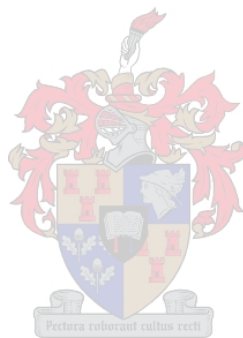


## **Governance of virtual private networks using COBIT as framework**

Zaida Sherry

Assignment presented in partial fulfilment of the degree of Master of Accounting at Stellenbosch University



Professor Willie Boshoff  
April 2007

## Declaration

I, the undersigned, hereby declare that the work contained in this assignment is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Signature: .....

Date: .....



## **Abstract**

The purpose of this assignment is to ascertain whether the COBIT framework is an adequate framework to assist in the governance of virtual private networks. The assignment focuses on whether the framework can ensure the identification of virtual private network-related risks and address IT compliance with policies and statutory regulations.

A brief summary of the risks and issues pertaining to the pre-implementation, implementation and post-implementation phases of virtual private networks is included in the assignment. These risks and issues are then individually mapped onto a relevant COBIT control objective. The scope of the assignment does not include the intricacies of how these networks operate, the different types of network topologies or the different technologies used in virtual private networks.

It was found that the COBIT framework can be implemented to manage and/or mitigate virtual private network risks.

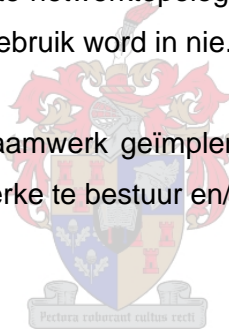


## Opsomming

Die doel van hierdie werkstuk is om te bepaal of die COBIT-raamwerk 'n toereikende raamwerk is om tot die beheer van virtuele privaat netwerke by te dra. Die werkstuk fokus op die vraag of die raamwerk die risiko's verbonde aan virtuele privaat netwerke kan identifiseer en IT se nakoming van beleid en statutêre regulasies kan verseker.

'n Bondige opsomming van die risiko's van die voor-implementerings-, implementerings- en ná-implementeringsfases van virtuele privaat netwerke en die kwessies verbonde daaraan maak deel van die werkstuk uit. Hierdie risiko's en kwessies word dan elkeen afsonderlik op 'n tersaaklike COBIT-beheerdoelwit afgebeeld. Die werkstuk se omvang sluit nie die fynere punte van hierdie netwerke se werking, die verskillende soorte netwerktopologieë of die verskillende tegnologieë wat in virtuele privaat netwerke gebruik word in nie.

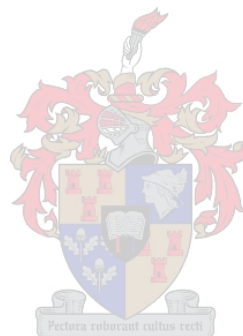
Daar is gevind dat die COBIT-raamwerk geïmplementeer kan word om risiko's ten opsigte van virtuele privaat netwerke te bestuur en/of te temper.



## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	Background and problem statement.....	1
1.2	Purpose of the study.....	3
1.3	Scope.....	3
1.4	Research methodology and subsequent chapters .....	3
<b>2</b>	<b>VIRTUAL PRIVATE NETWORKS (VPNs).....</b>	<b>5</b>
2.1	An overview of VPNs .....	5
2.2	The importance of VPNs.....	6
2.3	VPN types and models.....	7
2.3.1	Trusted VPNs .....	7
2.3.2	Secure VPNs .....	7
2.3.3	Hybrid VPNs .....	8
2.4	Requirements for VPNs .....	8
2.5	VPNs explained .....	9
2.5.1	Tunnelling and encapsulation .....	9
2.5.2	Encryption.....	9
2.5.3	Key management.....	10
2.5.4	User authentication and data authentication .....	10
<b>3</b>	<b>VPN GOVERNANCE.....</b>	<b>11</b>
3.1	Governance explained.....	11
3.2	The importance of governance and internal control .....	12
3.3	Risks inherent to VPNs.....	13
3.4	VPN control objectives .....	14
<b>4</b>	<b>COBIT.....</b>	<b>15</b>
4.1	The reason for selecting COBIT.....	15
4.2	The COBIT framework.....	16
4.2.1	Process-oriented.....	17
4.2.2	COBIT IT processes defined within the four domains .....	18
<b>5</b>	<b>VPN COBIT MATRIX.....</b>	<b>21</b>
5.1	Methodology .....	21
5.2	Matrices.....	21

5.2.1 Plan and organise.....	23
5.2.2 Acquire and implement.....	31
5.2.3 Deliver and support.....	34
5.2.4 Monitor and evaluate.....	44
<b>6 SUMMARY AND CONCLUSION .....</b>	<b>49</b>
<b>BIBLIOGRAPHY.....</b>	<b>51</b>



# Chapter 1

## 1 Introduction

### 1.1 Background and problem statement

Haymaker (2003:18) states the following:

A good governance framework pays big dividends. Beyond corporate governance, organisations also need to look at their enterprise governance and IT (Information Technology) governance activities. Firms need to make sure they have a comprehensive and coordinated accountability framework that streamlines and focuses the tremendous resources of their firms to provide maximum and sustainable value.

Corporate scandals over the past several years have resulted in an increased focus on enterprise and corporate governance. A rise in antiterrorism, privacy and other laws has raised the stakes for all organisations, clearly conveying the message that governance is no longer a luxury, and that it should be embedded in the way organisations conduct their business. (Haymaker & Hutton, 2004:48)

The US Sarbanes-Oxley Act of 2002 serves as an example of legislation instituted to address these imbalances. According to Shue (2004:28), the Act has essentially changed the way business and the regulatory environment view corporate governance and will ultimately strengthen corporate accountability, financial disclosure and reporting.

IT governance is an integral part of corporate governance in setting a standard of corporate integrity and enhancing shareholder value. IT governance goes beyond IT audit and beyond what the chief information officer can accomplish by him- or herself. Depending on the organisation, IT governance may be the enabler for an organisation to move to the next level or it may be the only way an organisation can meet regulatory and legal requirements (Haymaker & Hutton, 2004:50).

The Board Briefing on IT Governance (IT Governance Institute, 2003:36) states that “COBIT (Control Objectives for Information and related Technology), issued by the IT Governance Institute, is increasingly accepted internationally as good practice for control over information, IT and related risks. Its guidance enables an enterprise to implement effective governance over the IT that is persuasive and intrinsic throughout the enterprise”.

It is therefore necessary that IT governance is properly understood to ensure that overall governance and proper controls are implemented. It is also important that IT management has a suitable approach, guidelines and the proper tools to ensure that IT governance is implemented appropriately to be in line with best practices and the organisation's needs.

One of the many IT technology areas that require effective governance and would have an impact on the organisation's overall governance is virtual private networks (VPNs). This form of technology has numerous risks – associated with security, third parties, business, implementation, and operations – that need to be mitigated (ISACA, 2004:4). Virtual private networks extend the reach of LANs without requiring owned or leased private lines. Companies can use VPNs to provide remote and mobile users with network access, connect geographically separated branches into a unified network, and enable the remote use of applications that rely on external servers (Heller, 2006).

The purpose of this technology is to enable remote users to have access to the organisation's network and applications regardless of their location. In utilising these networks, the organisation may be faced with numerous security and data integrity issues (Fowler, 1999:175). It is therefore of utmost importance that adequate control objectives are developed to address these potential risks and that compliance with these objectives is properly governed.

To govern IT effectively, it is important to appreciate the activities and risks with relation to IT that need to be managed (ISACA, 2005:13). To determine whether COBIT is a suitable framework for the governance of VPNs, a comprehension of the risks and issues that would affect VPNs is required. It is therefore necessary to first understand the different VPN models, VPN technology requirements and how VPNs work in order to value the risks and issues pertinent to VPNs.

There are several other standards and collections of best practices available that prescribe how to manage specific facets of the IT function within organisations (ISACA, 2007:6). To ensure that VPNs are properly governed, a framework that identifies VPN-related risks and addresses IT compliance with policies, regulations and laws is required. This research study documents an analysis to determine whether COBIT can be implemented to manage and/or mitigate VPN risks.



## **1.2 Purpose of the study**

The purpose of this study is to evaluate if COBIT is a suitable framework that can be used to assist in the governance of VPNs. It focuses on whether COBIT provides an adequate framework to ensure the identification of VPN-related risks and addresses IT compliance with policies and statutory regulations. The assignment also includes a synopsis of whether the principles of COBIT can be implemented to identify, mitigate and manage VPN risks. It furthermore encourages awareness of the importance of IT governance, indicates the necessity of properly understanding IT governance and highlights the importance of implementing adequate internal controls.

## **1.3 Scope**

The scope of the assignment does not include the intricacies of how VPNs operate, the technical issues surrounding the different types of networks, network topologies or the different technologies used in VPNs. However, to provide the reader with an understanding of the risks and issues pertinent to VPNs, the concept of VPNs, the different types of networks and the different technologies used within VPNs are briefly described. The VPN-related risks and issues documented in the individual matrices have been identified at the pre-implementation, implementation and post-implementation phases of VPNs. The mapping of the identified VPN risks and issues onto a suitable governance framework has been limited to the COBIT principles and control objectives. The decision to use the COBIT framework as the only preferred framework was made because it is an internationally recognised IT governance and control framework which does not only address specific aspects of IT (see Chapter 3).

## **1.4 Research methodology and subsequent chapters**

To determine whether the COBIT framework is an adequate framework to govern VPNs, an understanding of what VPNs as concept entails and how it could potentially affect the organisation's risks and goals was required. This was achieved through studying technical manuals and literature on VPNs as well as understanding the technology, architecture, requirements, advantages and disadvantages. An overview of VPNs, the concept, types, and technologies used in VPNs are briefly described in Chapter 2. This overview of VPN technology should provide the reader with an elemental understanding of how VPNs operate and enable the reader to comprehend the risks and issues pertinent to this form of technology.

To effectively govern VPNs, the concept of governance should be understood, the risk inherent to VPNs should be identified, and an adequate governance framework should be utilised. This was achieved through investigating the different types of governance frameworks available, and by visiting their respective websites and reviewing their respective literature. An analysis of the different frameworks was performed and a preferred framework was chosen. The reasons for selecting COBIT as the most suitable framework for the purpose of this study are documented in Chapter 3. This chapter also states the risks and the issues inherent to VPNs, and highlights the importance of good governance in VPNs through an overview of what good governance entails.

A thorough understanding of the COBIT framework, the IT processes defined in the four domains and the COBIT control objectives was required to ascertain whether this framework is adequate to address the risks and issues documented in Chapter 3. Therefore, a summary of the principles and objectives of the COBIT framework is documented in Chapter 4. This chapter explains the COBIT principles, COBIT information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability) and the organisation's IT resources (people, applications, technology, facilities and data) that it will impact on.

The VPN identified risks and issues documented in Chapter 3 were then allotted to the relevant COBIT processes and subsequently mapped to the pertinent COBIT control objective in the form of a matrix. Chapter 5 comprises the individual matrices divided into the four COBIT domains, namely plan and organise, acquire and implement, deliver and support, and monitor and evaluate. Finally, a summary of this study and the outcome of the mapping performed are presented in Chapter 6.

## Chapter 2

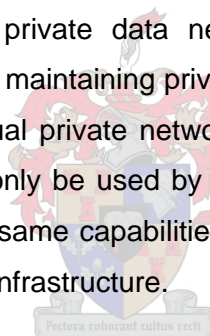
### 2 Virtual private networks (VPNs)

#### 2.1 An overview of VPNs

A brief synopsis on the VPN technology is described in this chapter mainly to provide the reader with an elemental understanding of how VPNs operate and to enable the reader to comprehend the risks and issues pertinent to this form of technology. Numerous security and data integrity risks could arise from the implementation and utilisation of a VPN. It is necessary for the organisation to identify these potential risks and ascertain the impact of these risks on the organisation's operations. When addressing these risks and considering the most appropriate solution set, IT management should consider the impact on the current IT governance processes as well as the overall business governance processes.

The Virtual Private Network Consortium (VPNC, 2004) defines a VPN as follows:

A virtual private network is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnel protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower costs by using the shared public infrastructure.



According to Fowler (1999:5):

There are several uses for a VPN. It can be an extended intranet, connecting geographically distant facilities into a cohesive network. It can also be an extranet, linking, for example, customers and suppliers for increased efficiency, such as electronic data exchange (EDI). [...] But there is a third service that a VPN can offer that no leased-line WAN can offer, and that is in providing remote access services. A VPN lets road warriors with their laptops connect into the home office through an Internet service provider, riding through the public Internet to log on to the office network, rather than running up long-distance charges by dialling up to a remote access server thousands of miles away.

## 2.2 The importance of VPNs

The need for businesses to provide a secure and speedy form of communication that is not only reliable but also cost effective is one of the main reasons for organisations to create their own VPNs. A VPN allows the company to extend its network capabilities beyond physical boundaries. It also affords the business the opportunity to form communication channels with its distant local branches, foreign branches, business partners, mobile workers and e-commerce customers (Tyson, 1998–2005).

According to Fowler (1999:154), the following factors should be considered when justifying the implementation of a VPN:

- The need for cost-effective remote access, as a result of either of the following:
  - A mobile workforce that will benefit from regular access to the company network, such as an organisation's sales force that needs regular updates of sales data and product information and is making frequent telephone calls to source the information.
  - Widely dispersed small facilities that need regular but not constant access to the company network, such as an overseas office that needs to send daily reports and do not need to be online frequently. The costs to dial in long distance are more expensive when compared to using a local ISP dial-up account.
  - Overseas offices that are incurring expensive long-distance costs for telephone calls that could be handled using IP phone technology or remote access through the Internet.
  
- The need for a organisational intranet connecting distributed services that will provide:
  - Administrative efficiencies such as transfers of accounting data and timekeeping records from remote offices.
  - Improved communication amongst geographically separated offices.
  - Mutual projects amongst dispersed employees.
  - Improved forms of communication like e-mail, message-based conferencing and video conferencing.
  - Efficiencies gained through the sharing of centralised and/or decentralised databases.
  
- The need for a organisational extranet that will provide enhanced communications with suppliers and customers and lead to:

- Enhanced business efficiency through electronic data interchange.
- Improved cooperation on design and engineering efforts.
- Better customer relations through enhanced communications.

## **2.3 VPN types and models**

The organisation's communication needs will impact and determine its VPN usage. Examples of VPN usage include site-to-site, remote access and extended enterprise extranet connectivity. There are several methods of implementing VPN architecture and topologies, including firewall-to-client, LAN-to-LAN, firewall-to-intranet/extranet and hardware/software VPNs (Ledesma, 2004:23).

The Virtual Private Network Consortium (VPNC, 2004) describes the following three important VPN technologies:

### **2.3.1 Trusted VPNs**

Prior to the Internet, most VPNs comprised networks of leased circuits whereby a communications provider (VPN provider) would provide a service of leasing the circuits to the party interested in establishing a VPN (VPN customer). This VPN model has one disadvantage when compared with other VPN models, in that the leased circuits would run through one or more communications switches and unauthorised parties wanting to observe the network traffic could compromise it. As the VPN customer would entrust the governance of the circuits' integrity and security to the VPN provider, this model is known as a trusted VPN. The privacy of the data travelling through these circuits is assured solely because only the specific VPN customer and no other VPN customer would be utilising a particular circuit. In this model, the VPN provider assures the properties of the path that the data will travel, but does not provide security against data interception, snooping or altering of the data.

### **2.3.2 Secure VPNs**

Because the Internet is a more cost-effective communication medium than the leased-line option, securing the data became a priority. Protocols were created to secure the data moving between networks. The data would be encrypted either at the start of the network or at the originating computer and then transported over the Internet to the organisation's network or the receiving computer. When the encrypted data reaches its final destination, it would then be decrypted. These networks are secure networks because the flow of the data between recipients is secured. Although unauthorised parties can view the intercepted

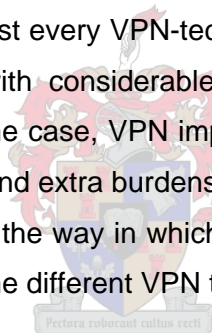
encrypted data, the data cannot be read. Because of the secure nature of these networks, the encrypted data flow cannot be diverted without the recipient being aware of it. The major advantage of a secure VPN is that data is secured but the path that the encrypted data travels is not assured.

### 2.3.3 Hybrid VPNs

The Internet forms the communication medium for this new type of trusted VPN. The transfer of the data is still not secured but this model provides the VPN customer with an easy means to create network segments for their wide-area networks. A secure VPN can form part of a trusted VPN, thereby creating the hybrid VPN. The VPN customer can secure parts of a hybrid VPN by using secure VPN equipment at their site, or the VPN provider can offer to secure the data.

## 2.4 Requirements for VPNs

According to Brown (1999:56), almost every VPN-technology article published mentions that VPN technology is synonymous with considerable cost savings and ease of use. He mentions that, while this might be the case, VPN implementation does come with additional costs, organisational requirements and extra burdens placed upon the organisation's IT staff. These additional burdens all impact the way in which VPNs are governed and it is therefore essential that the requirements for the different VPN technologies are understood.



The requirements for the different VPN technologies are as follows (VPNC, 2004):

#### *Secure VPN requirements*

- All traffic on the secure VPN must be encrypted and authenticated.
- All parties in the VPN must agree on the security properties of the VPN.
- No one outside the VPN can affect the security properties of the VPN.

#### *Trusted VPN requirements*

- No one other than the trusted VPN provider can affect the creation or modification of a path in the VPN.
- No one other than the trusted VPN provider can change data, inject data or delete data on a path in the VPN.
- The routing and addressing used in a trusted VPN must be established before the VPN is created.

### *Hybrid VPN requirements*

- The address boundaries of the secure VPN within the trusted VPN must be extremely clear.

## **2.5 VPNs explained**

Organisations should utilise secure, current and sophisticated authentication; cryptography; and encryption technologies at each end of the VPN tunnel to ensure that the VPN provides an effective means for electronic commerce, extranet applications and Internet transactions. To ensure a secure connection in a VPN, a process of tunnelling and encapsulation is applied, whereby the LAN address is concealed through hiding the existing network headers of packets sent through the network. Unauthorised users are prevented access through the establishing of user authentication by security gateways. The confidentiality of the data is maintained using encryption, whereby the users who exchange data would have to encrypt and decrypt the information. Data verification is also performed to detect any signs of data tampering or manipulation. (Brown, 1999:46)

### **2.5.1 Tunnelling and encapsulation**

Fowler (1999:19) makes the following distinction between tunnelling and encapsulation:

Probably the simplest way to differentiate between them is that tunnelling is applied to the whole process of moving the message through the Internet for a VPN, while encapsulation refers to what is done to each individual packet that makes up the message. In tunnelling, each packet, including any existing header it has acquired from the Local Area Network (LAN) where it originated, is encapsulated – wrapped up, hidden – by a new envelope or capsule that carries the addresses of the source and destination VPN servers.

### **2.5.2 Encryption**

The technique of scrambling and unscrambling information is called encryption. The unscrambled information is called clear-text, and the scrambled information is called cipher-text. A VPN gateway is located at either end of the VPN tunnel in either hardware or software form. The VPN gateway at the sending location encrypts the information into cipher-text before sending the encrypted information through the tunnel over the Internet. At the receiving location, the VPN gateway would then decrypt the information back into clear-text. Data confidentiality is maintained by the fact that the data exchanged would have to be

encrypted and decrypted by using a particular key. In most VPNs, the encryption and decryption are automatically handled by the VPN hardware or software. The two types of encryption are symmetric or secret-key encryption and asymmetric or public-key encryption. Combinations of the use of public and private keys are utilised to encrypt and decrypt the data. (ADTRAN, 2001)

### **2.5.3 Key management**

According to Fowler (1999:91),

... one of the greatest challenges a VPN administrator faces is making sure that the right person and only the right person is getting the right keys. To do that, the key management authority, whatever and wherever it may be, must have some way of being sure that the person getting the key is who he claims to be. It is one of the most difficult problems in VPNs or any other kind of network.

Key management therefore entails ensuring a secure method of generating, registering and allocating private and public keys to the authenticated users. It also includes activating or deactivating, replacing, updating and managing these encryption keys.

### **2.5.4 User authentication and data authentication**

“The last bit of housekeeping involved in VPN transmission is authentication. At this step, recipients of data can determine if the sender is really who he says he is (User/System Authentication) and if the data was redirected or corrupted en route (Data Authentication).” (ADTRAN, 2001). The process whereby only the right people are given access to the system and are then subsequently able to decipher the encrypted data is called user authentication. This process also involves ensuring that the users receive the necessary keys required to decode the data. Data authentication/verification is performed to ensure that the data received was not corrupted, manipulated or tampered with during its transit.

To reiterate, in order to determine whether the COBIT framework is an adequate framework to utilise in the governance of VPNs and assist in the identification of VPN-related risks, it is necessary to acknowledge what risks and issues are associated to this technology and to understand what governance entails.



## Chapter 3

### 3 VPN governance

#### 3.1 Governance explained

The Information Systems Audit and Control Foundation (quoted by IFAC, 2004) describes enterprise governance as “the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly”.

The alignment of the organisation’s business and IT is one of the significant components in IT governance. Proper alignment of these objectives would lead to the achievement of business goals. The organisation can accomplish this by recognising that IT governance is a subset of enterprise governance and by implementing and utilising an IT governance framework with best practices. (De Haes & Van Grembergen, 2004:32)

In the COBIT framework (ISACA, 2000:9), IT governance is defined as follows:

IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

Essentially, IT governance is concerned about IT’s delivery of value to the organisation and mitigation of IT risks. The first concern is motivated by the need to strategically align IT with the organisation’s business. The underlying factor of establishing and inculcating accountability into the enterprise drives the second. Both elements should to be supported by adequate resources and measured to ensure that the required outcome is achieved. (IT Governance Institute, 2003:19)

### **3.2 The importance of governance and internal control**

Johnson (2005:17) indicates that, due to the current emphasis on the US Sarbanes-Oxley Act of 2002 and similar global regulatory requirements pertaining to enterprise governance and control, it is important that internal control and IT governance be understood, positioned and implemented well in the context of overall governance.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO, 2006) states that “[i]nternal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting and compliance with the applicable laws and regulations”. An IT governance framework aids management and the organisation’s board of directors to understand the strategic importance of IT and IT related issues. It also assists the organisation by providing assurance that the business can sustain its operations and implement the necessary strategies required to expand its activities. Furthermore, it provides assurance that IT expectations are achieved and IT risks are addressed. (IT Governance Institute, 2003:37)

Kordel (2004:40) states that, “[w]hen properly implemented, IT governance is an organisational structure and set of processes that manage and control the enterprise’s IT activities to achieve the enterprise’s goals by adding value while balancing risk and return over IT.” Parkes (2004:17) stresses that when referring to IT governance one should not only consider the IT department or the physical attributes and manifestations of IT but look at how the entire activity using IT is controlled. The business knowledge and information required for the activity’s successful operation should also be considered.

It is therefore necessary to ensure that IT governance is properly understood and that overall governance and proper internal controls are implemented. It is also important that IT management has a suitable approach, guidelines and the proper tools to ensure that IT governance is implemented appropriately to be in line with best practices and the organisation’s needs.

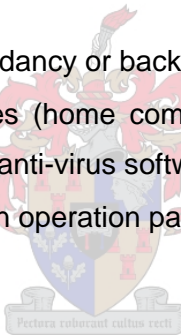
### 3.3 Risks inherent to VPNs

The Information Systems Audit and Control Association (ISACA, 2004) categorises the risks associated with VPNs as related to security, third parties, business, implementation or operations.

The VPN risks stated in its auditing guideline are as follows:

- *Security and legal risks*
  - Inadequate assessment of security and legal risks arising out of using VPNs
  - Insufficient security programs to mitigate risks to information assets arising out of VPNs
  - Inadequate protection of data while they are at the point before entering the VPN, or once they arrive at the point on leaving the VPN
  - Failure to secure information while unencrypted over a given network path (internal networks before encryption device or external networks after decryption device)
  - Lack of implementation that could result in confidentiality, integrity, non-repudiation and/or availability issues
- *Third-party risks*
  - Choice of an inappropriate provider
  - Inadequate relationship management
  - Inadequacies in service level agreements (SLAs) and metrics
  - Inappropriate governance and management process
  - Inadequate measuring and monitoring of SLAs and metrics
  - Inadequate backup and/or redundancy strategy
  - Insufficient benchmarking of the relationship and services
  - Abuse of access to data on the VPN
- *Business risks*
  - Inadequate alignment to business strategy
  - Inadequate cost savings
  - Failure to achieve security requirements
  - Insufficient ease of use
  - Failure to address scope and span of user needs
  - Loss or degradation of service in other areas of organisation or process
- *Implementation risks*
  - Inadequate attention to and investment in up-front design

- Inappropriate selection of the VPN model for the organisation
  - Inadequate use of third parties where appropriate
  - Insufficient attention to security in design
  - Inappropriate recovery processes
  - Failure to design service level expectations and measurements
  - Inappropriate integration strategy
  - Ineffective change, project or implementation management processes
  - VPN client risk (same interface accepts Internet and VPN traffic)
- *Operating risks*
    - Inadequate resources to operate effectively
    - Lack of reliability
    - Impairment of quality of service
    - Lack of interoperability
    - Failure to encapsulate
    - Inadequate capacity
    - Failure to provide redundancy or backup
    - Use of personal devices (home computing) for business purposes (lack of security configurations, anti-virus software, personal firewalls)
    - Lack of confidentiality on operation parameters or data



### 3.4 VPN control objectives

According to the Institute of Internal Auditors (IIA, s.a.), possible control objectives for VPNs could include:

- Protection from unauthorised access
- Protection from attacks such as denial of service or unauthorised use of service
- Reliability – VPN is always operating
- Ease and consistency of implementation
- Minimum impact on network users – the VPN is transparent to end users
- Minimum network management impact
- Secure transport for sensitive content
- Centralised management of VPN
- Flexibility – open system interoperability
- Open standards
- Provide for recovery and accountability – audit trails.

## Chapter 4

### 4 COBIT

The motivation for selecting the COBIT framework as the preferred framework for this research study is presented in this chapter. A brief summary of the principles of the COBIT framework is documented in the latter part of this chapter in order to provide the reader with an understanding of the COBIT domains and control objectives mapped in VPN matrices discussed in Chapter 5.

The information included in this chapter has been extracted and in certain instances directly paraphrased from ISACA (2005).

#### 4.1 The reason for selecting COBIT

According to ISACA (2005:5),

... IT governance integrates and institutionalises good practices to ensure that the enterprise's IT supports the business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits in with and supports the Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control–Integrated Framework, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

COSO's Internal Control–Integrated Framework has become the most commonly used framework by companies complying with the US Sarbanes-Oxley Act. However, COSO does not provide a great deal of guidance to assist in the design and implementation of IT controls (IT Governance Institute, 2006:12). Coe (2005:3) states that the COSO framework defines internal control, describes the components and provides criteria against which users can evaluate control systems. However, he asserts that some companies may require an additional framework to assist in the evaluation of IT controls, as COSO does not provide specific criteria for IT controls. According to Heschl (2004:38), "[t]he primary goal of COSO is the improvement of the way of controlling enterprises, whereas COBIT's primary goal is to derive IT control objectives for day to day use." For these specific reasons, the COSO framework was not regarded as a suitable framework for the purpose of this research study.

The COBIT framework was considered a more adequate framework because a broad base of more than 40 international detailed IT standards, frameworks, guidelines and best practices were used during the development and subsequent updating of COBIT. This ensured the completeness of COBIT in addressing all areas of IT governance and control. (ISACA, 2005:179)

Guldentops (2003:3) affirms that COBIT is a global standard that includes guidelines offering management and auditors a way to bridge the gap among business risks, control needs and technical issues. He states that COBIT is accepted as international IT governance best practice and mentions that the framework is 100 percent COSO-compliant and easy to understand and apply.

Because COBIT is focused on what is required to achieve adequate management and control of IT, it is positioned at a high level. The more detailed IT standards and best practices are at a lower level of detail in describing how to manage and control specific aspects of IT. COBIT acts as an integrator of these difference guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements. (ISACA, 2005:179)

So the decision to use the COBIT framework for this study was based on the facts that COBIT is an internationally recognised IT governance and control framework, and that it does not only address specific aspects of IT.

Furthermore, COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused on control and less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things go wrong (ISACA, 2005:5).

## **4.2 The COBIT framework**

COBIT is an IT governance tool that assists with the understanding and managing of the risks and benefits associated with information and related IT. As mentioned in the executive overview of COBIT (ISACA, 2005:8), "COBIT is a framework and supporting toolset that

allows managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT throughout enterprises”.

COBIT thus 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. (ISACA, 2005:6)

“The COBIT framework is based on the following principle: to provide information that the enterprise requires to achieve its objectives, the enterprise needs to manage and control IT resources using a structured set of processes to deliver the require information services” (ISACA, 2005:11).

According to the Board Briefing on IT Governance (IT Governance Institute, 2003:62), COBIT addresses the fiduciary, quality and security needs of organisations and provides seven information criteria that can be used to define business IT requirements – effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

#### **4.2.1 Process-oriented**

COBIT defines IT activities in a generic process model with four domains. These domains are:

- Plan and organise
- Acquire and implement
- Deliver and support
- Monitor and evaluate. (ISACA, 2005:13)

The COBIT framework provides the following descriptions for the four domains identified for high-level classification (ISACA, 2005:14):

<b>1. Plan and organise</b>	This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.
<b>2. Acquire and implement</b>	To realise IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.
<b>3. Deliver and support</b>	This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities.
<b>4. Monitor and evaluate</b>	This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance.

#### 4.2.2 COBIT IT processes defined within the four domains

In order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. The COBIT IT processes defined within the four domains are as follows:

Plan and organise:

- PO1 – Define a strategic IT plan
- 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. (ISACA, 2005:29-72)

Acquire and implement:

- 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. (ISACA, 2005:73-102)

Deliver and support:

- DS1 – Define and manage service levels
- DS2 – Manage third-party services
- DS3 – Manage performance and capacity
- DS4 – Ensure continuous service
- DS5 – Ensure systems 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. (ISACA, 2005:103-154)

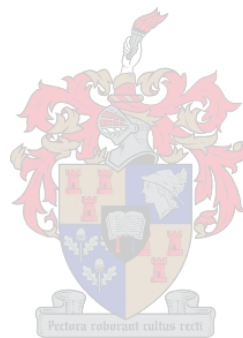
Monitor and evaluate:

- ME1 – Monitor and evaluate the IT process
- ME2 – Monitor and evaluate internal control
- ME3 – Ensure regulatory compliance
- ME4 – Provide IT governance. (ISACA, 2005:155-170)

The Board Briefing on IT Governance (IT Governance Institute, 2003:62) states that for each of these 34 IT processes, a high-level control objective is defined:

- Identifying which information criteria are most important in that IT process
- Listing which resources will usually be leveraged
- Providing considerations on what is important for controlling that IT process.

As mentioned in Chapter 1, the abovementioned domains and control objectives have been reviewed and the relevant control objectives have been documented in the VPN matrices in Chapter 5. The VPN risks and issues that have been highlighted in Chapter 3 are mapped to the control objectives in each of the domains.



## Chapter 5

### 5 VPN COBIT MATRIX

#### 5.1 Methodology

The methodology applied in preparation for and during the documentation of this research study is summarised as follows:

- Understanding the concept of governance and what governance entails
- Recognising the importance of good governance in VPNs through researching what governance encapsulates
- Investigating the different types of governance frameworks available by visiting their respective websites and reviewing the literature
- Analysing the different frameworks and selecting the most suitable framework for the purpose of this study
- Obtaining an understanding of what the concept of VPNs entails and how it could potentially effect the organisation's risks and goals
- Studying technical manuals and literature on VPNs – the technology, architecture, requirements, advantages and disadvantages
- Identifying the risks and issues inherent to VPNs
- Gaining a thorough understanding of the COBIT framework by studying the IT processes defined in the four domains
- Allocating the identified risks or issues to the relevant COBIT processes
- Mapping the identified risk or issue onto the pertinent COBIT control objective.

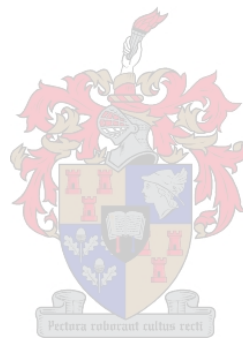
#### 5.2 Matrices

The matrices documented on the subsequent pages have been categorised according to the four COBIT framework domains mentioned in Chapter 4. The possible risks or weaknesses documented in the matrices have been adapted from the risks mentioned in Chapter 3. The individual matrices also include columns for the information requirements defined in the COBIT framework, namely effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability (ISACA, 2005:11).

These information requirements columns have been populated with one of the following:

<b>P</b>	Primary: The degree to which the control objective would affect the information requirement.
<b>S</b>	Secondary: The degree to which the control objective would affect the information requirement.
<b>Blank</b> ( )	Columns that have not been populated may be applicable; however, the degree of relevance may not be of a primary or secondary nature.

The affected IT resources defined in the COBIT framework (ISACA, 2005:12) have also been documented and populated in the individual matrices.



### 5.2.1 Plan and organise

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
-----------------	-------------	-----------------------------------	-------------------------

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
---------------	------------	-----------------	-----------	--------------	------------	-------------

Applications	Information	Infrastructure	People
--------------	-------------	----------------	--------

#### PO1 – Define a strategic IT plan

1.1	Existing or new	<ul style="list-style-type: none"> <li>The benefits of utilising a VPN are not considered when defining the organisation's strategic and tactical plans.</li> <li>IT management's intentions regarding the use of or change to an existing VPN is not aligned with the organisation's overall strategic plan.</li> </ul>	Senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation's long- and short-range plans.
1.6	Existing or new	<ul style="list-style-type: none"> <li>The organisation's management does not communicate the intention to implement a VPN or effect changes to an existing VPN to the relevant parties.</li> </ul>	Management should ensure that IT's long- and short-range plans are communicated to business process owners and other relevant parties across the organisation.
1.7	Existing	<ul style="list-style-type: none"> <li>Inadequate communication channels are made available to the business process owners and users of the VPN to inform IT management of the possible changes to be made concerning the strategy and tactical plans.</li> </ul>	Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans.

P	S					
P	S					
P	S					

X	X	X	X
X	X	X	X
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
1.8	Existing or new	<ul style="list-style-type: none"> <li>The advantages and disadvantages of implementing a VPN are not properly considered by the organisation.</li> <li>Management does not properly assess an existing VPN when considering upgrading or changing the type of VPN.</li> </ul>	Prior to developing or changing the strategic or long-range IT plan, IT management should assess the existing information systems in terms of the degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses in order to determine the degree to which the existing systems support the organisation's business requirements.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	S					

Applications	Information	Infrastructure	People
X	X	X	X

**PO3 – Determine technological direction**

3.1	Existing	<ul style="list-style-type: none"> <li>Management does not properly assess an existing VPN when considering upgrading or changing the type of VPN.</li> <li>The current VPN technology utilised by the organisation becomes obsolete.</li> <li>The existing VPN architecture and configuration are not the most effective design to be utilised.</li> </ul>	Analyse existing and emerging technologies and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also, identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.
-----	----------	---	---

P	P					
---	---	--	--	--	--	--

X		X	
---	--	---	--

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
3.2	Existing or new	<ul style="list-style-type: none"> <li>The detail documented in the technological infrastructure plan in respect of VPNs is not aligned with the IT strategic and tactical plans.</li> </ul>	Create and maintain a technological infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan is based on the technological direction and includes contingency arrangements and direction for acquisition of technology resources. It considers changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.
3.3	Existing or new	<ul style="list-style-type: none"> <li>Management does not consider changes to trends and regulatory conditions in VPN technology, VPN architecture, configuration/topology and VPN usage when developing and/or maintaining a VPN.</li> </ul>	Establish a process to monitor trends in the business sector/industry, technology, infrastructure, and legal and regulatory environment. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan.
3.4	Existing	<ul style="list-style-type: none"> <li>Management does not consider changes to trends and technology standards in VPNs when developing and/or maintaining a VPN.</li> </ul>	To provide consistent, effective and secure enterprise-wide technological solutions, establish a technology forum to provide technology guidelines, advice on infrastructure

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
P	P						X		X	
P	P						X		X	
P	P						X		X	

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum directs technology standards and practices based on their business relevance, risks and compliance with external requirements.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability

Applications	Information	Infrastructure	People

**PO5 – Manage the IT investment**

5.1	Existing or new	<ul style="list-style-type: none"> <li>Costs incurred to implement a VPN or maintain an existing VPN are not included in the IT budget.</li> <li>The VPN cost detail reflected in the IT budget is not aligned with the overall organisational plans.</li> </ul>	Establish a financial framework for IT that drives budgeting and cost/benefit analysis, based on investment, service and asset portfolios. Maintain the portfolios of IT-enabled investment programmes, IT services and IT assets, which form the basis for the current IT budget. Provide input to business cases for new investments, taking into account current IT asset and service portfolios. New investments and maintenance to service and asset portfolios will influence the future IT budget. Communicate the cost and benefit aspects of these
-----	-----------------	--	---

P	P					S
---	---	--	--	--	--	---

X		X	X
---	--	---	---



COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
			portfolios to the budget prioritisation, cost management and benefit management processes.											
5.5	Existing or new	<ul style="list-style-type: none"> <li>Loss of possible cost savings due to inadequate management attention to the initial VPN design and investment.</li> <li>Inappropriate VPN model selected for the organisation.</li> </ul>	Implement a benefit monitoring process. IT's expected contribution to business results, either as a component of IT-enabled investment programmes or as part of regular operational support, should be identified, agreed to, monitored and reported on. Reports should be reviewed and, where there are opportunities to improve IT's contribution, appropriate actions should be defined and taken. Where changes in IT's contribution or changes to other related projects impact the programme, programme business case should be updated.	P	P					S	X		X	X

**PO9 – Assess and manage IT risks**

9.3	Existing or new	<ul style="list-style-type: none"> <li>The risks arising from the relevant parties associated with the VPN are not considered when performing the risk assessment.</li> </ul>	Identify any event (threat and vulnerability) with a potential impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and	S	S	P	P	P	S	S	X	X	X	X
-----	-----------------	---	---	---	---	---	---	---	---	---	---	---	---	---

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			operational aspects. Determine the nature of the impact – positive, negative or both – and maintain this information.
9.4	Existing or new	<ul style="list-style-type: none"> <li>Management performs an inadequate assessment on the risks arising from utilising a VPN, i.e. not all elements/risk aspects are considered when evaluating the VPN's risks.</li> </ul>	Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.
9.6	Existing or new	<ul style="list-style-type: none"> <li>Management has not initiated a process to prepare an action plan to address the VPN risks identified during the risk assessment phase and to design and implement controls to mitigate these risks.</li> </ul>	Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Seek approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report any deviations to senior management.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
S	S	P	P	P	S	S
S	S	P	P	P	S	S

Applications	Information	Infrastructure	People
X	X	X	X
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
-----------------	-------------	-----------------------------------	-------------------------

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
---------------	------------	-----------------	-----------	--------------	------------	-------------

Applications	Information	Infrastructure	People
--------------	-------------	----------------	--------

**PO10 – Manage projects**

10.7	Existing or new	<ul style="list-style-type: none"> <li>The organisation's management has inadequate project management structures and project monitoring mechanisms in place to ensure that the VPN project is completed within the standards and required budgets.</li> <li>An adequate training plan is not prepared and implemented for the VPN development, implementation and modification phases.</li> </ul>	Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and project control throughout the life of the project. The activities and interdependencies of multiple projects within the project should be understood and documented. The project plan, and changes to it, should be approved in line with the programme and project governance framework.
10.10	Existing or new	<ul style="list-style-type: none"> <li>The organisation's management has inadequate project management structures and project monitoring mechanisms in place to ensure that the project is completed within the standards and required budgets.</li> </ul>	Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.
10.13	Existing or new	<ul style="list-style-type: none"> <li>Testing is not performed and documented during the VPN development, implementation and modification phases.</li> </ul>	Measure project performance against key project criteria (e.g. scope, schedule, quality, cost and risk); identify any deviations from the

P	P					
P	P					
P	P					

X		X	X
X		X	X
X		X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			plan; assess their impact on the project and overall programme; report results to key stakeholders; recommend, implement and monitor remedial action when required, in line with the programme and project governance framework.
10.14	Existing or new	<ul style="list-style-type: none"> <li>Management does not perform a post-project review to ascertain the outcome of the development, implementation and/or modification of the VPN.</li> </ul>	Require that at the end of each project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	P					

Applications	Information	Infrastructure	People
X		X	X

## 5.2.2 Acquire and implement

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
<b>AI3 – Acquire and maintain technology infrastructure</b>														
3.1	Existing or new	<ul style="list-style-type: none"> <li>The proposed VPN design and technology requirements selected is inappropriate and will not meet the organisation's needs.</li> <li>Insufficient review and maintenance of the VPN model, architecture and configuration.</li> </ul>	Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction. The plan should consider future flexibility for capacity additions, transition costs, technical risks and the lifetime of the investment for technology upgrades. Assess the complexity costs and the commercial viability of the vendor and product when adding new technical capability.	S	P		S	S					X	
3.4	Existing or new	<ul style="list-style-type: none"> <li>IT management does not consider all the potential problems that could occur when integrating the VPN with the applications.</li> </ul>	Establish development and test environments to support effective and efficient feasibility and integration testing of applications and infrastructure in the early stages of the acquisition and development	S	P		S	S					X	

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
			process. Consider functionality, hardware and software configuration, integration and performance testing, migration between environments, version control, test data and tools, and security.											

#### AI4 – Enable operation and use

4.1	Existing or new	<ul style="list-style-type: none"> <li>Insufficient information is documented in user procedure and/or operations manuals, resulting in inadequate manuals being prepared by IT management.</li> <li>The user procedure and/or operations manuals are not updated for changes resulting from VPN development, implementation or modification.</li> </ul>	Develop a plan to identify and document all technical aspects, operational capability and requires service levels, so all stakeholders can take timely responsibility for the production of management, user and operational procedures, as a result of the introduction or upgrade of automated systems or infrastructure.	P	P		S	S	S	S	X		X	X
4.2	Existing	<ul style="list-style-type: none"> <li>Modifications are made to the VPN and users do not have the necessary skill or competency to use the VPN since implementation.</li> <li>The training materials are not regularly updated for changes resulting from VPN development, implementation or modification.</li> </ul>	Transfer knowledge to business management to allow them to take ownership of the system and data and exercise responsibility for service delivery and quality, internal control, and application administration processes. The knowledge transfer should include	P	P		S	S	S	S	X		X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
			access approval, privilege management, segregation of duties, automated business controls, backup/recovery, physical security, and source document archival.											

**AI6 – Manage changes**

6.1	Existing or new	<ul style="list-style-type: none"> <li>The change, project or implementation management process performed by the organisation is ineffective.</li> </ul>	Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications procedures, processes, system and service parameters, and underlying platforms.	P	P		P	P		S	X	X	X	X
6.5	Existing or new	<ul style="list-style-type: none"> <li>Management does not update relevant documentation such as user, operations and training manuals with the necessary changes.</li> </ul>	Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.	P	P		P	P		S	X	X	X	X

### 5.2.3 Deliver and support

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
-----------------	-------------	-----------------------------------	-------------------------

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
---------------	------------	-----------------	-----------	--------------	------------	-------------

Applications	Information	Infrastructure	People
--------------	-------------	----------------	--------

#### DS1 – Define and manage service levels

1.1	Existing or new	<ul style="list-style-type: none"> <li>The organisation's management fails to design appropriate service level expectations and measurements.</li> <li>Inadequate service level agreements between the organisation and external and/or internal service providers are drafted.</li> </ul>	<p>Define a framework that provides a formalised service level management process between the customer and service provider. The framework maintains continuous alignment with business requirements and priorities and facilitates common understanding between the customer and provider. The framework includes processes for creating service requirements, service definitions, service level agreements, operating level agreements and funding sources. These attributes are organised in a service catalogue. The framework defines the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.</p>
-----	-----------------	--	---

P	P	S	S	S	S	S
---	---	---	---	---	---	---

X	X	X	X
---	---	---	---



COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
1.5	Existing or new	<ul style="list-style-type: none"> <li>The services provided by internal and/or external VPN service providers are inadequately monitored and measured.</li> </ul>	Continuously monitor specified service level performance criteria. Reports on achievement of service levels are provided in a format that is meaningful to the stakeholders. The monitoring statistics are analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.
1.6	Existing or new	<ul style="list-style-type: none"> <li>The VPN service level agreements and quality of service assessments are not reviewed and addressed frequently for timely actions.</li> </ul>	Regularly review service level agreements and underpinning contracts with internal and external service providers to ensure that they are effective and up to date, and that changes in requirements have been accounted for.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	P	S	S	S	S	S
P	P	S	S	S	S	S

Applications	Information	Infrastructure	People
X	X	X	X
X	X	X	X

**DS2 – Manage third-party services**

2.1	Existing or new	<ul style="list-style-type: none"> <li>Services provided by internal and/or external VPN service providers are not properly identified and documented.</li> <li>All technical and organisational interfaces with third parties are not properly documented.</li> <li>The current VPN service providers</li> </ul>	Identify all supplier services and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables and
-----	-----------------	---	--

P	P	S	S	S	S	S
---	---	---	---	---	---	---

X	X	X	X
---	---	---	---

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
		are not supplying the most appropriate services.	credentials of representatives of these suppliers.
2.2	Existing or new	<ul style="list-style-type: none"> <li>Management fails to design appropriate internal and/or external VPN service level expectations, agreements, and appropriate measurements prior to contracting their services.</li> </ul>	Formalise the supplier relationship management process for each supplier. The relationship owners must liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g. through service level agreements).
2.3	Existing or new	<ul style="list-style-type: none"> <li>Management selects an inappropriate third-party service provider, i.e. a service provider that is unable to provide a proper VPN service or a provider whose service does not meet the organisation's quality standards.</li> <li>Management selects a third-party service provider that has an inadequate backup or redundancy strategy.</li> <li>Third parties who have access to the VPN have not signed a security and confidentiality agreement.</li> <li>Third parties who have access to the VPN are not conforming to the agreed security and confidentiality</li> </ul>	Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements, escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	P	S	S	S	S	S
P	P	S	S	S	S	S

Applications	Information	Infrastructure	People
X	X	X	X
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
		agreements.	
2.4	Existing or new	<ul style="list-style-type: none"> <li>Management fails to adequately measure and monitor the service level agreement between the organisation and third-party service provider.</li> </ul>	Establish a process to monitor service delivery to ensure the supplier is meeting current business requirements and is continuing to adhere to the contract agreements and service level agreements, and that performance is competitive with alternative suppliers and market conditions.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	P	S	S	S	S	S

Applications	Information	Infrastructure	People
X	X	X	X

**DS4 – Ensure continuous service**

4.1	Existing or new	<ul style="list-style-type: none"> <li>A VPN continuity plan detailing the procedures to be followed in the event of a disruption to the VPN is not adequately documented.</li> <li>The staff responsibilities and roles are not clearly defined and documented in the continuity plan.</li> </ul>	Develop a framework for IT continuity to support enterprise-wide business continuity managements with a consistent process. The objective framework is to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and
-----	-----------------	--	--

P	S			P		
---	---	--	--	---	--	--

X	X	X	X
---	---	---	---

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			their customers, and the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should address items such as the identification of critical resources, the monitoring and reporting of the availability of critical resources, alternative processing and the principles of backup and recovery.
4.2	Existing or new	<ul style="list-style-type: none"> <li>▪ The VPN continuity plan is not aligned with the overall business continuity plans or the IT strategy and tactical plans.</li> <li>▪ The most feasible continuity procedures and the impact on the hardware, software, personnel and facilities requirements are not considered.</li> </ul>	Develop IT continuity plans based on the framework, designed to reduce the impact of a major disruption on key business functions and processes. The plans should address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes and the testing approach.
4.4	Existing or new	<ul style="list-style-type: none"> <li>▪ The VPN continuity plan is not amended for changes made to the VPN due to development, implementation or modification.</li> </ul>	Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
P	S			P		
P	S			P		

Applications	Information	Infrastructure	People
X	X	X	X
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			continually reflects actual business requirements. It is essential that changes in procedures and responsibilities be communicated clearly and in a timely manner.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability

Applications	Information	Infrastructure	People

**DS5 – Ensure system security**

5.1	Existing or new	<ul style="list-style-type: none"> <li>Inadequate IT assessment of the security risks arising out of the VPN usage.</li> <li>Management of security risks is not in accordance with the organisation's business requirements.</li> <li>Management does not formulate, implement and subsequently monitor an IT security plan.</li> </ul>	Manage IT security at the highest appropriate organisational level, so that the management of security actions is in line with business requirements.
5.3	Existing or new	<ul style="list-style-type: none"> <li>The security programs and mechanisms designed and implemented by the organisation to prevent unauthorised access to the VPN are inadequate.</li> </ul>	All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights

		P	P	S	S	S
		P	P	S	S	S

X	X	X	X
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			are requested by user management, approved by the system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.
5.4	Existing or new	<ul style="list-style-type: none"> <li>▪ A formal approval procedure for amendments, deletions and additions of users and access privileges are not properly documented and followed.</li> <li>▪ Third parties abuse the fact that they have access to data on the VPN.</li> </ul>	Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply to all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
		P	P	S	S	S

Applications	Information	Infrastructure	People
X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			arranged for all types of users. Perform regular management review of all accounts and related privileges.
5.5	Existing or new	<ul style="list-style-type: none"> <li>▪ Inadequate recording of security activity resulting in a lack of timely investigations and follow-up of possible violations.</li> <li>▪ Access rights and violations are not regularly reviewed and followed up by management.</li> </ul>	Ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure that the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.
5.8	Existing or new	<ul style="list-style-type: none"> <li>▪ Security schemes and encryption technologies are not working as designed.</li> <li>▪ Encryption keys are not adequately managed and become compromised.</li> </ul>	Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
		P	P	S	S	S	X	X	X	X
		P	P	S	S	S	X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
						P	P	S	S	S	X	X	X	X
5.10	Existing or new	<ul style="list-style-type: none"> <li>Inappropriate security tools and processes are implemented to detect intruders and viruses and to secure the information.</li> </ul>	Ensure that security techniques and related management procedures (e.g. firewalls, security appliances, network segmentation and intrusion detection) are used to authorise access and control information flow from network to network.			P	P	S	S	S	X	X	X	X
5.11	Existing or new	<ul style="list-style-type: none"> <li>IT management fails to secure information while unencrypted over a given network path.</li> <li>Inadequate security architecture and encryption technologies used by IT management.</li> <li>Encryption technologies are not working as intended.</li> <li>Sensitive information is not encrypted when sent over a VPN.</li> </ul>	Ensure sensitive transaction data are exchanged only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.			P	P	S	S	S	X	X	X	X
<b>DS12 – Manage the physical environment</b>														
12.1	Existing or new	<ul style="list-style-type: none"> <li>Physical security and access control measures are not properly considered, adequately documented and communicated to all users.</li> </ul>	Define and implement physical security measures in line with business requirements. Measures should include, but are not limited to, the layout of the security parameter, security zones, locations of critical equipment, and shipping				P	P						X



COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
			and receiving areas – in particular, keeping a low profile about the presence of critical IT operations. Responsibilities for monitoring and procedures for reporting and resolving physical security incidents need to be established.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability

Applications	Information	Infrastructure	People



### 5.2.4 Monitor and evaluate

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
<b>ME1 – Monitor and evaluate IT performance</b>														
1.1	Existing or new	<ul style="list-style-type: none"> <li>The organisation's management has inadequate mechanisms in place to monitor the performance of services provided by the IT function.</li> <li>Inadequate performance indicators are used by management to assess IT services.</li> </ul>	Ensure that management establishes a general monitoring framework and approach to define the scope, methodology and process to be followed for monitoring IT's contribution to the results of the enterprise's portfolio management and programme management processes and those processes that are specific to delivery of IT capability and services. The framework should integrate with the corporate performance management system.	P	P	S	S	S	S	S	X	X	X	X
<b>ME2 – Monitor and evaluate internal control</b>														
2.1	Existing or new	<ul style="list-style-type: none"> <li>Management does not regularly assess services provided by the IT function.</li> </ul>	Continuously monitor the IT control environment and control framework. Assessment using industry best practices and benchmarking should be used to improve the IT control environment and control framework.	P	P	S	S	S	S	S	X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective
2.5	Existing or new	<ul style="list-style-type: none"> <li>Management has not implemented an action plan to address and resolve potential issues of non-compliance and breaks in internal control in a timely manner.</li> </ul>	Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. Such reviews may be conducted by the corporate compliance function or, at management's request, by internal audit or commissioned to external auditors and consultants or certified bodies. Qualifications of individuals performing the audit, e.g. Certified Information Systems Auditor (CISA) certification, must be ensured.
2.6	Existing or new	<ul style="list-style-type: none"> <li>The contracts between the organisation and third parties are inadequate, leading to inadequate security standards, possible communication breaches and inferior communication standards.</li> </ul>	Assess the status of each external provider's internal controls. Confirm that external service providers comply with the legal and regulatory requirements and contractual obligations. This can be provided by a third-party audit or obtained from a review by management's internal audit functions and the results of the audits.

Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
P	P	S	S	S	S	S	X	X	X	X
P	P	S	S	S	S	S	X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
<b>ME3 – Ensure regulatory compliance</b>														
3.1	Existing or new	<ul style="list-style-type: none"> <li>The contracts between the organisation and third parties are inadequate, leading to inadequate security standards, possible communication breaches and inferior communication standards.</li> </ul>	Define and implement a process to ensure timely identification of local and international legal, contractual, policy and regulatory requirements related to information, information service delivery – including third-party services – and the IT organisation, processes and infrastructure. Consider laws and regulations for electronic commerce, data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property and copyright, and health and safety.						P	S	X	X	X	X
3.3	New and existing	<ul style="list-style-type: none"> <li>Management does not have procedures in place to identify non-compliance to statutory IT governance and other relevant external requirements.</li> </ul>	Efficiently evaluate compliance with IT policies, standards and procedures, including legal and regulatory requirements, based on business and IT management's governance oversight and operation of internal control.						P	S	X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
<b>ME4 – Provide IT governance</b>														
4.1	Existing or new	<ul style="list-style-type: none"> <li>Management does not implement a proper governance tool to address the organisation's VPN-related risks and achieve the organisation's goals.</li> </ul>	Work with the board to define and establish an IT governance framework including leadership, processes, roles and responsibilities, information requirements and organisational structures to ensure that the enterprise's IT-enabled investment programmes are aligned with and deliver on the enterprise's strategies and objectives.	P	P	S	S	S	S	S	X	X	X	X
4.2	Existing or new	<ul style="list-style-type: none"> <li>Insufficient awareness of VPN technology, the benefits of VPNs and the impact on business strategy are communicated to management.</li> </ul>	Enable board and executive understanding of strategic IT issues such as the role of IT, technology insights and capabilities. Make sure there is a shared understanding between the business and IT of the potential contribution of IT to the business strategy.	P	P	S	S	S	S	S	X	X	X	X
4.4	Existing or new	<ul style="list-style-type: none"> <li>Management does not have procedures in place to identify and measure non-compliance to statutory IT governance and other relevant external requirements.</li> </ul>	Work with the board to define the enterprise's appetite for IT risk. Communicate IT risk appetite into the enterprise and agree on an IT risk management plan. Embed risk	P	P	S	S	S	S	S	X	X	X	X

COBIT reference	Type of VPN	Possible risk/weakness identified	COBIT control objective	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
			management responsibilities within the organisation, ensuring that the business and IT regularly assess and report IT-related risks and the impact on business.											
4.7	Existing or new	<ul style="list-style-type: none"> <li>Management has not implemented an action plan to address and resolve potential issues of non-compliance in a timely manner.</li> </ul>	Ensure that the organisation establishes and maintains a function that is competent and adequately staffed and/or seeks internal assurance services – most likely through an audit committee – to provide the board with timely independent assurance about the compliance of IT with its policies, standards and procedures, as well as with generally accepted practices.	P	P	S	S	S	S	S	X	X	X	X

## Chapter 6

### 6 Summary and conclusion

Numerous security and data integrity risks could arise from the implementation and utilisation of a virtual private network. It is necessary for the organisation to identify these potential risks and ascertain the impact of these risks on the organisation's operations. When addressing these risks and considering the most appropriate solution set, IT management should consider the impact on the current IT governance processes as well as the overall business governance processes.

An analysis to determine whether COBIT provides an adequate framework to ensure the identification of virtual private network-related risks and addresses IT compliance with policies, regulations and laws is presented in this research study. The assignment also includes a synopsis of whether the principles of COBIT can be implemented to identify, mitigate and manage virtual private network risks.

The purpose of this study was to evaluate if COBIT is a suitable framework that can be used to assist in the governance of VPNs. It focuses on whether COBIT provides an adequate framework to ensure the identification of VPN-related risks and addresses IT compliance with policies and statutory regulations. It furthermore encourages awareness of the importance of IT governance, points to the necessity of understanding IT governance properly, and highlights the importance of implementing adequate internal controls.

In order to achieve this goal, the problem statement documented in Chapter 1 was analysed and divided into three categories, namely governance, technology (VPNs), and the risks arising from the technology. Firstly, the concept of governance was investigated, during which the importance of good governance for VPNs was recognised. The next step was to identify a framework that would be suitable for this research study. This was done by investigating the different types of governance frameworks available, by visiting their respective websites, reviewing the available literature and eliminating unsuitable frameworks.

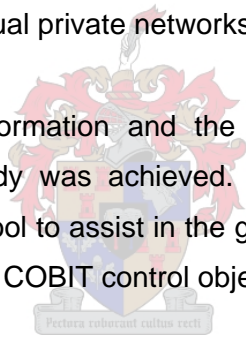
As the COBIT framework was selected as the suitable tool, a thorough understanding of the framework principles was required. This task was achieved by performing a detailed study of the IT processes defined in the model's four domains. Furthermore, understanding VPNs as concept, as well as VPN technology, architecture and requirements, was necessary. In order to obtain this level of understanding, technical manuals and literature was reviewed. This review of the technology assisted in identifying the risks and issues inherent to VPNs,

as well as providing direction on how the risks would affect the organisation's strategies, management and goals.

The final task was to allocate the identified VPN risks and/or issues to the relevant COBIT processes and then map the identified risk or issue onto the pertinent COBIT control objective. The possible VPN risks and/or issues documented in the respective matrices are in no way a comprehensive list and have been based primarily on the risks and issues documented in the preceding chapters of this study. To ascertain whether the COBIT framework is a suitable tool to assist in the governance of VPNs, all the VPN risks and issues identified had to be associated with the framework.

In conclusion, it is essential that the organisation's IT management obtains a suitable approach, guidelines and tools to ensure that IT governance is implemented to be in line with best practices and the organisation's needs. The governance tool implemented by the organisation – whether a VPN is currently utilised or its implementation is planned – should present an adequate framework that can be utilised to effectively manage and/or mitigate the risks and issues associated with virtual private networks.

Through the documentation of information and the mapping exercise executed in the matrices, the objective of this study was achieved. It was concluded that the COBIT framework is a suitable evaluation tool to assist in the governance of VPNs, as all VPN risks identified could be associated with a COBIT control objective.





## Bibliography

**ADTRAN. 2001.** *Understanding Virtual Private Networking: A technology guide from ADTRAN* [Online]. Available: <http://www.alliancedata.com/Understanding%20Virtual%20Private%20Networking.pdf> [2005, 24 October].

**BROWN, S. 1999.** *Implementing virtual private networks*. 1<sup>st</sup> ed. New York: McGraw-Hill.

**COE, M.J. 2005.** A better way to evaluate IT controls. *Journal of Accountancy*, 199(3), March. [Online]. Available: <http://www.aicpa.org/publs/jofa/mar2005/coe.htm> [2006, 26 December].

**COSO (Committee of Sponsoring Organisations of the Treadway Commission).** COSO Definition of Internal Control. [Online]. Available: <http://www.coso.org/key.htm> [2006, 28 December].

**DE HAES, S. & VAN GREMBERGEN, W. 2004.** IT governance and its mechanisms. *Information Systems Control Journal*, (1):27–33.

**FOWLER, D. 1999.** *Virtual private networks: making the right connection*. 1<sup>st</sup> ed. San Francisco: Morgan Kaufmann.

**GULDENTOPS, E. 2003.** Statutory Audit and IT Governance. *Information Systems Control Journal* [Online]. Available: [http://www.isaca.org/Content/ContentGroups/Journal1/20033/Statutory\\_Audit\\_and\\_IT\\_Governance.htm](http://www.isaca.org/Content/ContentGroups/Journal1/20033/Statutory_Audit_and_IT_Governance.htm) [2006, 24 December].

**HAYMAKER, S. 2003.** Spotlight on governance. *Information Systems Control Journal*, (1):15–19.

**HAYMAKER, S. & HUTTON, A. 2004.** Principles of IT governance. *Information Systems Control Journal*, (2):47–50.

**HELLER, M. 2006.** *Virtual private networks* [Online]. Available: <http://www.computerworld.com/article.do?command=viewArticleBasic&articleID=9002090&pageNumber=1> [2006, 24 December].

**HESCHL, J. 2004.** COBIT in relation to other international standards. *Information Systems Control Journal*, (4):37–40.

**IFAC (International Federation of Accountants). 2004.** *Enterprise governance: getting the balance right* [Online]. Available:  
<http://www.ifac.org/MediaCenter/files/EnterpriseGovernance.pdf> [2006, 28 December].

**IIA (Institute of Internal Auditors). s.a.** *Virtual office: risk management, security, control, and auditing* [Online]. Available:  
[http://www.theiia.org/index.cfm?act=content.print&doc\\_id=870](http://www.theiia.org/index.cfm?act=content.print&doc_id=870) [2005, 24 October].

**ISACA (Information Systems Audit and Control Association). 2000.** *COBIT 3<sup>rd</sup> Edition – Control objectives for information and related technology* [Online]. Available:  
<http://www.isaca.org/cobit> [2005, 24 October].

**ISACA (Information Systems Audit and Control Association). 2004.** *IS auditing guideline 25: Review of virtual private networks.* [Online]. Available: <http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18678> [2005, 24 October].

**ISACA (Information Systems Audit and Control Association). 2005.** *COBIT 4<sup>th</sup> Edition – Control objectives for information and related technology.* [Online]. Available:  
<http://www.isaca.org/cobit> [2006, 20 December].

**ISACA (Information Systems Audit and Control Association). 2007.** *Mapping of ITIL with COBIT 4* [Online]. Available:  
<http://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=29058> [2006, 24 January].

**IT GOVERNANCE INSTITUTE. 2003.** *Board briefing on IT governance.* 2<sup>nd</sup> ed. [Online]. Available:  
[http://www.isaca.org/Template\\_ITGI.cfm?Section=Business,\\_Management\\_and\\_Governance1&CONTENTID=9822&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.isaca.org/Template_ITGI.cfm?Section=Business,_Management_and_Governance1&CONTENTID=9822&TEMPLATE=/ContentManagement/ContentDisplay.cfm) [2006, 24 December].

**IT GOVERNANCE INSTITUTE. 2006.** *IT control objectives for Sarbanes-Oxley.* 2<sup>nd</sup> ed. [Online]. Available:

[http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT\\_Control\\_Objectives\\_for\\_Sarbanes-Oxley\\_2nd\\_research.pdf](http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_2nd_research.pdf) [2006, 24 December].

**JOHNSON, E.C. 2005.** IT governance: new players, challenges and opportunities. *Information Systems Control Journal*, (2):17–18.

**KORDEL, L. 2004.** IT governance hands-on: using COBIT to implement IT governance. *Information Systems Control Journal*, (2):39–46.

**LEDESMA, C. 2004.** Virtual private network: Audit approach based on standard SDLC concepts. *Information Systems Control Journal*, (4):23–24.

**PARKES, H. 2004.** IT governance and outsourcing. *Information Systems Control Journal*, (5):17-21.

**SHUE, L. 2004.** Sarbanes-Oxley and IT outsourcing. *Information Systems Control Journal*, (5):28–30.

**TYSON, J. 1998-2005.** *How virtual private networks work* [Online]. Available: <http://computer.howstuffworks.com/vpn.htm/printable> [2005, 25 October].

**VPNC (Virtual Private Network Consortium). 2004.** *VPN technologies: definitions and requirements* [Online]. Available: <http://www.vpnc.org/vpn-technologies.html> [2005, 24 October].