are not in place to secure the organisation's assets.

ISO 27002

ISO 27002 is exclusive to information security, and only addresses that issue.

The upside of using ISO 27002 for information security governance is that it is more detailed than COBIT, and provides much more guidance on precisely 'how' things must be done. Because of this more detailed, and perhaps more 'technical' orientation of ISO 27002, it is, in many cases, the framework of choice of IT managers and information security managers.

The downside of using ISO 27002 is that it is very much a ‘stand alone’ guidance, and is not integrated into a wider framework for IT governance.

Therefore, it seems logical that to get the benefits of both the wider reference and integrated platform provided by COBIT, and the more detailed guidelines provided by ISO 27002, there can be a great deal of benefit in using these in combination for information security governance.

This research treatise focuses more on highlighting to small to medium-sized organisations what is wrong or missing in their information security governance programme by performing an audit, and because it is more focussed on the ‘what’, the COBIT framework will be used in the rest of this research treatise.

2.9 Conclusion

This chapter has explained what information security governance involves, its importance, critical success factors and benefits. To achieve effective information security governance, management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme. COBIT and ISO 27002 were evaluated as possible reference frameworks that can be used as a foundation for an information security governance programme. COBIT was selected to be used throughout this research treatise because it focuses on ‘what’ controls must be implemented, which is the main objective of this research treatise.

Chapter 3: THE COBIT FRAMEWORK

3.1 Introduction

As discussed in the previous chapter, the Control Objectives for Information and related Technology (COBIT) are based on the analysis and harmonisation of existing IT standards and best practices and conform to generally accepted IT governance principles.

COBIT's high-level status is recognised widely because of its understanding of business requirements, covering the full range of IT activities, and its concentration on what should be achieved, rather than how to achieve effective governance, management and control. Therefore, it acts as an integrator of IT governance practices and appeals to executive, business and IT managements and governance, assurance and security professionals, as well as IT audit and control professionals (IT Governance Institute, 2005).

The objectives of this chapter are to describe COBIT, its components and the benefits of using it as an information security governance framework. The COBIT control objectives related to information security will also be highlighted, as these will assist us in the development of the solution described in chapter one.

3.2 What is COBIT?

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for IT management, created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximising the benefits

derived through the use of IT and developing appropriate IT governance and control in a company (IT Governance Institute, 2007b).

COBIT was first released in 1996. Its mission is "to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted IT control objectives for day-to-day use by business managers and auditors". Managers, auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies' assets through the development of an IT-governance model (IT Governance Institute, 2007).

COBIT 4.1 (IT Governance Institute, 2007b) is the version that is referred to throughout this document.

COBIT appeals to different users:

- Executive management - to obtain value from IT investments and balance risk and control investment in an often unpredictable IT environment;

- Business management - to obtain assurance on the management and control of IT services provided by internal or third parties;

- IT management - to provide the IT services that the business requires to support the business strategy in a controlled and managed way;

- Auditors - to substantiate their opinions and/or provide advice to management on internal controls.

COBIT has been developed and is maintained by an independent, non-profit research institute, drawing on the expertise of its affiliated associations' members, industry experts, and control and security professionals. Its content is based on ongoing research into IT good practice and is

continuously maintained, providing an objective and practical resource for all types of users.

COBIT is oriented toward the objectives and scope of IT governance, ensuring that its control framework is comprehensive, in alignment with enterprise governance principles and, therefore, acceptable to boards, executive management, auditors and regulators.

COBIT 4.1 has 34 high-level processes that cover 210 control objectives categorised into four domains (IT Governance Institute, 2007b). Each of these domains will be discussed:

DOMAIN 1: Planning and Organisation

The Planning and Organisation domain covers the use of information and technology and how best they can be used in a company to help achieve the company's goals and objectives. It also highlights the organisational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from its use.
The following lists the high-level IT processes for the Planning and Organisation domain:

- PO1: Define a Strategic IT Plan and Direction;
- PO2: Define the Information Architecture;
- PO3: Determine Technological Direction;
- PO4: Define the IT Processes, Organisation and Relationships;
- PO5: Manage the IT Investment;
- PO6: Communicate Management Aims and Direction;

- PO7: Manage IT Human Resources;
- PO8: Manage Quality;
- PO9: Assess and Manage IT Risks;
- PO10: Manage Projects.

This domain provides direction to solutions' delivery (AI) and service delivery (DS).

DOMAIN 2: Acquisition and Implementation

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components.

The following lists the high-level IT processes for the Acquisition and Implementation domain:

- AI1: Identify Automated Solutions;
- AI2: Acquire and Maintain Application Software;
- AI3: Acquire and Maintain Technology Infrastructure
- AI4: Enable Operation and Use;
- AI5: Procure IT Resources;
- AI6: Manage Changes;

- AI7: Install and Accredit Solutions and Changes.

This domain provides the solutions and passes them on to be turned into services in the next domain.

DOMAIN 3: Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of IT. It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

The following lists the high-level IT processes for the Delivery and Support domain:

- DS1: Define and Manage Service Levels;
- DS2: Manage Third-party Services;
- DS3: Manage Performance and Capacity;
- DS4: Ensure Continuous Service;
- DS5: Ensure System Security;
- DS6: Identify and Allocate Costs;
- DS7: Educate and Train Users;
- DS8: Manage Service Desk and Incidents;
- DS9: Manage the Configuration;

- DS10: Manage Problems;
- DS11: Manage Data;
- DS12: Manage the Physical Environment;
- DS13: Manage Operations.

This domain receives the solutions and makes them usable for end users.

DOMAIN 4: Monitoring and Evaluation

The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still 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 an IT system in its ability to meet business objectives and the company's control processes by internal and external auditors.

The following lists the high-level IT processes for the Monitoring domain:

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

This domain monitors all processes to ensure that the direction provided is followed.

COBIT has become the integrator for IT best practices and the umbrella framework for IT governance because it is harmonised with other standards and continuously kept up to date. The process structure of COBIT, in conjunction with its high-level, business-oriented approach, provides an end-to-end view of IT that aids organisations in getting the most value possible from their IT investments.

COBIT provides benefits to managers, IT users and auditors. Managers benefit from COBIT because it provides them with a foundation upon which IT-related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service and monitoring the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them by COBIT's defined controls, security and process governance. COBIT benefits auditors because it helps them identify IT control issues within a company’s IT infrastructure. It also helps them corroborate their audit findings.

COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business;
- IT enables the business and maximises benefits;
- IT resources are used responsibly;
- IT risks are managed appropriately.

COBIT is oriented toward the objectives and scope of IT governance, ensuring that its control framework is comprehensive, in alignment with enterprise governance principles and, therefore, acceptable to boards, executive management, auditors and regulators.

The characteristics of the COBIT framework will be analysed in more detail in the next section.

3.3 The Characteristics of the COBIT Framework

The COBIT framework was created with the following main characteristics of being (IT Governance Institute, 2007b):

- **Business-focussed**

  Business orientation is the main theme of COBIT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more importantly, to provide comprehensive guidance for management and business process owners.

  The COBIT framework is based on the principle to provide the information that the enterprise requires to achieve its objectives, the enterprise needs to invest in and to manage and control IT resources using a structured set of processes to provide the services that deliver the required enterprise information.

  Managing and controlling information are at the heart of the COBIT framework and help ensure alignment to business requirements.

- **Process-oriented**

  COBIT defines IT activities in a generic process model within four domains. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

  The domains map to IT's traditional responsibility areas of plan, build, run and monitor. The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities. Incorporating an operational model and a

common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices. A process model encourages process ownership, enabling responsibilities and accountability to be defined.

- **Controls-based**

  COBIT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

- **Measurement-driven**

  A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. To decide on the right level, management should ask itself: How far should we go and is the cost justified by the benefit? Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement.

These COBIT characteristics emphasise the basic principle of the COBIT framework which is that IT resources are managed by IT processes to achieve IT goals that respond to business requirements.

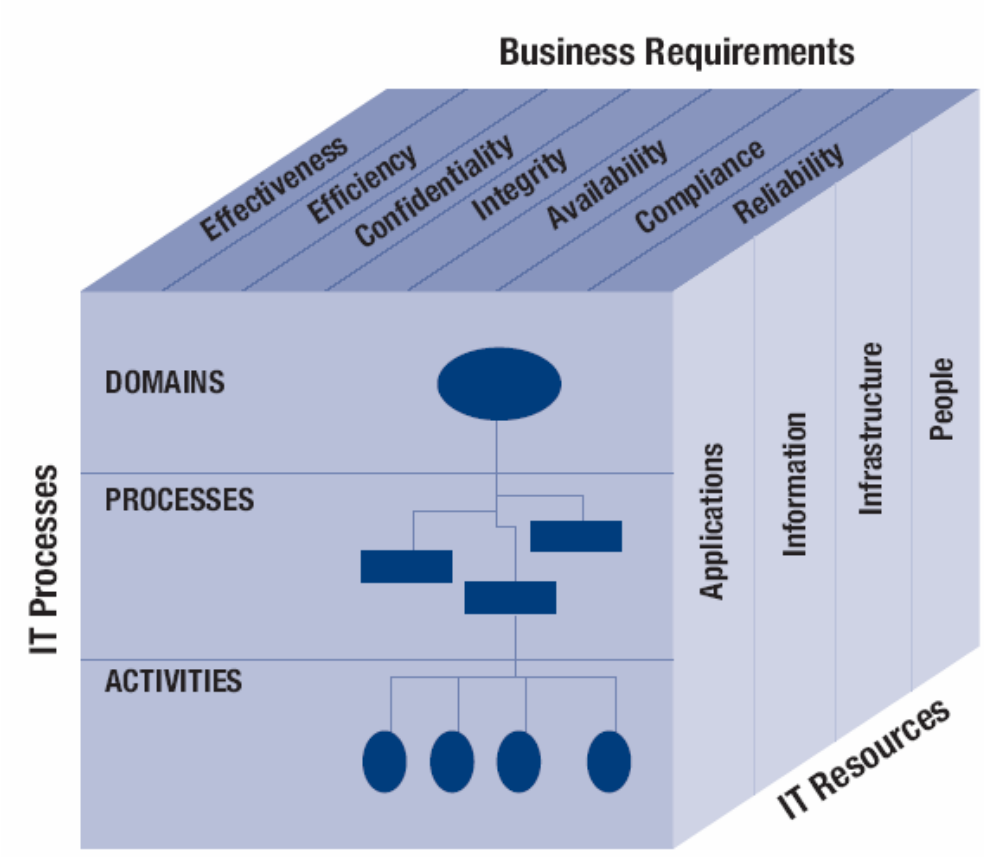


Figure 3.1: The COBIT Cube (IT Governance Institute, 2007)

A successful organisation is, therefore, built on a solid framework of data and information. The COBIT framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The framework identifies which of the seven Business Requirements (Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance and Reliability), as well as which IT resources (People, Applications, Information and Infrastructure) are important for the IT processes to fully support business. This is illustrated by the COBIT cube in Figure 3.1.

The overall COBIT framework is graphically depicted in Figure 3.2 below.

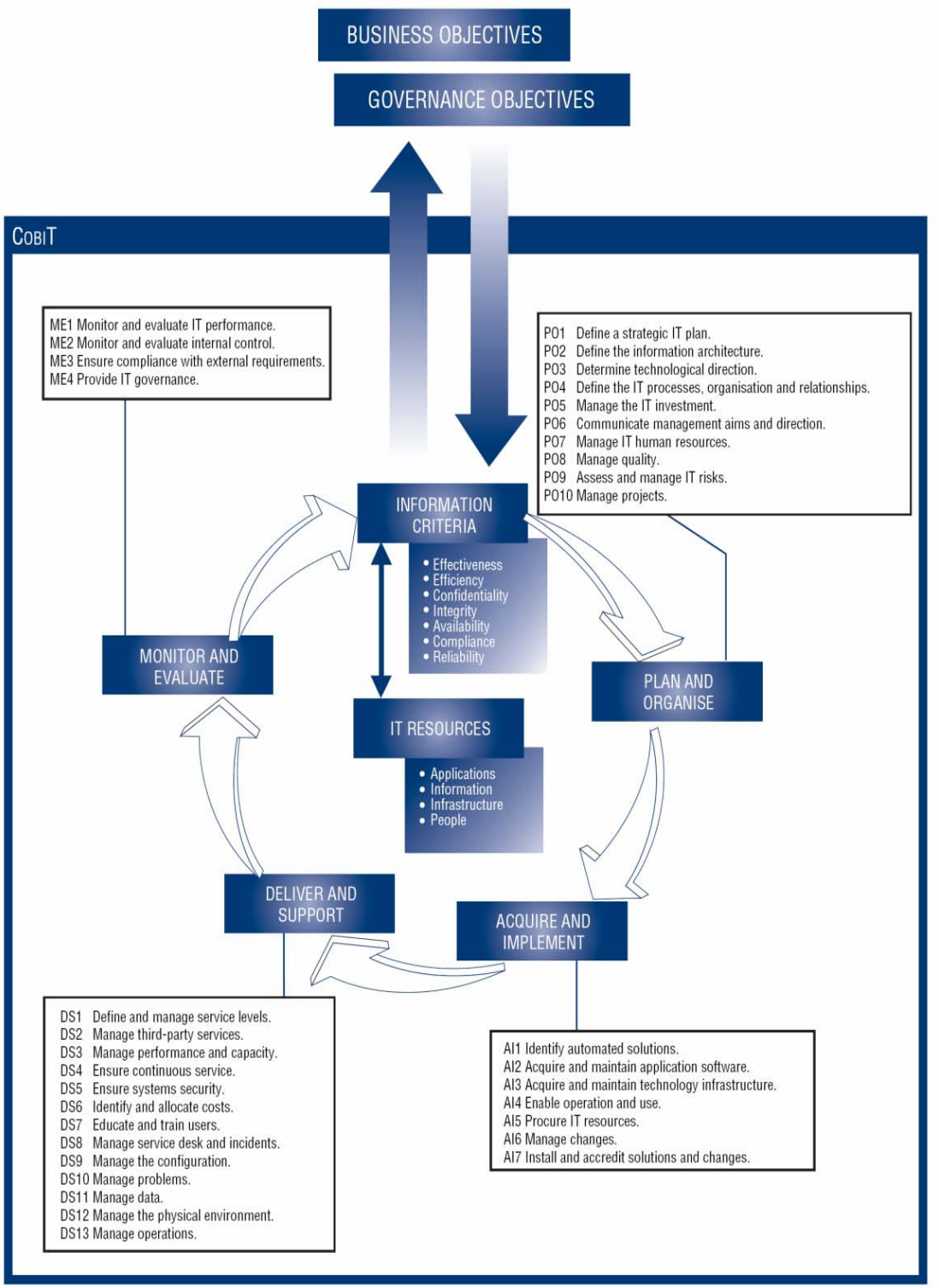


Figure 3.2: The COBIT Framework (IT Governance Institute, 2007)

The next section will highlight the benefits of using COBIT as an IT governance framework.

3.4 What are the Benefits of Using the COBIT Framework?

Having discussed the characteristics of the COBIT framework above, this section will explore the benefits of using COBIT as an IT governance framework.

The benefits of implementing COBIT include the following (Gray, 2004):

- It is an internationally recognised best practice, and by adopting a best practice, one:
    - Avoids re-inventing the wheel;
    - Reduces dependency on technology experts;
    - Increases the potential to utilise less-experienced staff, if properly trained;
    - Makes it easier to leverage external assistance;
    - Overcomes vertical silos and non-conforming behaviour;
    - Reduces risks and errors;
    - Improves quality;
    - Improves the ability to manage and monitor;
    - Increases standardisation leading to cost reduction;
    - Improves trust and confidence from management and partners;
    - Creates respect from regulators and other external reviewers;

  - Safeguards and proves value;

- COBIT enables managements to obtain value from their IT investments and assists in balancing risk and control investment in an often unpredictable IT environment;

- COBIT has a business focus, which ensures that the information security strategy of a company is aligned with the overall business strategy;

- COBIT is a comprehensive control framework and is in aligned with corporate governance principles and, therefore, acceptable to boards, executive management, auditors and regulators;

- COBIT is a framework that will guide management in deciding on the level of risk to accept, the most appropriate control practices and the path to follow when it is necessary to improve the level of control;

- COBIT is used by IT auditors and IT risk managers as a framework of choice (von Solms, 2005). Therefore, it is to any company's benefit to use the same framework that auditors use to perform company IT audits, even if IT audits are not performed by that particular company. The auditors of the company could, for some reason, at any time, insist that an IT audit be performed;

- Information security is 'integrated' into a larger or wider IT governance framework. Even if COBIT is used only for information security governance, it still provides the rest of the framework if the company later decides to base future IT governance also on COBIT. The then existing information security governance framework will fit seamlessly into the wider framework defined by COBIT (von Solms, 2005).

The above-mentioned benefits emphasise the importance of implementing COBIT as an information security governance framework, but as stated in the last benefit, only some of the control objectives of COBIT relate to information security. Therefore, in the next section, the COBIT control objectives related to information security will be extracted.

3.5 Which COBIT Control Objectives Relate to Information Security?

It has become very clear that if a company is serious about information security governance, it needs to apply the COBIT controls that deal with information security.

The COBIT Security Baseline (IT Governance Institute, 2007c) document highlights the high-level COBIT control objectives related to information security within the four domains in the COBIT framework.

The information security control objectives for the **Plan and Organise** domain are listed in Figure 3.3 below.

	Control Objective	**Control Objective Description**	**COBIT 4.1**
1	Define the security strategy and the information architecture	Identify information and services critical to the enterprise and consider their security requirements.	PO1: 1.2,1.4,1.6 PO2: 2.2, 2.3 PO3: 3.4 PO4: 4.9 DS5: 5.1, 5.2
2	Define the IT organisation and relationships	Define and communicate information security responsibilities.	PO4: 4.8,4.10,4.114.15 PO7: 7.3

3	Communicate management aims and direction	Define and communicate management aims and directions with respect to information security.	PO6: 6.2, 6.3, 6.4, 6.5 DS5: 5.2
4	Manage IT human resources	Ensure that security functions are staffed properly with people who possess the necessary skills to fulfil the role.	PO7: 7., 7.2, 7.5, 7.6, 7.7 PO4: 4.13
5	Assess and manage IT risks	Discover, prioritise, and either contain or accept relevant information security risks.	PO2: 2.3 PO9: 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 PO7: 7.4 AI1: 1.1, 1.2

Figure 3.3: The Information Security Control Objectives in the Plan and Organise Domain of the COBIT framework

The information security control objectives for the **Acquire and Implement** domain are listed in Figure 3.4 below.

	Control Objective	**Control Objective Description**	**COBIT 4.1**
1	Identify automated solutions	Consider security when identifying, automated solutions.	AI1: 1.1, 1.2, 1.3 AI2: 2.2, 2.4 AI4: 4.1, 4.4 AI5: 5.2, 5.3, 5.5, 5.5

2	Acquire and maintain application and technology infrastructure	Consider security when acquiring and maintaining the technology infrastructure.	PO8: 8.3 AI2: 2.3, 2.4, 2.5, 2.6, 2.8 AI3: 3.1, 3.2, 3.3, 3.4 AI6: 6.1 DS5: 5.9
3	Enable operation and use	Consider security when enabling operational use.	AI4: 4.1, 4.2, 4.3, 4.4, AI7: 7.1
4	Manage changes	Ensure that all changes, including patches, support enterprise objectives and are carried out in a security manner. Ensure that day-to-day business processes are not impacted.	AI6: 6.1, 6.2, 6.3, 6.4, 6.5 AI3: 3.4 AI2: 2.8 AI7: 7.2, 7.4, 7.6
5	Install and accredit solutions and changes	Ensure that all new systems and changes are accepted only after sufficient testing of security functions.	PO8: 8.3 AI3: 3.4 AI7: 7.2, 7.4, 7.6, 7.7, 7.8, 7.9

Figure 3.4: The Information Security Control Objectives in the Acquire and Implement Domain of the COBIT framework

The information security control objectives for the **Deliver and Support** domain are listed in Figure 3.5 below.

	Control Objective	**Control Objective Description**	**COBIT 4.1**
1	Define and manage service levels	Define and manage security aspects of service levels.	AI5: 5.2 DS1: 1.3, 1.5, 1.6 DS2: 2.4
2	Manage third-party services	Manage security aspects of third-party services.	AI5: 5.3 DS2: 2.3, 2.4 ME2: 2.6
3	Ensure continuous services	Ensure that the enterprise is capable of carrying on its day-to-day automated business activities with minimal interruption from a security incident.	PO2: 2.3 PO9: 9.3, 9.4 DS4: 4.1, 4.2, 4.3, 4.4, 4.5, 4.8, 4.9 DS5: 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 DS10: 10.1, 10.2, 10.3 DS11: 11.5, 11.6 DS12: 12.3, 12.5 DS13: 13.4
4	Manage the configuration	Ensure that all configuration items are appropriately secured and security risks minimised by ensuring the enterprise's awareness of its IT-related assets and licences.	DS9: 9.1, 9.2, 9.3

5	Manage data	Ensure that all data remain complete, accurate and valid during input, processing, storage and distribution.	DS5:5.11 DS4: 4.9 DS11: 11.2, 11.4, 11.6
6	Manage the physical environment	Protect all IT equipment from damage.	DS12: 12.1, 12.2, 12.3, 12.4, 12.5

Figure 3.5: The Information Security Control Objectives in the Deliver and Support Domain of the COBIT framework

The control objectives related to information security for the **Monitor and Evaluate** domain are listed in Figure 3.6 below.

	Control Objective	**Control Objective Description**	**COBIT 4.1**
1	Monitor and evaluate IT performance - assess internal control adequacy	Regularly monitor the performance of information security	ME1: 1.2, 1.4, 1.5, 1.6 ME2: 2.1, 2.4
2	Obtain independent assurance	Gain confidence and trust in security through reliable and independent sources	ME2: 2.5, ME4: 4.7
3	Ensure regulatory compliance	Ensure that information security functions comply with applicable laws, regulations and other external requirements	ME3: 3.1, 3.2, 3.3, 3.4 PO3: 3.3

Figure 3.6: The Information Security Control Objectives in the Monitor and Evaluate Domain of the COBIT framework

The rest of this research paper will focus only on these information security control objectives.

3.6 Conclusion

This chapter has described what COBIT is, its characteristics and its benefits. The final section of this chapter highlighted the COBIT control objectives related to information security, as this treatise focuses only on the information security aspects of COBIT.

In the next chapter, the assurance guidelines for these COBIT information security control objectives will be analysed to assist in the development of an Information Security Control Audit Model, which will be specifically focussed on small to medium-sized organisations.

Chapter 4: AN INFORMATION SECURITY CONTROL AUDIT MODEL (ISCAM)

4.1 Introduction

The previous chapter highlighted the control objectives from the COBIT framework which relate to information security. Organisations need to implement these controls to ensure their sensitive and valuable information is being protected from potential loss, inaccessibility, alteration or wrongful disclosure.

This chapter will examine the audit guidelines of these information security controls and how they can assist organisations to ensure these objectives are being met and that no system weaknesses exist.

The evaluation of these audit guidelines will assist in the development of the Information Security Control Audit Model (ISCAM). However, the first focus is on the reason why an audit is so important.

4.2 Purpose of an Audit

The purpose of an audit is to evaluate the performance of a control. Due to the prevalent use of information technology systems today, it is important that controls are in place. IT controls are specific IT processes designed to support a business process. IT controls can be categorised as either general controls or application controls.

General controls are those controls that are pervasive to all systems components, processes, and data for a given organisation or systems environment. They include controls over such areas as the data centre and network operations, systems software acquisition and maintenance, access security and application system acquisition, development and maintenance.

Application controls are those controls that are appropriate for individual accounting subsystems, such as payroll or accounts payable. They relate to the processing of individual applications and help ensure that transactions occurred, are authorised, and are completely and accurately recorded, processed, and reported.

This means organisations need to investigate whether or not the controls are achieving their objectives by performing an audit (IT Governance Institute, 2000).

The objectives of an audit are to:

- Provide management with reasonable assurance that control objectives are being met;
- Substantiate the risk where there are significant control weaknesses;
- Advise management on corrective actions.

The generally accepted structure of the audit process is to:

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

Audit guidelines assist an assessor to provide assurance that the process is actually under control so that the information requirements necessary to achieve business objectives will be satisfied (IT Governance Institute, 2000).

Therefore, the basis for an audit is to provide assurance. According to COBIT's IT Assurance Guide (IT Governance Institute, 2007), an organisation must constantly and consistently audit its controls to achieve the desired goals and objectives.

The assurance testing steps provide guidance at the control objective level. The steps are derived from the control practices, which, in turn, are derived from each control objective. The assurance-testing steps include the following:

- Evaluate the design of the controls;
- Confirm that controls are placed in operation;
- Assess the operational effectiveness of the control.

These assurance or audit steps and types are referred to throughout the Audit Guidelines used in this research treatise.

The Audit Guidelines outline and suggest actual activities to be performed, corresponding to each of the 34 high-level COBIT IT processes, while substantiating the risk of control objectives not being met (IT Governance Institute, 2007). This will provide information systems' managers assurance and/or advice for improvement in their IT processes and controls.

In order to provide assurance that information security controls are achieving their objectives, a consistent audit process must be followed and continuously executed. Continuous auditing will give end users of information more timely assurance that the information is correct. This is one of the focus areas of the ISCAM, which will be discussed in the next section.

4.3 The Information Security Control Audit Model

Figure 4.1 graphically illustrates the global view of the ISCAM. This section discusses its components.

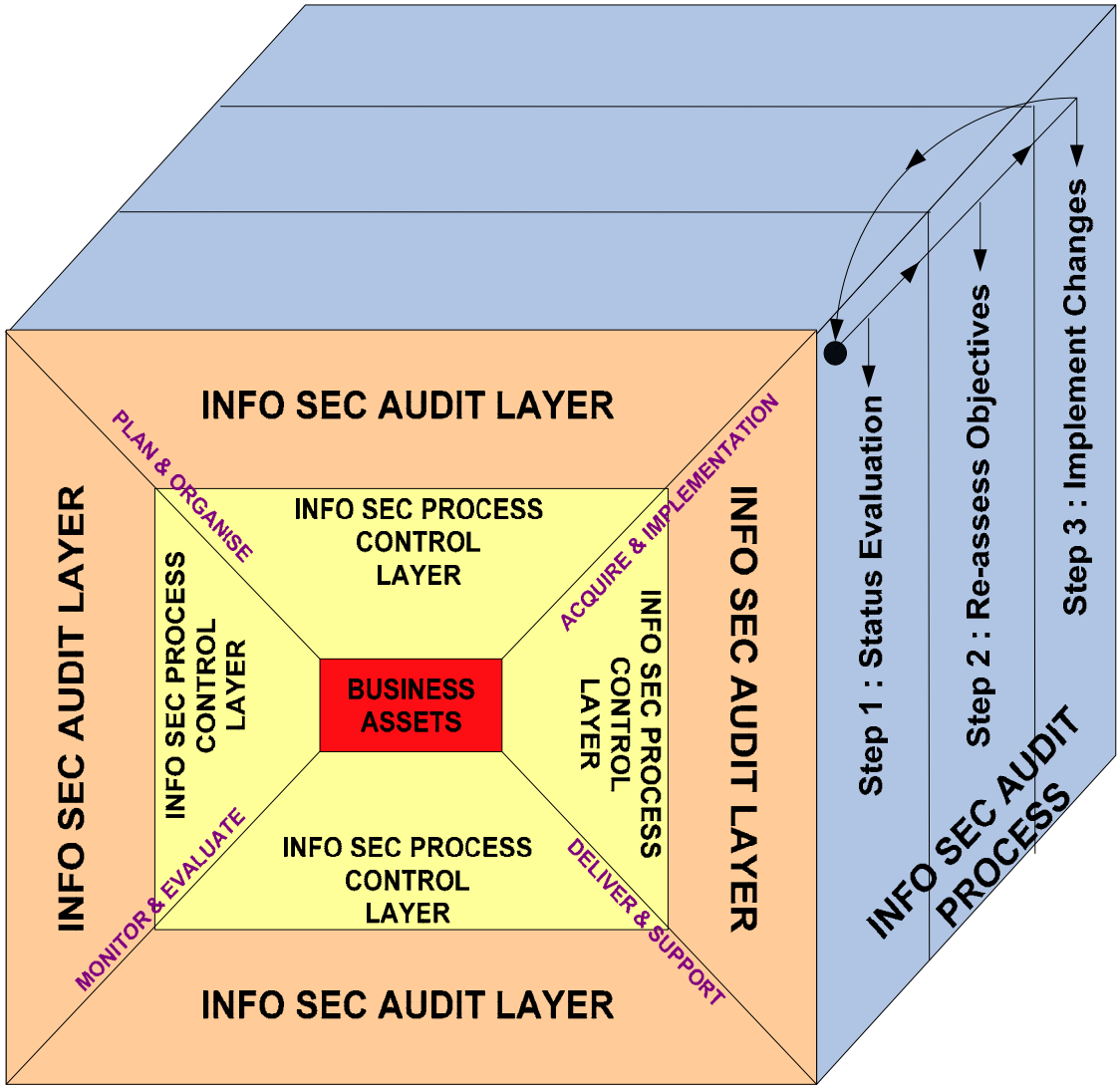


Figure 4.1: The Information Security Control Audit Model

At the core of the ISCAM are the business assets (in red) that must be protected. This research paper has highlighted that management requires assurance that its assets, which include hardware, software and information, are being protected from harmful threats, as an organisation could cease to exist if these were compromised in any possible way.

In order to protect these business assets, certain control objectives are implemented in the processes that use these assets. Therefore, the next block around the “Business Assets” one is the “Information Security Control Layer” that represents these control objectives.

In order to ensure these control objectives are actually being implemented and adhered to, an “Information Security Control Audit Layer” is formed around the “Information Security Control Layer”, which provides assurance to management that the controls are achieving their objectives. In this layer, information security control audit questions are developed related to the four domains in the COBIT framework, which is executed through the audit process.

The “Information Security Audit Process”, illustrated to the right in Figure 4.1, highlights the very important fact that this is not a once-off process, but must be applied on a continuous basis, for example, every six months. This audit process ensures that an organisation is constantly reviewing its current status to verify if there are any new weaknesses or threats that could compromise the safety of the business assets.

This process involves the following steps:

- Step 1: Status Evaluation

  This step is the actual audit to be executed to determine the current status of the organisation’s information security. The output of this step will provide an overall information security status report to management. This report will illustrate, at a glance, if there are any warning signs that must be resolved immediately.

- Step 2: Re-assess Objectives

  This step is where each control objective, which relates to the warning sign areas reported in the previous step, is reviewed and relevant action plans are developed, which will include new or changed information security control objectives to be implemented to resolve areas where potential disaster could strike and ruin the organisation.

- Step 3: Implement Changes

  In this step, the changes and/or new control objectives, decided upon in the previous step, are actually implemented. After completing, this step, the process starts again at step 1 until the management of the organisation is completely satisfied with the overall "Health Check/Status" report.

The ISCAM will be supported by a self-help Information Security Control Audit Tool (ISCAT), which will assist organisations in ensuring that information security controls are achieving their objectives.

4.4 The Information Security Control Audit Tool (ISCAT)

The ISCAT has been developed in a language that can be understood by people who do not have an IT background; therefore, enabling a small to medium-sized organisation to implement an information security governance programme themselves (SANS Institute, 2003).

The tool provides results of an organisation's information security status and will identify potential warning signs that can assist it to take action immediately to prevent any ruinous disasters and also increase the information security status so that it is compliant with COBIT's information security controls.

The objectives of the ISCAT are listed as follows:

- It is a comprehensive tool, based on COBIT, an internationally recognised IT management framework;
- It provides regular assurance that business assets, particularly information, are properly protected from internal and external threats;
- It is a self-help tool, which is easy to use and can be implemented by personnel with limited IT backgrounds;
- It is specific to small to medium-sized organisations, and therefore, more focussed.

The ISCAT consists of three sections. The first section, which the user needs to complete, is the detailed information security control level, where information security-related audit questions are asked for each IT process defined in the COBIT framework.

This section contains 145 audit questions and next to each audit question, the user needs to provide the desired and the actual compliance key in accordance with the compliance reference list, described in the heading section.

Please refer to Appendix A, which contains the results of the case study performed in chapter five. Figure 4.2 provides an extraction of the audit questions from the Information Security Control Audit Tool.

		Compliance Key				
COBIT 4.0	Audit Question	Desired 0 1 2 3 4 5	Actual 0 1 2 3 4 5	Description None Very Bad Weak Acceptable Satisfactory Excellent	Score	Non-compliance Risk
DS	**Deliver and Support**	**5**	**3**	**Acceptable**	**60%**	
DS5	**Ensure Systems Security**	**5**	**3**	**Acceptable**	**60%**	
	Does the organisation have policies and procedures in place regarding information security?	5	3	Acceptable	60%	Lack of IT security governance. Unprotected data and information assets
	Do all systems require identification and authentication for all users, systems or external vendors before access is granted?	5	4	Satisfactory	80%	Unspecified security requirements for all systems – Compromised system information
	Do all systems clearly define access rights based on least privileges?	5	5	Excellent	100%	Segregation-of-duty violations
	Is the number of concurrent sessions limited to the user?	5	0	None	100%	Limit unauthorised access to systems and data

Figure 4.2: An Extract from the Information Security Control Audit Tool

The next section is a summary of the information security status per IT process, derived from the compliance keys provided by the user in the detailed section. Please refer to Appendix B, which contains the results of the case study performed in the next chapter.

The last section is an overall summary of the information security status per the four domains in the COBIT framework. This is also derived from the compliance keys provided by the user in the detailed section. Please refer to Appendix C, which contains the results of the case study performed in chapter five.

The final two sections of the ISCAT, depicted in Appendices B and C, are dashboard summaries to provide management with an overall view of its company's information security state without actually having to look at the details.

The ISCAT includes the following components:

- Audit questions for each detailed information security control objective in the COBIT framework (IT Governance Institute, 2007);

- Each audit question requires a desired and actual compliance key. The desired compliance key basically indicates how important that control is for the business. This assists the scores to be calculated based on the actual versus the desired compliance to the information security control;

- The compliance rating is indicated in the table below:

Key	**Compliance**	**Description**
0	None	No controls exist
1	Very Bad	Limited controls implemented and no compliance
2	Weak	Some controls implemented and some compliance
3	Acceptable	Some controls implemented and complied with
4	Satisfactory	Most controls implemented and complied with
5	Excellent	All controls implemented and complied with

- The score highlights the non-compliance business impact risk to the assessor in different colours, which are ranked as follows:

Range	Colour	Description
0 – 60 %	Red	Critical – requires immediate attention
61 – 80 %	Orange	Satisfactory – can be improved
Above 80 %	Green	Excellent – no attention required

- The non-compliance business impact refers to COBIT's IT Assurance Guide (IT Governance Institute, 2007) and the ISO/IEC 27002 standard (IT Governance Institute, 2006b; ISO/IEC 27002, 2005). COBIT's IT Assurance Guide details these business impact items as risk drivers. Risk drivers provide examples of the risks that may need to be avoided or mitigated. To assurance professionals and IT governance implementers, they provide the argument for implementing controls and substantiate the impact of not implementing them;

- The overall score (%) is calculated for the detailed control objectives by totalling the compliance rating and dividing it by the total of the weighting in terms of a percentage;

- This score is then referred to by the summary page to calculate the high-level control objectives' score. This then provides management with an overall information security status report, which highlights the most critical areas that require immediate attention. Management can then, based on this analysis, develop an action plan to make the necessary changes.

An instance of the ISCAT can be executed and saved and another instance created to re-iterate through the audit questions. This process continues until management accepts the results of the overall information security status report and all domains have a green colour – meaning no more attention is required.

The ISCAT was developed in Microsoft Excel and has all the relevant data validation rules in place to ensure the user can only enter the required values into the required data entry points.

4.5 Conclusion

This chapter introduced the Information Security Control Audit Model (ISCAM) and the Information Security Control Audit Tool (ISCAT) that supports it. The model focuses on the COBIT framework and COBIT's IT Assurance Guide; therefore, it is based on an internationally recognised IT governance framework.

The ISCAT has been developed in a language that can be understood by people who do not have an IT background; therefore, it enables a small to medium-sized organisation to implement an information security governance programme itself.

The next chapter will report on a case study in which the ISCAT was used to assess the information security status of an organisation. The chapter also reports on the results of an interview with the CEO of this particular company so as to include an independent review of the tool.

Chapter 5: CASE STUDY

5.1 Introduction

The previous chapter introduced the Information Security Control Audit Model (ISCAM) and the Information Security Control Audit Tool (ISCAT), a self-help audit tool that supports the model. It was, however, necessary to test the effectiveness of this tool. In order to do this, an actual organisation was requested to use the audit tool to evaluate its current information security status.

ABC Insurance, a small insurance company, agreed to use the ISCAT. The company provides a service to its customers and relies entirely on their information. ABC Insurance is an actual company, based in the Eastern Cape of South Africa; however, its name has been changed in this document.

In the initial interview with the CEO of ABC Insurance, he emphasised the importance of information security for the business as information is its livelihood - the organisation would cease to exist if the information was ever compromised in any way. The CEO did, however, mention that he did not actually know if all the controls and measures were in place to protect the information; rather, he merely assumed that they were. He, therefore, welcomed the implementation of the ISCAT and gave his full support for this project.

Before evaluating the process and results of the implementation of the ISCAT at ABC Insurance, some background information about the company is provided.

5.2 The Business Scenario

ABC Insurance's main objective is to provide income-protection benefits to its members in the event of them being unable to work due to illness. ABC receives a monthly premium (based on a percentage of the payroll of an employer) and pays benefits to an employee of the company, via the payroll, when that employee is unable to work due to illness.

In addition, supplementary benefits are offered to provide relief in the event of loss of income caused by periods of family bereavement, disability, maternity, lay-off and retrenchment.

The primary product which ABC has taken to market has been the CAPP product (Corporate Absenteeism Protection Programme).

The key components of this programme include:

- An initial risk assessment to understand the extent of absenteeism and the nature of the problem;
- The definition of a premium, normally based on no more than the exiting cost of absenteeism in the company;
- A proactive programme, including the Absenteeism Management Report, which will assist the customer in managing absenteeism;
- The customer recovers from ABC all of the costs of sick pay;
- The customer retains benefits derived from reduced indirect costs of absenteeism as a result of the reduction in absenteeism.

Key to the CAPP programme is the commitment by ABC to work with the customer to reduce absenteeism. The key advantage of and difference

between ABC products and other products is the ability of ABC to take on risk for absenteeism, which allows it to guarantee a fixed cost for absenteeism for customers.

Customers

ABC's customers include companies like Goodyear, Trentyre, Bridgestone, Dorbyl Automotive Technologies, Eveready, Welfit Oddy, amongst others.

Vision

ABC's vision is working for a healthier and more productive work force by proactively managing the time that employees are not at work.

Mission

ABC's mission is to be the dominant manager and insurer of time away from work.

Critical Success Factors

ABC has identified the following critical success factors in its business-strategy document:

- Obtain new business and sales;
- Develop new products;
- Successful customer relationship management and services;
- Efficient claims' management;
- Control cost, internal efficiency and accounting;
- Streamline internal business processes by using technology as an enabler.

The last point in this list highlighted the importance of ABC's business processes and underlining technology. Therefore, before we initiated the audit process, further investigation was carried out to obtain a background of the company's IT processes and technology in place, specifically focussing on the information security aspects.

5.3 Information Technology Background

The investigation into the IT background assisted us to understand more clearly ABC's IT processes and also to corroborate the truthfulness of the results of the audit tool.

ABC Insurance upgraded all its hardware and software about a year ago and standardised to HP machines. It also signed a service-level agreement with an external IT company to maintain all hardware, software, backups and disaster-recovery procedures.

ABC Insurance only has one IT Manager who must manage all IT projects and service requests to the external IT company.

The service-level agreement between ABC Insurance and the external IT company includes the following.

- Ensure back-ups are run on a daily basis, to be scheduled overnight;
- Test backups monthly;
- Test disaster recovery (quarterly);
- Change back-up tapes on a daily basis;
- Perform server and desktop support with regards to software additions, moves and changes;

- Ensure all equipment is running at peak performance and efficiency;
- Keep software patches/drivers up to date;
- Ensure Antivirus definitions are updated daily;
- Test network connectivity daily.

ABC Insurance only recently updated its IT Disaster Prevention and Recovery Plan, which was drafted with the assistance of the external IT company. The service-level agreement states that the Disaster Recovery Plan must be tested every quarter. This has been tested and the overall results were excellent, according to the reports provided to management.

The DRP document is split into two groups: disaster preventative measures and disaster recovery procedures.

The external IT company is responsible for most of the preventative measures related to:

- System security (firewall, web security and anti-virus software and network access management);
- Data storage and backup (successful backup every day, replacement of backup tapes and ensuring off-site storage of data backup tapes.)

ABC Insurance is responsible for the physical access to the building and information servers.

The following is a small subset of the rules included in the IT Disaster Prevention Plan:

- Password rules: (minimum length, alphanumeric, not easily guessable, expires every 6 weeks, changed with no reuse of old passwords, not to be shared amongst users under any circumstances);

- Users granted relevant access rights to resources according to job function and requirements;

- User accounts will be automatically locked when more than three attempts where made to gain access to the server;

- User accounts must be removed immediately from system on staff members leaving the company;

- Screen-saver passwords must be activated;

- Anti-virus protection must be installed on each PC;

- The Symantec Firewall must be monitored daily to investigate possible intrusion.

These measures all lessen the possibility or the impact of an adverse incident occurring. Thus, the risk and effects of disaster are managed, but not eliminated.

The disaster recovery section is very detailed and includes all parties involved (telephone numbers and backup numbers for them) and each party's responsibilities in the different scenarios, for example, what procedures to follow if the server crashed, or if the all hardware was stolen, or if the building burnt down, etc.

It also includes the location of backup tapes, the contact person to gain access to the office building, possible property management contact numbers

(to get a temporarily office location), contact numbers for other software vendors, etc.

In terms of security awareness, the employees at ABC Insurance are aware of information security to a certain extent, but no formal training has been given to them and no formal training has been planned for in the future. The IT person sends e-mails to staff to update them on latest virus news and what a user should do and not do, which has created some security awareness.

ABC Insurance has no formal information security awareness plan, which would make all employees aware of the risks and threats that exist and how they can ensure the protection of the organisation's information and systems.

ABC Insurance has no or little security procedures when hiring new employees or at the termination of an employee's contract.

In the contract that a new employee must sign is a clause stating that the employee undertakes to keep the employer's trade secrets or confidential information confidential.

ABC Insurance does not have any termination procedures for when an employee leaves the organisation such as an exit interview, where the employee is reminded of his/her contractual obligations such as nondisclosure agreements.

At this point of the project a great deal of information about ABC Insurance and on the overall IT functions in it was obtained. A meeting was then scheduled with the CEO, the Financial Manager, the IT Manager and the Technical Manager from the external IT Company to go through each audit question in the ISCAT together in order to obtain consensus on each answer among these four key ABC people and the outsourced IT company.

These results can be reviewed in Appendices A, B and C. In the next section, these results will be evaluated in more detail.

5.4 Evaluation

The overall summarised results, depicted in Appendix A, reflect a “Weak” to “Acceptable” state of information security at ABC Insurance. The management of ABC Insurance was quite shocked at these results as it had expected a “Satisfactory” overall rating in all four domains.

The CEO stated that this assessment had really opened their eyes and made them realise that they need to be more actively involved in the governance of information security in their organisation. The two domains that depict a “Weak” status are clearly areas that they need to attend to immediately themselves.

The first domain – Plan and Organise is the domain the management should be more involved in, as it needs to give direction in terms of information security. When management communicates its commitment to information security, the rest of the organisation will follow that commitment and be more aware of its importance.

In addition to the above statements, the following is a list of concerns raised in the audit that need to be attended to immediately:

- No information security strategy;
- No information security roles and responsibilities defined;
- No segregation of duties. ABC Insurance relies on one single IT person and the outsourced IT company that has access to all documentation and data in the organisation;

- No formal security incident reporting process;
- No formal process to ensure that the right information security skills are available;
- No formal security clearance process for staff;
- No formal termination process for staff to ensure all rights are revoked;
- No formal risk assessment process to ensure all security risks are identified and mitigated;
- No security evaluation process to ensure that all applications have all security requirements necessary to protect the organisation's assets;
- No security procedure documentation that staff can refer to;
- No change control procedure in place;
- The service-level agreement with the outsourced IT company does not include a non-disclosure guarantees section;
- No formal employee indoctrination process exists to ensure new staff members are aware of their information security responsibilities;
- No formal procedure in place to handle any problems;
- Visitors to the physical premises of the organisation are not signed in;
- No formal procedure in place to govern the receipt, removal and disposal of sensitive documentation;
- No internal information security control-monitoring process exists.

The last point in this list clearly highlights the need for the implementation of the model documented in chapter four, which is supported by the ISCAT used in this case study. The case study only performed step 1, the status evaluation step, of the ISCAM.

However, the entire ISCAM was discussed with the CEO of ABC Insurance and he has indicated that the company would like to implement this model to ensure the consistent monitoring of information security controls. He would then have peace of mind as he would know exactly what the position is regarding information security.

The CEO expressed his gratitude for approaching their company to test this audit tool and for opening his eyes to what the risks are for not complying with these information security controls.

5.5 Conclusion

In this chapter the effectiveness of the Information Security Control Audit Tool (ISCAT) was tested in a case study. The case study included the execution of the ISCAT at ABC Insurance. ABC found the tool quite simple and easy to use. The results clearly indicated the high risk areas to the management of ABC. They were unaware of their information security status and also unaware of the risks, presented in the ISCAT, for not complying with the audit question.

In an interview with the management of ABC they expressed how this tool has highlighted the importance of ensuring the right information security controls are in place to protect their business assets against potential threats. This just proves that the ISCAT has achieved its objectives.

Chapter 6: CONCLUSION

6.1 Introduction

Chapter one stated the fact that organisations are increasingly dependent on their information systems to support their business tasks. Compromise of these systems, either in terms of loss, or inaccuracy of information, or competitors gaining unauthorised access to the information in these systems can be extremely costly to an organisation.

Therefore, information security has become a major concern for all organisations, large and small. Information security is concerned with the protection of a company's biggest asset, its information. Many organisations implement some information security controls, but the biggest question is whether or not that is enough. Therefore, an organisation needs to develop and implement an information security governance programme that is based on an internationally accepted framework.

There are many standards and frameworks that can assist organisations to make sure they have all the right information security controls implemented, but many of these standards and frameworks are complex and more focussed on large enterprises.

The primary objective of this treatise, therefore, was to provide small to medium-sized organisations with a simple solution. This solution is the Information Security Control Audit Model (ISCAM), which is based on an internationally recognised framework, COBIT that will assist organisations to continuously conduct internal audits to help ensure all the right information security controls are implemented and adhered to.

The secondary objective of this treatise was to build a self-help audit tool, the Information Security Audit Tool (ISCAT) to support the ISCAM. This tool will

help small to medium-sized organisations to make the auditing process simple and easy to use, thus removing the complexity of ensuring they have all the right information security controls in place to protect their precious assets, their information.

The objective of this treatise is however not to assist an organisation with how to ensure information security, but to highlight for it where the risks are by conducting an audit and highlighting problem areas.

6.2 Review

IT auditing adds security, reliability and accuracy to those information systems integral to people's lives. Without IT auditing, it would not be possible to safely shop on the internet or control identities (Gallegos, Senft, Manson, & Gonzales, 2004). The role IT auditors play is perhaps unknown to most but it impacts upon the lives of everybody. This really emphasises the need for conducting information security audits in all organisations.

However, these audits need to be based on an already developed standard or framework, known to many organisations. The COBIT framework was used in this treatise, because IT auditors use it and it is an internationally recognised framework. The detailed control objectives within the COBIT framework address 'what' must be done, which is what the ISCAM must be based on.

Therefore an intense study on the COBIT framework was undertaken. The COBIT framework focuses on IT as a whole; therefore, the information security related controls that were used in ISCAM were highlighted.

The ISCAM was developed with the organisation's assets at its core, highlighting the importance of the protection of these assets. The information security controls govern the assets and the information security audit layer ensures the right controls are implemented.

The information security process included in the model was supported by the ISCAT. The audit tool was used first to evaluate an organisation's current status. In the next steps, the organisation had to review all the warning signs identified by the audit tool and develop and implement action plans to resolve the problems in these areas. The organisation then reiterated through these steps until the ISCAT revealed an acceptable status for all IT processes within all four domains of the COBIT framework.

An acceptable or satisfactory information security status will provide peace of mind to the management of the organisation that all necessary information security controls have been implemented.

However, organisations have to realise that this model has to be regularly applied to ensure a consistent, acceptable information security status.

6.3 Achievements

The success of implementing the ISCAT at ABC Insurance in the case study in chapter five illustrates the fact that the objectives set out in chapter one, to assist small to medium-sized organisations in ensuring that the most effective information security controls are implemented and that audit guidelines are consistently applied, have been achieved.

6.4 Further Research

This research document could form the basis for a technical project to develop an actual web-based ISCAT. This web-based application project could include all the steps of the ISCAM and track the assessments and actions performed by an organisation to achieve an acceptable information security status.

Because the model only focused on ‘what’ must be done, this future project could then also include the ISO 27002 standard to assist organisations in exactly ‘how’ to implement the right information security controls to achieve an acceptable information security status and ensure that all measures have been put in place to protect them from potential threats.

BIBLIOGRAPHY

Corporate Governance Task Force. (2004). *Information Security Governance – A Call to Action*. Retrieved April 15, 2006, from http://www.technet.org.

Gallegos, F., Senft, S., Manson, D. P. and Gonzales, C. (2004). *Information Technology Control and Audit, 2nd edition,* Auerbach Publications, New York

Gray, H. (2004). *Is there a relationship between IT governance and corporate governance?* Retrieved June 03, 2006, from http://www.itgi.org

Horton, T.R., Le Grand, C.H., Murray, W.H., Ozier, W.J. & Parker, D.B. (2000). *Information Security Management and Assurance: A Call to Action for Corporate Governance.* United States of America: The Institute of Internal Auditors.

ISO/IEC 27002. (2005). *ISO/IEC 27002:2005(E) – Information technology – Security techniques – Code of practice for information security management.* Geneva: Author.

IT Governance Institute. (2000). *COBIT 3rd Edition Audit Guidelines.* Rolling Meadows: Author. Retrieved May 8, 2006, from http://www.isaca.org

IT Governance Institute. (2000b). *COBIT 3rd Edition Control Objectives.* Rolling Meadows: Author. Retrieved May 8, 2006, from http://www.isaca.org

IT Governance Institute. (2001). *Information Security Governance: Guidance for Boards of Directors and Executive Management*. Rolling Meadows: Author. Retrieved May 8, 2006, from http://www.isaca.org

IT Governance Institute. (2003). *Board Briefing on IT Governance, 2nd Edition.* Rolling Meadows: Author. Retrieved May 8, 2006, from http://www.isaca.org

IT Governance Institute. (2005). *(COBIT) 4.0*. Rolling Meadows: Author. Retrieved April 20, 2006, from http://www.isaca.org

IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

IT Governance Institute. (2006b). COBIT Mapping. Mapping of ISO/IEC 27002:2000 with COBIT*, 2nd Edition*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

IT Governance Institute. (2007). *IT Assurance Guild using COBIT*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

IT Governance Institute. (2007b). *COBIT 4.1*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

IT Governance Institute. (2007c). *COBIT Security Baseline. An Information Security Survival Kit*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

IT Governance Institute. (2008). *Information Security Governance: Guidance for Information Security Manager*. Rolling Meadows: Author. Retrieved June 30, 2008, from http://www.isaca.org

SANS Institute. (2003). *Information Security Management. BS 7799.2:2002 Audit Check List*, London: Val Thiagarajan. Retrieved June 30, 2008, from www.sans.org

Von Solms, B. (2005). Information Security Governance: COBIT or ISO 27002 or Both? [Electronic version] *Computers & Security*, 24, 99-104.

Appendix A

Information Security Control Audit Status (Detailed Information Security Control Level)

Company:		ABC Insurance	Compliance Key				
		Please complete all Desired and Actual Compliance Keys next to each Audit Question!	**Desired**	**Actual**	**Description**		
			0	**0**	**None**		
			1	**1**	**Very Bad**		
			2	**2**	**Weak**		
			3	**3**	**Acceptable**		
	COBIT		**4**	**4**	**Satisfactory**		
Number	**4.0**	**Audit Question**	**5**	**5**	**Excellent**	**Score**	**Non-compliance Risk**
	PO	**Plan and Organise**	**5**	**2**	**Weak**	**38%**	
	PO1	**Define a Strategic IT Plan**	**5**	**3**	**None**	**69%**	
1		Does the company have an information security strategic plan document in place that defines the overall direction and goals of the organisation in terms of information security?	5	5	Excellent	100%	Benefits and risks of IS-enabled initiatives unclear or misunderstood.
2		Is this information security strategic plan aligned with the overall business and general IT strategic plan?	5	5	Excellent	100%	Not aligned with business objectives.

3		Does the information security strategic plan include an environmental study that will assist the organisation to look outside the organisation and how it might effect the organisation?	5	3	Acceptable	60%	Not compliance with regulatory requirements.
4		Does the information security strategic plan include a SWOT analysis to determine what is going on inside the organisation which will identify the internal strengths, weaknesses, opportunities and threats related to information security?	5	5	Excellent	100%	Opportunities and capabilities not leveraged and ineffective use of existing resources
5		Does the information security strategic plan include the organisations information security mission, vision and values?	5	5	Excellent	100%	Not focussed on the right priorities, which will result in confusion and lack support and commitment.
6		Does the information security strategic plan include the information security goals to accomplish in the next 3 years?	5	5	Excellent	100%	Long-range goals not achieved and priorities misunderstood
7		Does the information security strategic plan include the strategies/initiatives of how these goals (objectives), mentioned in the previous question?	5	3	Acceptable	60%	Unnecessary initiatives and investment
8		Does the information security strategic plan include who is responsible for these strategies/initiatives mentioned	5	0	None	0%	Undefined or confusing accountability and responsibility

		in previous question?					
9		Does the information security strategic plan include a timeline of when these information security goals/objectives must be met?	5	0	None	0%	Missed business opportunities due to deadlines not being met.
	PO2	**Define the Information Architecture**	**5**	**0**	**None**	**6%**	
10		Does the company have a data dictionary which incorporates the organisation's data syntax rules, which provides a common understanding of data amongst IT and business users?	5	0	None	0%	Data inconsistency between the organisation and systems.
11		Has all the critical data (data that must not be misused or lost), services (that need to be available) and transactions (that must be trusted) been identified in the data classification scheme?	5	0	None	0%	Business assets at risk if security requirements not documented
12		Is an inventory or register maintained with the important assets associated with each information system?	5	0	None		Business assets at risk if not identified and documented.
13		Has all the security requirements been identified for each of the components (data, services and transactions) in the data classification scheme?	5	0	None	0%	Business threats not identified.
14		Does the data classification scheme include the data ownership information, the definition of appropriate	5	0	None		Inappropriate security requirements. Occurrence of privacy, data confidentiality,

		security levels/controls, and a brief description of data retention and destruction requirements?					integrity and availability incidents.
15		Has security requirements been confirmed with business owners at regular intervals?	5	1	Very Bad	20%	Inappropriate security requirements.
16		Does the company ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives?	5	1	Very Bad	20%	Compromised information integrity and incompatible and inconsistent data.
	PO3	**Determine Technological Direction**	**5**	**2**	**Weak**	**40%**	
17		Has the organisations defined, in a information security technology infrastructure plan document, the information security technology standards and practices to be used, which is based on the business relevance, risks and compliance with external requirements?	5	2	Weak	40%	Non-compliance with regulatory requirements. Incompatibilities between technology platforms and applications. Licensing violations. Inability to access historical data on unsupported technology.
	PO4	**Define the IT Processes, Organisation and Relationships**	**5**	**2**	**Weak**	**32%**	
18		Has the organisation defined the specific processes, tasks and responsibilities for the management of information security?	5	2	Weak	40%	Conflicts and unclear interdependencies amongst processes.

19		Has these responsibilities mentioned in previous question been assigned, communicated and properly understood by the relevant resources?	5	1	Very Bad	20%	Insufficient support due to misunderstood responsibilities.
20		Has the risk been evaluated of concentrating too many security roles and responsibilities in one person?	5	1	Very Bad	20%	Financial loss and reputation damage; Malicious or unintentional damages.
21		Has the right resources been provided to exercise information security responsibilities effectively?	5	3	Acceptable	60%	Lack of appropriate skills.
22		Do the policies and procedures include the information security responsibilities of contractors and are they being implemented?	5	1	Very Bad	20%	Failure of contracted staff to adhere to organisational policies for the protection of information assets.
	PO6	**Communicate Management Aims and Direction**	**5**	**3**	**Acceptable**	**66%**	
23		Does management demonstrate a strong commitment to information security to foster a positive internal control environment throughout the organisation?	5	3	Acceptable	60%	Staff not committed if management is not committed.
24		Are the basic rules for meeting information security requirements and responding to security incidents consistently defined, communicated and regularly discussed?	5	2	Weak	40%	Greater number and impact of security breaches.

25		Are employees consistently reminded of security risks and their personal responsibilities?	5	4	Satisfactory	80%	Sensitive corporate information disclosed. Financial losses.
26		Are employees made aware of the requirement for the timely reporting of suspected security incidents?	5	4	Satisfactory	80%	Irregularities not identified or not identified in time to take precautionary action.
27		Do policies, standards and procedures exist that support the information security and the information control environment?	5	3	Acceptable	60%	Poor organisational security culture
28		Has a policy update process been defined that requires, at minimum, an annual review?	5	3	Acceptable	60%	Out-of-date or incomplete policies
29		Is there a management process that regularly communicate IT's objectives and direction.	5	4	Satisfactory	80%	Poor acceptance or understanding of the organisation policy due to miss-communication, which will result in lack of confidence and trust in IT's mission.
	PO7	**Manage IT Human Resources**	**5**	**2**	**Weak**	**37%**	
30		Does management identify information security skills needed, including appropriate education, cross-training and certification requirements to address the information security requirements of the organisation?	5	1	Very Bad	20%	Lack of appropriate information security skills.
31		Do the organisation’s personnel clearance procedures include the verification of skills using references and do	5	3	Acceptable	60%	Increased risk of threats occurring from within the organisation. Disclosure of

		background checks when hiring new staff?					customer or corporate information and increased exposure of corporate assets.
32		Does the information security training programme include the internal control framework and the security requirements based on the organisation's security policies and internal controls?	5	1	Very Bad	20%	Insufficient security awareness, causing errors or incidents.
33		Does the organisation perform an annual review of security skills and qualifications of staff to determine if they are up-to-date and in accordance to requirements?	5	2	Weak	40%	More security incidents and errors with greater impact.
34		Does the organisation prevent the reliance on a single individual for critical processes with the organisation?	5	1	Very Bad	20%	Increased number and impact of incidents caused by unavailability of essential skills to perform a critical role due e.g. to rely on a single individual that might not be available at time of security related incident.
35		Does the organisation have exit procedures of termination of employment that includes the revoking of security rights to the organisation's asses?	5	3	Acceptable	60%	Unauthorised access when employees are terminated.
36		Does the organisation perform information security-related performance evaluation for related employees?	5	2	Weak	40%	Dissatisfied and disgruntled staff, leading to retention of problems and possible

							incidents. Loss of competent staff members and related corporate knowledge.
	PO8	**Manage Quality**	**5**	**3**	**Acceptable**	**60%**	
37		Does the organisation implement development and acquisition standards that will enable an appropriate level of control for changes to existing IT resources (e.g. secure coding practices; software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standard; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; unit, regression and integration testing)?	5	3	Acceptable	60%	Unidentified errors occurring in production.
	PO9	**Assess and Manage IT Risk**	**5**	**0**	**None**	**0%**	
38		Does the organisation have a formal risk assessment procedure that is executed on a regular basis?	5	0	None	0%	Risks not identified and could lead to loss of IT assets, confidentiality or integrity breaches of the IT assets.
39		Does the risk assessment procedure include the identification of agreed-upon IT risks, mitigation	5	0	None	0%	Significant risks not given appropriate attention. Unidentified residual business

		strategies and residual risks?					risks.
40		Does the risk identification process consider both external and internal threats?	5	0	None	0%	
41		Does management discuss, with key staff from business and IT management, where and when security problems can adversely impact business objectives and how to protect against them?	5	0	None	0%	Ineffective support for risk assessment by senior management. IT risks and business risks managed independently.
42		Is the risk assessment results inspected to identify whether mitigating response were allocated to avoid, transfer, reduce, share or accept each risk and align with the mechanisms used to manage risk in the organisation?	5	0	None	0%	Ineffective use of resources to respond to risks. Unidentified residual business risks. Risk responses not effective.
43		Is there sufficient coverage that offset the accepted residual risk?	5	0	None	0%	Financial losses.
44		Is a risk management action plan developed to address all risks?	5	0	None	0%	Loss of IT assets
	AI	**Acquire and Implement**	**5**	**3**	**Acceptable**	**51%**	
	AI1	**Identify Automated Solutions**	**5**	**1**	**Very Bad**	**15%**	
45		Was a full security evaluation performed for all	5	0	None	0%	Potentially significant risks not identified.

		automated and third-party solutions acquired?					
46		Did the organisation determine the trustworthiness of the selected automated security technology/services through references, external advice, contractual arrangements, etc?	5	0	None	0%	System security compromised
47		Was a risk analysis of the automated solutions prepared and signed off by the key stakeholders, including representatives from the business and IT?	5	0	None	0%	Management unaware of risk and failure of applying appropriate controls
48		Was appropriate information security risk mitigation mechanisms build into automated solution?	5	3	Acceptable	60%	System security compromised
	AI2	**Acquire and Maintain Application Software**	**5**	**4**	**Satisfactory**	**73%**	
49		Did the suppliers and developers ensure that the application infrastructure properly support security requirements in a consistent manner?	5	3	Acceptable	60%	Gaps between application controls and actual threats and risks. Undetected security violations
50		Does the organisation ensure that only appropriately licensed software is tested and installed and that installation is performed in accordance with vendor?	5	5	Excellent	100%	Violation of licence agreements.

51		Does the organisation review the detailed design document when acquiring new application software to determine if the availability, integrity and confidentiality of output data to other programmes are appropriately addressed?	5	3	Acceptable	60%	Data in application systems processed incorrectly.
	AI3	**Acquire and Maintain Technology Infrastructure**	**5**	**3**	**Acceptable**	**60%**	
52		Did the suppliers and developers ensure that the technology infrastructure properly support security requirements in a consistent manner?	5	3	Acceptable	60%	Information security compromised.
53		Did the organisation document which additional security measures are needed to protect the technology infrastructure itself?	5	1	Very Bad	20%	Unauthorised access to sensitive software
54		Does the organisation identify and monitor sources for keeping up to date with security patches, and implement those appropriate for the enterprise infrastructure?	5	5	Excellent	100%	Compromised confidentiality, integrity and availability of system due to new security breaches discovered if system patches and updates are not implemented.
55		Does the organisation ensure that temporary access granted for installation purposes is monitored and that passwords are changed immediately after installation?	5	3	Acceptable	60%	Unauthorised access to sensitive software

	AI4	**Enable Operation and Use**	**5**	**3**	**Acceptable**	**53%**	
56		Does staff member know how to integrate security in their day-to-day procedures?	5	3	Acceptable	60%	Problems in daily operations.
57		Do staff members have security procedure documentation available?	5	2	Weak	40%	Help desk overloaded.
58		Were staff members trained on security matters?	5	3	Acceptable	60%	Help desk overloaded.
	AI6	**Manage Changes**	**5**	**0**	**None**	**0%**	
59		Does the organisation have a formal change management procedure?	5	0	None	0%	No tracking of changes.
60		Does the organisation evaluate the impact a change could have on the data integrity, exposure or loss of sensitive data, availability of critical services, and validity of important transactions?	5	0	None	0%	Unintended side effects.
61		Does the organisation consider the security, legal, contractual and compliance implications in the assessment process of each change request?	5	0	None	0%	Adverse effects on capacity and performance of the infrastructure.
62		Does all change requests go through a formal approval process which includes the business process owners?	5	0	None	0%	Unauthorised changes applied, resulting in compromised security and unauthorised access to corporate information.

63		Does the organisation perform adequate testing prior to making the change?	5	0	None	0%	Reduced system availability as changes need to be fixed.
64		Does the organisation prioritise changes appropriately?	5	0	None	0%	Lack of priority management of changes.
65		Does the organisation properly track the status of a change request and is this properly documented?	5	0	None	0%	Changes not recorded and tracked.
	AI7	**Install and Accredit Solutions and Changes**	**5**	**4**	**Satisfactory**	**75%**	
66		Does the organisation validate the security and performance requirements of all new systems before they are made operational once developed or acquired?	5	3	Acceptable	60%	Degraded overall security.
67		Does the organisation test the fallback and backup plans prior to promoting system into production?	5	4	Satisfactory	80%	Disaster recovery procedures not in place or not properly tested.
68		Does the organisation test the systems in an appropriate test environment before deploying into production environment?	5	4	Satisfactory	80%	System and data errors in production environment.
69		Does the organisation involve key staff members when performing the testing of systems?	5	4	Satisfactory	80%	Unsupported systems.
	DS	**Deliver and Support**	**5**	**3**	**Acceptable**	**60%**	

	DS1	**Define and Manage Service Levels**	**5**	**3**	**Acceptable**	**60%**	
70		Does management ensure and regularly review that security requirements are included in all internal service level agreements and contracts (SLA's) with third-party service providers?	5	3	Acceptable	60%	Failure to meet security requirements for customer services. Financial losses and reputational damage because of vender services being interrupted due to security breaches.
	DS2	**Manage Third-party Services**	**5**	**3**	**Acceptable**	**50%**	
71		Are the capabilities of all third-party vendors assessed to ensure that they provide a contact person who possesses the authority to act upon enterprise security requirements and concerns?	5	4	Satisfactory	80%	Vendor not responsive or committed to the relationship.
72		Does the organisation consider the dependence on third-party suppliers for security requirements, and mitigate continuity, confidentiality and intellectual property risks by implementing such measures as escrow, legal liabilities, penalties and rewards?	5	4	Satisfactory	80%	Financial losses and reputational damage because of service interruption.
73		Does the third-party contract include a process to resolve problems?	5	1	Very Bad	20%	Problems and issues not resolved.
74		Does the third-party contract include a reporting of service process?	5	2	Weak	40%	Inadequate service quality.

75		Does the third-party contract include the roles and responsibilities of all resources?	5	4	Satisfactory	80%	Unclear roles and responsibilities leading to miscommunications, poor services and increased costs.
76		Does the third-party contract include the levels of access provided to the vendors?	5	2	Weak	40%	Unauthorised access to sensitive information.
77		Does the third-party contract include non-disclosure guarantees?	5	0	None	0%	Information security breaches.
78		Does the third-party contract state that the organisation has right to audit their services?	5	0	None	0%	Non-compliance with regulatory and legal obligations.
79		Is there a contingency plan in place for all contracted services, especially disaster recovery services for the IT function?	5	4	Satisfactory	80%	Financial losses and reputational damage because of service interruption.
80		Does the security access list only include minimum number of vender staff as required, and that access is the least needed?	5	4	Satisfactory	80%	Unauthorised access to sensitive information.
	DS4	**Ensure Continuous Service**	**5**	**5**	**Excellent**	**100%**	
81		Does the organisation have a formal continuity (disaster recovery) plan in place?	5	5	Excellent	100%	Insufficient continuity practices, which will lead to financial losses due to interruptions in service deliver to clients.
82		Is the continuity (disaster recovery) plan current?	5	5	Excellent	100%	Outdated recovery plans that do not reflect

							the current architecture.
83		Is the continuity (disaster recovery) plan communicated to all relevant resources?	5	5	Excellent	100%	Confusion and delays during recovery process.
84		Is the continuity (disaster recovery) plan reviewed and approved by the appropriate levels of senior management?	5	5	Excellent	100%	Shortcomings in recovery plans not identified.
85		Are the required business interruption or loss insurance policies in place for when a disaster occurs?	5	5	Excellent	100%	Financial losses due to replacement cost of equipment.
86		Does the content of the continuity (disaster recovery) plan include the roles and responsibilities of all the parties?	5	5	Excellent	100%	Confusion and delays during recovery process due to miscommunication of roles and responsibilities.
87		Does the content of the continuity (disaster recovery) plan include a listing from highest to lowest, based on business needs, of all the systems resources (e.g. hardware, peripherals, software) that must be purchased and redeployed?	5	5	Excellent	100%	Failure to recover business-critical systems and services in a timely manner.
88		Does the content of the continuity (disaster recovery) plan include the logistical information on location of key resources and names, addresses, telephone numbers of key personnel?	5	5	Excellent	100%	Unavailability of critical IT resources. Outdated contact information of key personnel.

89		Does the content of the continuity (disaster recovery) plan include the information about the backup-site and backup-tapes for recovering operating systems, applications, data files, operating manuals and programme/system/user documentation?	5	5	Excellent	100%	Inability to locate backup tapes when needed. Unavailability of backup data and media due to missing documentation in offsite storage.
90		Is the continuity (disaster recovery) plan tested on a regular basis?	5	5	Excellent	100%	Shortcomings in recovery plans not identified
	DS5	**Ensure Systems Security**	**5**	**4**	**Satisfactory**	**80%**	
91		Does the organisation have policies and procedures in place regarding information security?	5	3	Acceptable	60%	Lack of IT security governance. Unprotected data and information assets.
92		Do all systems require identification and authentication for all users, systems or external vendors before access is granted?	5	4	Satisfactory	80%	Unspecified security requirements for all systems – Compromised system information
93		Do all systems clearly define access rights based on least privileges?	5	5	Excellent	100%	Segregation-of-duty violations
94		Are all modifications to access rights of roles approved and regularly reviewed by process owner management?	5	3	Acceptable	60%	Access management failing business requirements and compromising the security of business-critical systems
95		Is the number of concurrent sessions limited to the user?	5	5	Excellent	100%	Limit unauthorised access to systems and data

96		At log-on, does an advisory warning message show to users regarding the appropriate use of hardware and software?	5	5	Excellent	100%	Inadequate User awareness of consequences to unlawful actions
97		Does the password policy include an appropriate minimum password length?	5	5	Excellent	100%	Limit password recovery software to prevent unauthorised access to systems and data
98		Does the password policy enforced frequency of password changes?	5	5	Excellent	100%	Limit password recovery software to prevent unauthorised access to systems and data
99		Does the password policy check passwords against list of not allowed values?	5	5	Excellent	100%	Limit password recovery software to prevent unauthorised access to systems and data
100		Does the dial-in procedure include dial-back authentication, frequent changes of dial-up number, software and hardware firewalls and frequent changes of password and deactivation of former employees' passwords?	5	5	Excellent	100%	Limit unauthorised access to systems and data
101		Does the security features include the identification and authentication process to be repeated after a specified period on inactivity (Auto-lock)?	5	5	Excellent	100%	Limit unauthorised access to systems and data

102		Does the organisation immediately revoke all access rights and close a user's account on termination of services?	5	2	Weak	40%	Failure to terminate unused accounts in a timely manner, thus impacting corporate security.
103		Does employee indoctrination include security awareness, ownership responsibility and virus protection requirements?	5	1	Very Bad	20%	Users not aware of the IT security plan and their responsibilities.
104		Are security breaches reported and resolved in a timely manner?	5	3	Acceptable	60%	Incidents not solved in a timely manner
105		Is security-related hardware and software, such as cryptographic modules and firewalls protected against tampering or disclosure, and is access to these hardware and software limited to a "need to know" basis?	5	5	Excellent	100%	Compromised overall security architecture
106		Do changes to the security software go through a formal change control procedure?	5	1	Very Bad	20%	Compromised overall security architecture
107		Has preventative and detective control measures been implemented with respect to computer viruses?	5	5	Excellent	100%	Systems attacked by viruses.
108		Does the network monitoring software alert management of security breaches?	5	4	Satisfactory	80%	Security breaches not detected in a timely manner.
109		Are all software checked for viruses prior to installation	5	2	Weak	40%	Systems attacked by viruses.

		and use?					
110		Does a policy exist on downloading, acceptance, and use of freeware and shareware, and is the policy adhered to?	5	5	Excellent	100%	Security breaches.
111		Are users trained on what procedures to follow in the event of detecting and reporting of viruses, which include the possibility of a machine being invested by a virus if the machine shows sluggish performance or mysterious growth of files?	5	2	Weak	40%	Users failing to comply with security policy
112		Are all installed software authorised and properly licensed?	5	5	Excellent	100%	Violation of legal and regulatory requirements
113		Is a firewall appliance or software in place to protect the internal network from the outside world?	5	5	Excellent	100%	Security breaches not detected in a timely manner.
114		Does all traffic going in and out through the network pass through the firewall?	5	5	Excellent	100%	Security breaches not detected in a timely manner.
115		Does the firewall implement strong authentication measures?	5	5	Excellent	100%	Security breaches not detected in a timely manner.
	DS7	**Educate and train users**	**5**	**3**	**Acceptable**	**60%**	
116		Do all employees have awareness and understanding of security, controls and fiduciary responsibilities of using IT	5	3	Acceptable	60%	Employees not aware of their security responsibilities.

		resources?					
	DS9	**Manage the Configuration**	**5**	**2**	**Weak**	**40%**	
117		Does the organisation ensure that access to the configuration of any hardware and software are restricted to appropriate personnel?	5	4	Satisfactory	80%	Unauthorised changes to hardware and software not discovered which could result in security breaches.
118		Does the organisation physically tag their assets accordingly?	5	0	None	0%	Assets not protected properly.
	DS10	**Manage Problems**	**5**	**0**	**None**	**0%**	
119		Does the organisation have adequate processes in place that are supported by appropriate tools that help register, classify, prioritise and track problems to resolution?	5	0	None	0%	Loss of information and disruption to business services.
	DS11	**Manage Data**	**5**	**5**	**Excellent**	**90%**	
120		Is data integrity (accuracy, completeness and validity) checked during input, process, storage and distribution processes?	5	4	Satisfactory	80%	Date integrity compromised. Unusable information.
121		Do audit trails exist in all systems to facilitate the tracing of transaction processing and the reconciliation of information?	5	5	Excellent	100%	Data altered by unauthorised users

122		Does adequate protection exist over sensitive information during transmission and transport against unauthorised access and modification?	5	5	Excellent	100%	Disclosure of corporate information.
123		Are sensitive reports only accessed by approved personnel?	5	5	Excellent	100%	Sensitive data misused or destroyed.
124		Does data retention period comply with user and legal requirements?	5	4	Satisfactory	80%	Business, legal and regulatory requirements not met.
125		Is the current media backup and restoration strategy appropriate?	5	5	Excellent	100%	Inability to restore data in the event of a disaster
126		Is the backup media stored in a secure off-site location?	5	5	Excellent	100%	Backup data unavailable when needed
127		Are the controls adequate enough for data at off-site storage and while data is in transit?	5	3	Acceptable	60%	Disclosure of corporate information.
	DS12	**Manage the Physical Environment**	**5**	**2**	**Weak**	**44%**	
128		Are the logical and physical access and security profiles for employees, vendors, visitors and facility maintenance staff sufficient?	5	2	Weak	40%	Visitors, employees, vendors or maintenance staff gaining unauthorised access to IT equipment or information.
129		Are the "key" and "card reader" management procedures and practices adequate and adhered to?	5	0	None	0%	Hardware stolen by unauthorised people.
130		Are the access and authorisation policies on entering/leaving, escort, registration, temporary required	5	0	None	0%	Physical attack on the IT site

		passes, surveillance camera adequate?					
131		Is the computer room separate, locked and accessed only by operations personnel and maintenance people on an as needed basis?	5	5	Excellent	100%	Unauthorised entry to secure areas.
132		Is staff with access actual employees?	5	5	Excellent	100%	Unauthorised entry to secure areas.
133		Are the alarm maintenance logs locked in such a way that it cannot be inappropriately changed?	5	3	Acceptable	60%	Devices reconfigured without authorisation.
134		Are the access codes changed on a regular basis?	5	1	Very Bad	20%	Unauthorised entry to secure areas.
135		Is a security penetration test of facilities performed on a regular basis by and external company?	5	0	None	0%	Physical attack on the IT site
136		Are the locks and hinges to the computer room checked on a regular basis?	5	4	Satisfactory	80%	Physical attack on the IT site
137		Are video monitoring tapes reviewed on an ongoing basis?	5	0	None	0%	Staff stealing equipment
138		Are uninterruptible power supplies (UPS) installed and maintained as an alternative infrastructure item necessary to implement security?	5	4	Satisfactory	80%	Security devices disrupted by power cuts.
	DS13	**Manage Operations**	**5**	**3**	**Acceptable**	**50%**	
139		Does the organisation have appropriate infrastructure	5	3	Acceptable	60%	Infrastructure problems undetected and

		monitoring in place that considers any risks that might exist?					occurrence of security incidents.
140		Does the organisation have procedures in place to govern the receipt, removal and disposal of sensitive documentation?	5	2	Weak	40%	Misuse of sensitive IT asses, leading to financial losses and other business impacts.
	ME	**Monitor and Evaluate**	**5**	**2**	**Weak**	**30%**	
	ME2	**Monitor and Evaluate Internal Control**	**5**	**0**	None	**0%**	
141		Are the actual internal controls compared to planned internal control reviews in all IT areas?	5	0	None	0%	Control weaknesses hampering effective business process execution.
142		Do internal control monitoring reports exist?	5	0	None	0%	Undetected malfunctioning of internal control components.
143		Does management review internal control reports and initiate corrective action where necessary?	5	0	None	0%	Management not informed about control deficiencies.
144		Are senior management satisfied with reporting on security and internal control monitoring?	5	0	None	0%	Inaccurate or incomplete control deficiency data, resulting in erroneous management decisions
	ME3	**Ensure Compliance with External Requirements**	**5**	**3**	**Acceptable**	**60%**	

145		Has an independent review been performed of the organisations IT security services?	5	3	Acceptable	60%	Financial losses and penalties

Appendix B

Information Security Control Audit Status

(Summary of IT Process Level)

Company:	ABC Insurance	Compliance Key				
		Desired	Actual	Description		
		0	0	None		
		1	1	Very Bad		
		2	2	Weak		
		3	3	Acceptable		
		4	4	Satisfactory		
COBIT 4.0	Domain and IT Processes	5	5	Excellent	Score	Non-compliance Risk
PO	**Plan and Organise**	**5**	**2**	**Weak**	**38%**	
PO1	Define a Strategic IT Plan	5	3	Acceptable	69%	Information security requirements not priorities and focussed on, which will result in confusion, lack of support and commitment.
PO2	Define the Information Architecture	5	0	None	6%	Business assets at risk if security requirements are not identified and documented.
PO3	Determine Technological Direction	5	2	Weak	40%	Licensing violations and non-compliance with regulatory requirements.

PO4	Define the IT Processes, Organisation and Relationships	5	2	Weak	32%	Insufficient support due to misunderstood security responsibilities.
PO6	Communicate Management Aims and Direction	5	3	Acceptable	66%	Staff not committed it management's commitment is not communicated.
PO7	Manage IT Human Resources	5	2	Weak	37%	More frequent security incidents because of lack of security skills, security awareness programmes and access rights not being reviewed on a regular basis.
PO8	Manage Quality	5	3	Acceptable	60%	Unidentified errors occurring in production.
PO9	Assess and Manage IT Risk	5	0	None	0%	Risks not identified and could lead to loss of IT assets, confidentiality or integrity breaches of the IT assets.
AI	**Acquire and Implement**	**5**	**3**	**Acceptable**	**51%**	
AI1	Identify Automated Solutions	5	1	Very Bad	15%	System security compromised
AI2	Acquire and Maintain Application Software	5	4	Satisfactory	73%	Gaps between application controls and actual threats and risks. Undetected security violations
AI3	Acquire and Maintain Technology Infrastructure	5	3	Acceptable	60%	Unauthorised access to sensitive software
AI4	Enable Operation and Use	5	3	Acceptable	53%	Problems in daily operations.

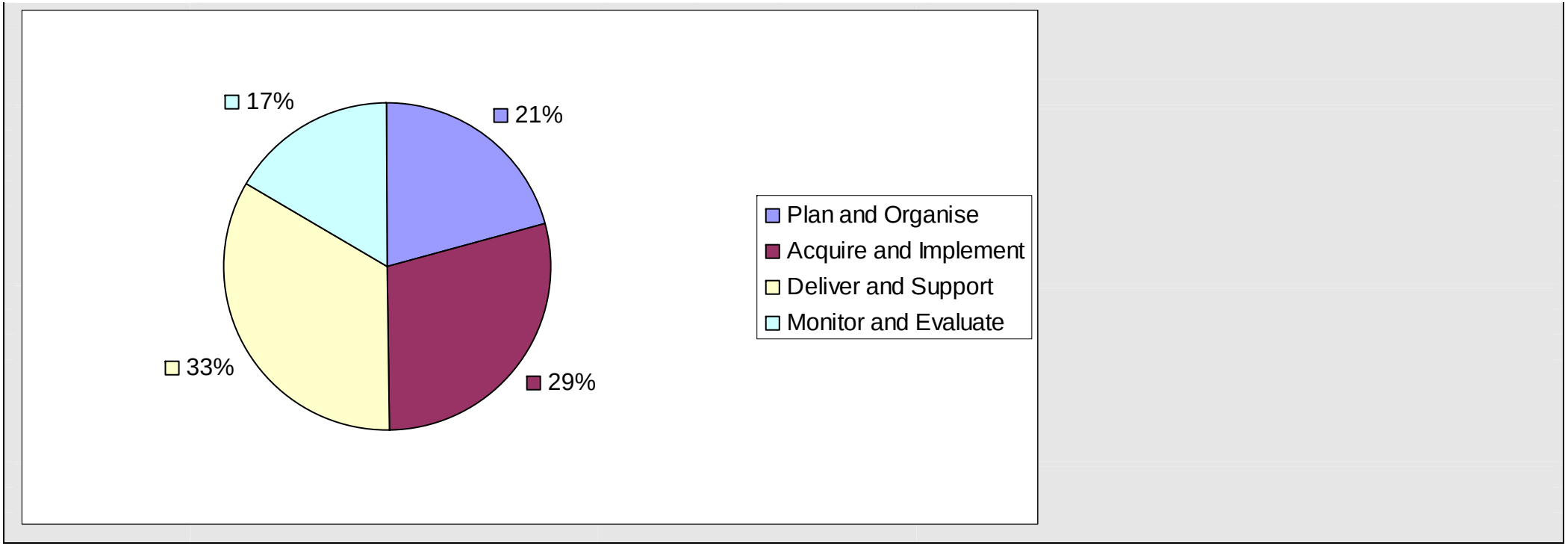
AI6	Manage Changes	5	0	None	0%	Unauthorised changes applied, resulting in compromised security and unauthorised access to corporate information.
AI7	Install and Accredit Solutions and Changes	5	4	Satisfactory	75%	Degraded overall security.
DS	**Deliver and Support**	**5**	**3**	**Acceptable**	**60%**	
DS1	Define and Manage Service Levels	5	3	Acceptable	60%	Failure to meet security requirements for customer services. Financial losses and reputational damage because of vender services being interrupted due to security breaches.
DS2	Manage Third-party Services	5	3	Acceptable	50%	Unauthorised access to sensitive information.
DS4	Ensure Continuous Service	5	5	Excellent	100%	Insufficient continuity practices, which will lead to financial losses due to interruptions in service deliver to clients.
DS5	Ensure Systems Security	5	4	Satisfactory	80%	Lack of IT security governance. Unprotected data and information assets.
DS7	Educate and train users	5	3	Acceptable	60%	Employees not aware of their security responsibilities.
DS9	Manage the Configuration	5	2	Weak	40%	Unauthorised changes to hardware and software are not discovered, which could result in security breaches.
DS10	Manage Problems	5	0	None	0%	Loss of information and disruption to business services.
DS11	Manage Data	5	5	Excellent	90%	Data altered by unauthorised users
DS12	Manage the Physical Environment	5	2	Weak	44%	Unauthorised entry to secure areas.

DS13	Manage Operations	5	3	Acceptable	50%	Infrastructure problems undetected and occurrence of security incidents.
ME	**Monitor and Evaluate**	**5**	**2**	**Weak**	**30%**	
ME2	Monitor and Evaluate Internal Control	5	0	None	0%	Undetected malfunctioning of internal control components.
ME3	Ensure Compliance with External Requirements	5	3	Acceptable	60%	Financial losses and penalties

Appendix C

Information Security Control Audit Status
(Summary of IT Process Level)

Company:	ABC Insurance	Compliance Key				
		Desired	Actual	Description		
		0	0	None		
		1	1	Very Bad		
		2	2	Weak		
		3	3	Acceptable		
		4	4	Satisfactory		
COBIT 4.0	Domain	5	5	Excellent	Score	Non-compliance Risk
PO	Plan and Organise	5	2	Weak	38%	No direction provided in terms of information security by management
AI	Acquire and Implement	5	3	Acceptable	51%	Information security not considered in the acquisition and implementation of all applications and infrastructure networks and devices
DS	Deliver and Support	5	3	Acceptable	60%	Information security not considered in all services provided by the organisation and services requested by vendors, which could lead to unauthorised access to sensitive information which will lead to financial losses and reputation damages.
ME	Monitor and Evaluate	5	2	Weak	30%	Information security controls are not all monitored to ensure that the direction provided is actually followed.


17%
21%
33%
29%
Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate