Fitting an Information Security Architecture

To

An Enterprise Architecture

Fitting an Information Security Architecture to an Enterprise Architecture

by

CHINTHAL KRISHNA NAIDOO

MINOR DISSERTATION

Submitted in partial fulfilment of the requirements for the degree

MASTERS in PHILOSOPHY

In

INFORMATION TECHNOLOGY

In the

FACULTY OF SCIENCE

at

THE UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF SH VON SOLMS

November 2007

TABLE OF CONTENTS

Preface

Abstract

Despite the efforts at international and national level, security continues to pose challenging problems. Firstly, attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user's knowledge, while the number of variants (and the rate of evolution) of malicious software (malware) is increasing rapidly. Spam is a good example of this evolution. It is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware, phishing and other forms of malware. Its widespread distribution increasingly relies on botnets, i.e. compromised servers and PCs used as relays without the knowledge of their owners. The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges, as IP-based services develop rapidly. These could eventually prove to be a more common route for attacks than personal computers since the latter already deploy a significant level of security. Indeed, all new forms of communication platforms and information systems inevitably provide new windows of opportunity for malicious attacks.

In order to successfully tackle the problems described above, a strategic approach to information security is required, rather than the implementation of ad hoc solutions and controls.

The strategic approach requires the development of an Information Security Architecture. To be effective, an Information Security Architecture that is developed must be aligned with the organisation's Enterprise Architecture and must be able to incorporate security into each domain of the Enterprise Architecture.

This mini dissertation evaluates two current Information Security Architecture models and frameworks to find an Information Security Architecture that aligns with Eskom's Enterprise Architecture.

Part 1

Chapter 1

Research overview and objectives

This study intends to identify an Information Security Architecture that aligns with the principles and requirements of the Enterprise Architecture of a large energy utility company called Eskom.

The aim of this chapter is to motivate the need for an Information Security Architecture and to give an overview of this dissertation. This chapter consists of the following:

1.1 Introduction
1.2 Problem description and objectives
1.3 Scope and limitations
1.4 Approach of this dissertation
1.5 Structure of this dissertation
1.6 Schematic description of the approach
1.7 Conclusion

The remainder of the chapter will be discussed under the above headings.

1.1 INTRODUCTION

1.1	**Introduction**
1.2	**Problem description and objective**
1.3	**Scope and limitations**
1.4	**Approach of this dissertation**
1.5	**Structure of this dissertation**
1.6	**Schematic description of the approach**
1.7	**Conclusion**

According to The Global State of Information Security 2005 [3], information security is an escaped wildfire and organisations are desperately trying to outflank the fire-line and prevent flare-ups and firestorms. According to the same report, "everyday its something else". Some of the known reported cases include millions of personally identifiable records stolen, intellectual property left on laptops that's gone missing, corporate espionage rings that use IT to infiltrate companies, phishing scams by the thousands. Then there's spam and spyware, zombie networks, DDoS (distributed denial of service) attacks and session hijacking, online auction fraud, online extortion, new variants of viruses and worms and the growing requirements of government regulations. Protecting an organisation's information and system resources is becoming "a thankless and impossible business" [3].

If information security is an escaped wildfire, is it because we are approaching the problem from a tactical rather than a strategic view.

According to the same survey report [3], only 37% of respondents reported that they had an information security strategy and only 24% of the rest said that creating one was in the plans for next year. With increasingly serious, complex, targeted and damaging threats continuously emerging, that's not a good thing. When you spend all the time fighting fires, you don't have the time to come up with the new ways to build things so they don't burn down [3].

To illustrate the focus on tactical approaches, according to the survey data in [3], respondents spent most of their time in reactive mode, responding to incidents, deploying firewalls, dealing with everyday nuisances like spam and spyware. Ironically the most proactive step respondents took was to develop business continuity and disaster

recovery plans. So even the proactive steps was an investment in reactive measures [3].

Many corporate organisations implement technical solutions to business security requirements on a tactical basis. Usually a requirement is identified and a product is sought and acquired to meet that requirement without regard to the broader implications. A point solution is implemented which is often effective in providing some security, but frequently no one is really sure that the security is appropriate to the risk, or that the cost is commensurate with the benefit, or that it meets a wide variety of other business requirements which are not specifically risk-related. This can lead to many problems. The security solutions are often isolated and incapable of being integrated together or of inter-operating with one another. The variety of security solutions leads to increased complexity and cost of support, and in particular can lead to an exploding workload with regard to administration and management. If business security is to be effective in enhancing the business process and achieving business goals, then a much more strategic view should be developed [2].

"Organisations are in the midst of an evolution in the computing environment – developing or acquiring new applications, integrating mainframe legacy systems with distributed and multi-platform processing environments, and employing new technologies to meet business needs. Several trends have occurred that make it a requirement for organisations to develop a strategic approach to information security" [1].

According to the Information Security Forum (ISF) [4], achieving an enterprise-wide security architecture is only possible by aligning security architecture with the organisation's enterprise architecture."

1.2 PROBLEM DESCRIPTION AND OBJECTIVES

1.1	Introduction
1.2	Problem description and objective of this dissertation
1.3	Scope and limitations
1.4	Approach of this dissertation
1.5	Structure of this dissertation
1.6	Schematic description of the approach
1.7	Conclusion

1.2.1 PROBLEM DESCRIPTION

Approaching information security from a tactical and operational view will not provide the solutions that will ensure that information security solutions are not isolated and incapable of being integrated together or of inter-operating with one another. It is evident that tackling the innumerable risks facing organisations cannot be approached by addressing each risk in isolation.

What is required is a strategic approach to information security. To succeed in attaining a strategic approach, it is proposed that "organisations must develop and implement a comprehensive and flexible enterprise wide Information Security Architecture (ISA) to protect the confidentiality, integrity and availability of their information and system resources in this new and evolving environment" [1].

Developing an Information Security Architecture should entail taking a holistic, enterprise-wide view and creating principles, policies and standards by which information security systems will be designed and built. It will ensure consistency of the design approach across large complex systems or across a complex array of smaller systems. Architectural approaches break up the complexity so as to present greater simplicity and thus make the design activity easier to manage [2].

Many companies are exposed to serious IT risks because they do not have an enterprise-wide Information Security Architecture. In the case of Eskom, the company has a comprehensive Enterprise Architecture, but does not have an information Security Architecture to support its Enterprise Architecture.

1.2.2 OBJECTIVE OF THIS DISSERTATION

The objective of this dissertation is to identify an Information Security Architecture that aligns with the principles and security requirements of the Enterprise Architecture of a large energy utility, Eskom.

1.3 SCOPE AND LIMITATIONS

1.1	Introduction
1.2	Problem description and objective of this dissertation
1.3	Scope and limitations
1.4	Approach of this dissertation
1.5	Structure of this dissertation
1.6	Schematic description of the approach
1.7	Conclusion

This dissertation will be limited to the identifying of an Information Security Architecture that is based on two current Information Security Architecture frameworks and models. The identified Information Security Architecture should align and fit within an overall Enterprise Architecture of a large energy utility, Eskom.
The quality and merits of the overall Enterprise Architecture will not be discussed in this dissertation. The Enterprise Architecture will therefore be accepted as is.

1.4 APPROACH AND DELIVERABLES

1.1	Introduction
1.2	Problem description and objective of this dissertation
1.3	Scope and limitations
1.4	Approach and Deliverable of this dissertation
1.5	Structure of this dissertation
1.6	Schematic description of the approach
1.7	Conclusion

1.4.1 Approach of the dissertation

A literature survey will be done to identify possible Information Security Architecture models and frameworks. Each of the identified frameworks and models will be analysed to understand the components that make up the framework.

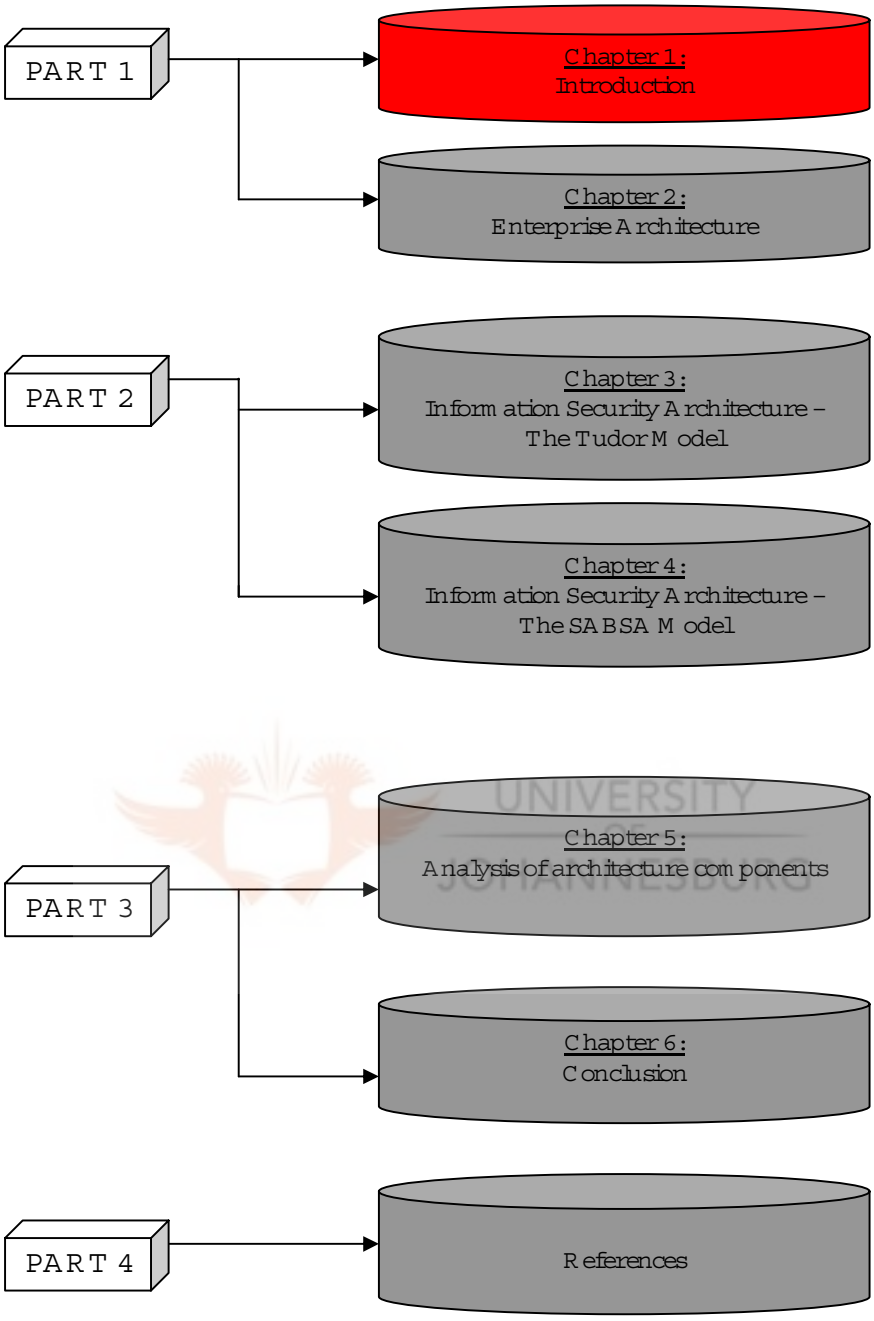
With the information obtained, an analysis will be conducted to assess the extent to which the analysed Information Security Architecture frameworks meet the information security services requirements identified by the Enterprise Architecture of Eskom.

1.4.2 Deliverable of the dissertation

The main deliverable will be a recommendation for an Information Security Architecture for Eskom which best aligns with Eskom's Enterprise Architecture.

1.5 STRUCTURE OF THIS DISSERTATION

1.1	Introduction
1.2	Problem description and objective of this dissertation
1.3	Scope and limitations
1.4	Approach of this dissertation
1.5	Structure of this dissertation
1.6	Schematic description of the approach
1.7	Conclusion



As reflected in the schematic above, this dissertation will be divided into four parts:

Part 1 will establish the need for an Information Security Architecture and will specify the components of a supporting Information Security Architecture as defined by the Eskom Enterprise Architecture. Included in Part 1 are Chapter 1 and Chapter 2.

Chapter 1

The objective of Chapter 1 is to motivate the need for an Information Security Architecture and to give an overview of the dissertation. The chapter includes the problem description and objective of this dissertation, the scope and limitations and the approach for this study.

Chapter 2
This chapter defines an Enterprise Architecture and the components of an Enterprise Architecture used by Eskom. It also identifies the requirements of an Information Security Architecture as specified by the Eskom Enterprise Architecture.

Conclusion of Part 1
Part 1 will have provided the motivation for requiring an Information Security Architecture . It will also have provided a background by describing the components of the Enterprise Architecture and its relationship to an Information Security Architecture. The next part will pick up and describe the components of two currently used Information Security Architecture models and frameworks.

Part 2
The components of two Information Security Architecture frameworks and models will be identified and discussed. Included in Part 2 are Chapters 3 and 4.

Chapter 3
In this chapter the Tudor Information Security Architecture will be discussed. [1]

Chapter 4
This chapter will discuss the components of the Sherwood Applied Business Security Architecture (SABSA) model [2].

Conclusion of Part 2

Part 2 will have provided a description of the components of two currently used Information Security Architectures. The next part will

use the components described in Part 1 and Part 2 to analyse and map the components to determine whether any of the Information Security Architectures described in Part 2 will meet the Enterprise Architecture requirements described in Part 1.

Part 3
The components of the two identified Information Security Architecture frameworks are analysed and mapped to the components of the Enterprise Architecture components. Included in Part 3 are Chapter 5 and Chapter 6.

Chapter 5
In this chapter the components of the two identified Information Security Architecture frameworks will be analysed and mapped to the components of the Enterprise Architecture.

Chapter 6
Conclusion
In chapter 6, a recommendation for selecting one of the two Information Security Architectures will be submitted as part of the conclusion.

Conclusion of Part 3
Part 3 will provide an analysis and a recommendation whether to adopt any of the Information Security Architectures that were analysed.

References
The references that were used will be listed.

1.6 Schematic description of the approach

1.1	**Introduction**
1.2	**Problem description and objective of this dissertation**
1.3	**Scope and limitations**
1.4	**Approach of this dissertation**
1.5	**Structure of this dissertation**
1.6	**Schematic description of the approach**
1.7	**Conclusion**

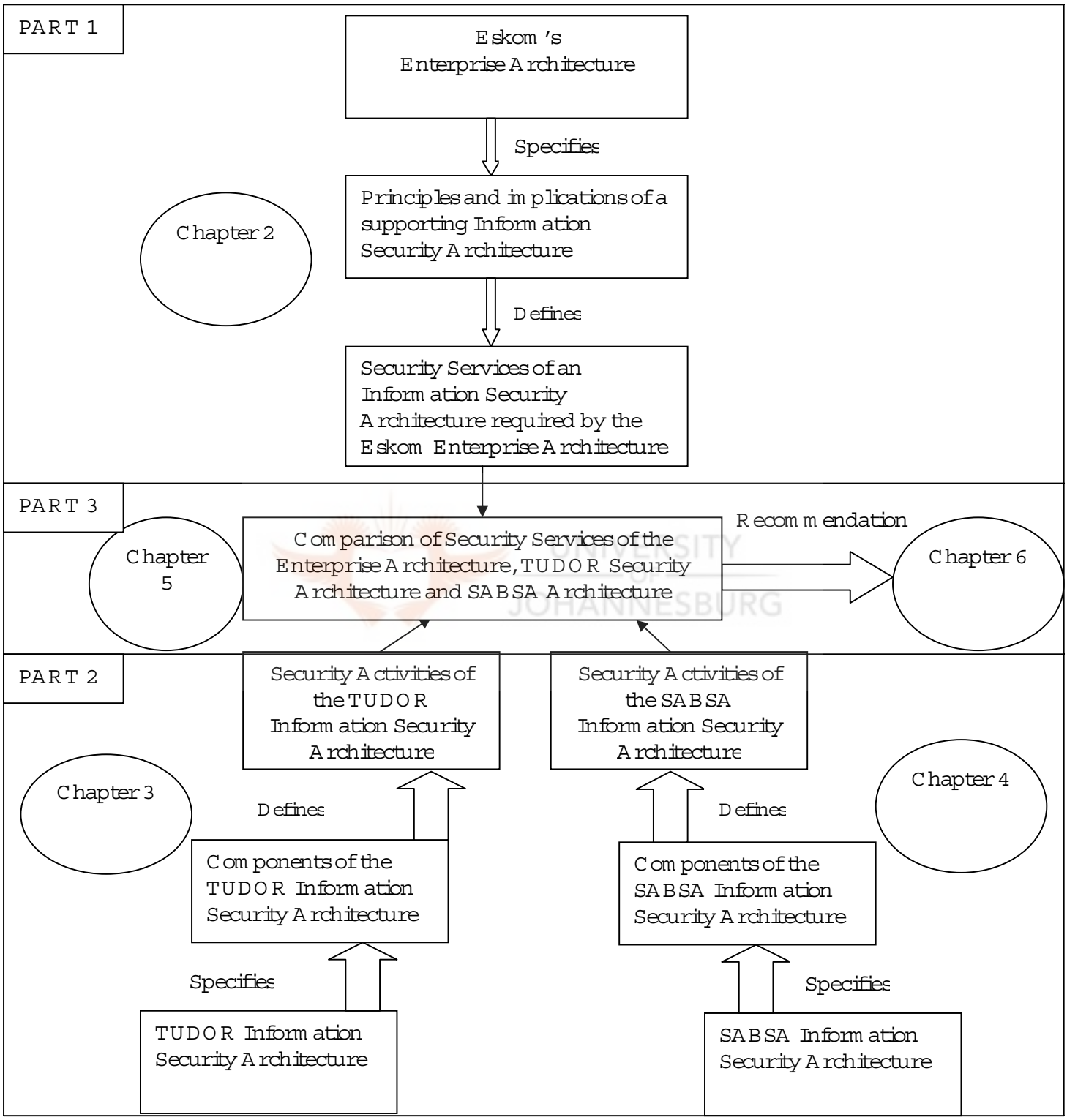

PART 1
Eskom's Enterprise Architecture
Specifies
Principles and implications of a supporting Information Security Architecture
Chapter 2
Defines
Security Services of an Information Security Architecture required by the Eskom Enterprise Architecture
PART 3
Chapter 5
Comparison of Security Services of the Enterprise Architecture, TUDOR Security Architecture and SABSA Architecture
Recommendation
Chapter 6
PART 2
Security Activities of the TUDOR Information Security Architecture
Security Activities of the SABSA Information Security Architecture
Chapter 3
Chapter 4
Defines
Defines
Components of the TUDOR Information Security Architecture
Components of the SABSA Information Security Architecture
Specifies
Specifies
TUDOR Information Security Architecture
SABSA Information Security Architecture

Figure 1.6

1.7 CONCLUSION

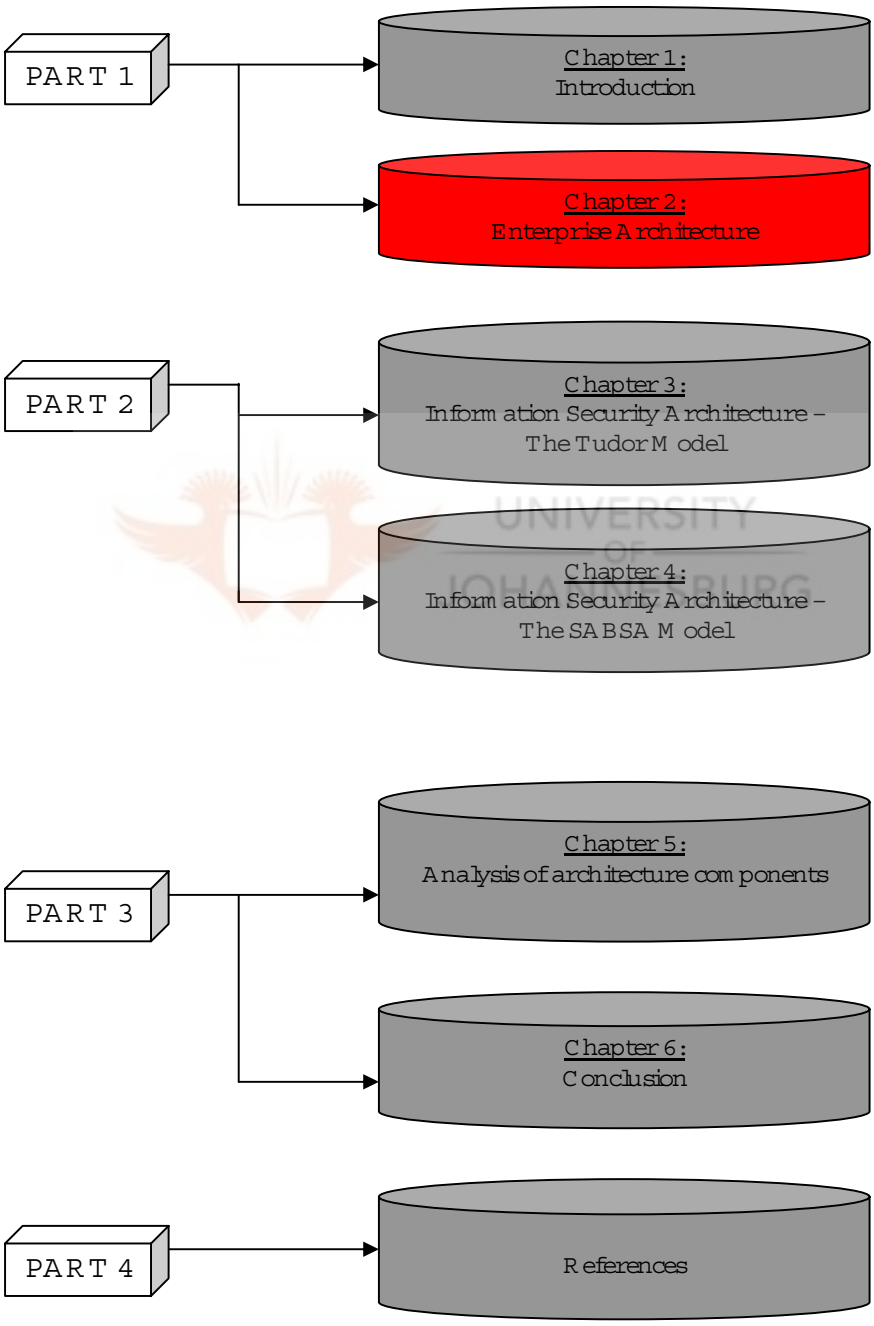
1.1	**Introduction**
1.2	**Problem description and objective of this dissertation**
1.3	**Scope and limitations**
1.4	**Approach of this dissertation**
1.5	**Structure of this dissertation**
1.6	**Schematic description of the approach**
1.7	**Conclusion**

Chapter 1 motivated the need for an Information Security Architecture and gave an overview of this mini dissertation. The chapter also described the scope and limitations, the approach of this mini dissertation and the structure of this mini dissertation.

Chapter 2, the next chapter, will define an Enterprise Architecture and the components of an Enterprise Architecture used by Eskom. It also shows the alignment between Enterprise Architectures and Information Security Architectures.

CHAPTER 2

ENTERPRISE ARCHITECTURE



CHAPTER 2

This chapter defines the Enterprise Architecture and the components of the Enterprise Architecture used by Eskom.

This chapter also provides a definition of Information Security Architecture and explains the alignment between Enterprise Architecture and Information Security Architecture.
The chapter consists of the following headings:

2.1 Definition of an Enterprise Architecture
2.2 Components of Eskom's Enterprise Architecture
2.3 Security requirements for an Enterprise Architecture
2.4 Alignment between an Enterprise Architecture and the Information Security Architectures
2.5 Conclusion

2.1 Definition of an Enterprise Architecture

2.1	**Definition of an Enterprise Architecture**
2.2	**Components of Eskom's Enterprise Architecture**
2.3	**Security requirements for an Enterprise Architecture**
2.4	**Alignment of an Information Security Architecture with an Enterprise Architecture**
2.5	**Conclusion**

The definition of an architecture used in ANSI/IEEE Standard 1471-2000 is:
"The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution." [6]

According to The Open Group Architecture Framework (TOGAF) [6], "architecture" has two meanings depending upon its contextual usage:

A formal description of a system, or a detailed plan of the system at component level to guide its implementation.

The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.

TOGAF states that the term "enterprise" in the context of "enterprise architecture" can be used to denote both an entire enterprise, encompassing all of its information systems, and a specific domain within the enterprise. In both cases, the architecture crosses multiple systems, and multiple functional groups within the enterprise. [6]

For the purposes of this dissertation, Enterprise Architecture is defined as "a consistent set of principles, policies and standards that sets the direction and vision for the development and operation of the organisation's business information systems so as to ensure alignment with and support for the business needs" [2]

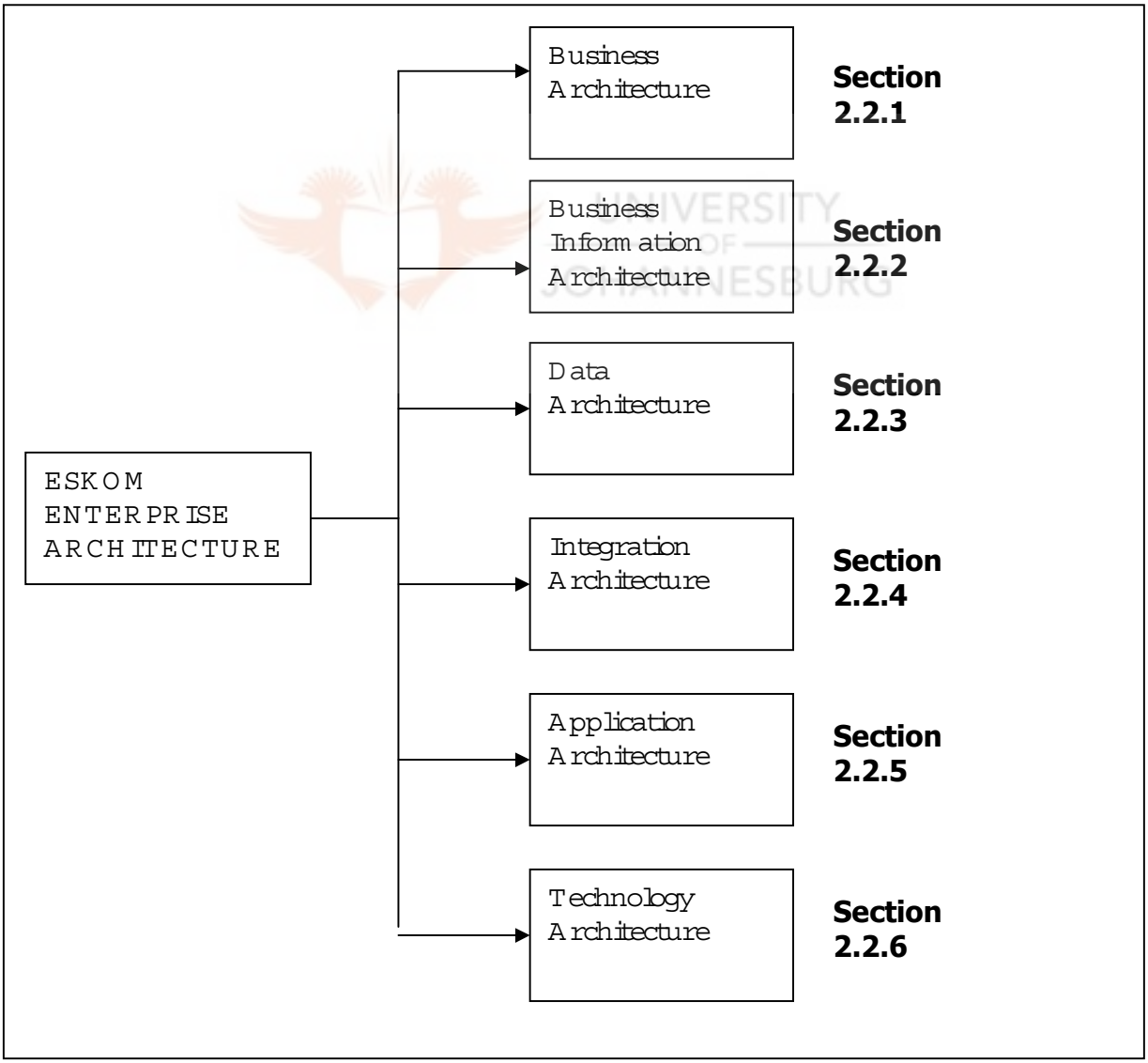
2.2 Components of Eskom's Enterprise Architecture.

2.1	**Definition of Enterprise Architecture**
2.2	**Components of Eskom's Enterprise Architecture**
2.3	**Security requirements for an Enterprise Architecture**
2.4	**Alignment of an Information Security Architecture with an Enterprise Architecture**
2.5	**Conclusion**

The Eskom Enterprise Architecture is comprised of the following components:

2.2.1	**The Business Architecture**
2.2.2	**The Business Information Architecture**
2.2.3	**The Data Architecture**
2.2.4	**The Integration Architecture**
2.2.5	**The Application Architecture**
2.2.6	**The Technology Architecture**

Schematic overview of the Eskom Enterprise Architecture



2.2.1 The Business Architecture

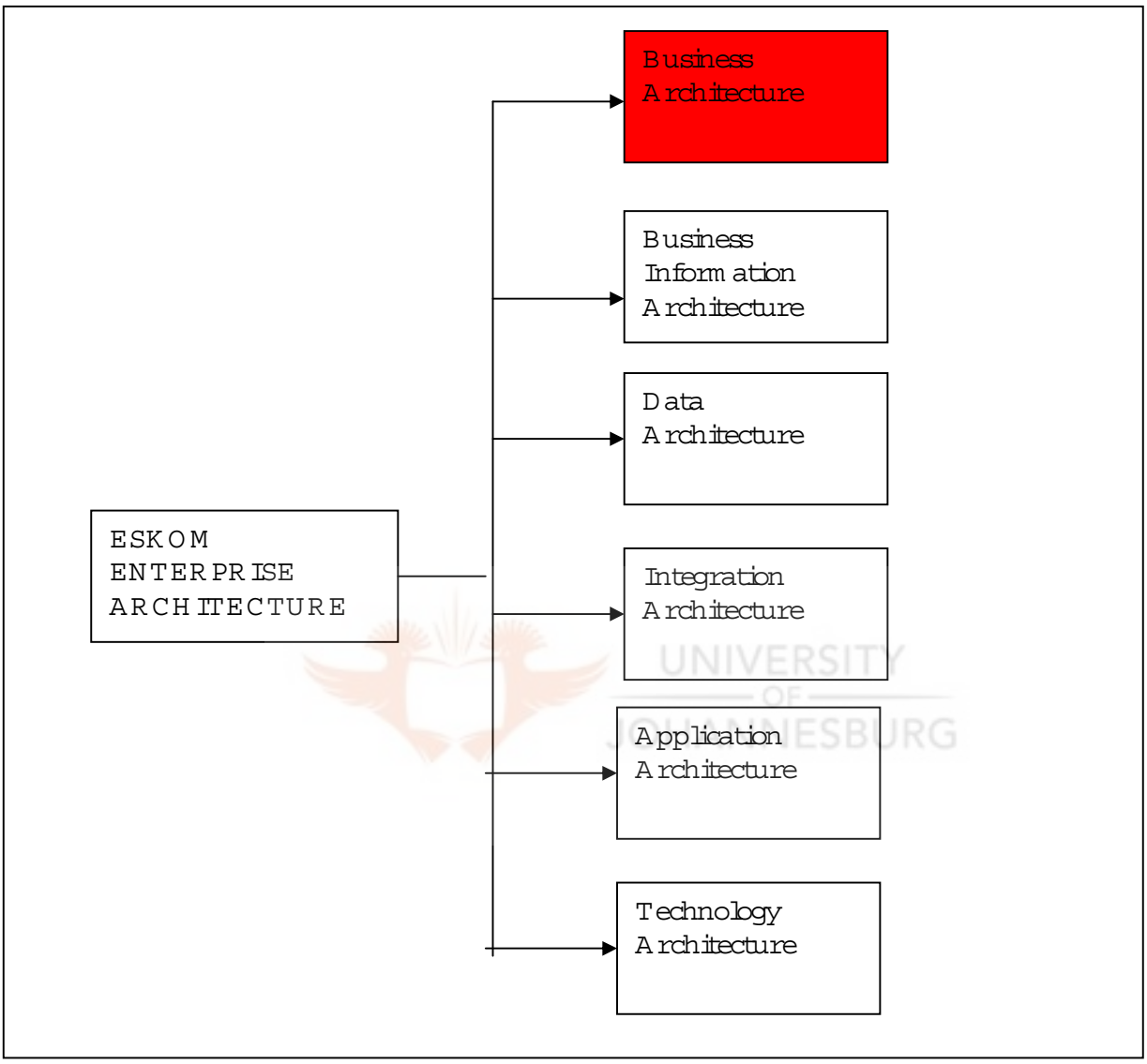


Figure 2.2.1

The Business Architecture of Eskom reflects from an enterprise-wide perspective how the business itself is structured. The Business Architecture of Eskom considers the businesses strategy and plans, its business processes and policies and the business organisation design. The Business Architecture consists of:

A) Organizational Structure. The organizational chart diagram of the organisation is used to develop the hierarchy in the organization and shows the relationship to the business locations where organizational units are located.

B) Business Goals and Objectives. The organisational goals and objectives are documented for each organizational unit
C) Business Functions. The functions of the business are modelled, starting from a high level and decomposing to lower levels.
D) Business Services. The services that the business provides to customers are modelled, both external customers and internal customers.
E) Business Processes. The business processes are documented
F) Business risks. The risks facing the business are assessed and documented.

The Business Architecture is the primary architecture because through the Business Architecture an understanding of the business and its requirements are obtained. An understanding of the business and its requirements is therefore a prerequisite for the designing of the Enterprise Architecture. The other architectures are all created in support of this single overriding architecture of how the business actually works and what it requires.

Arising from the Business Architecture are business information requirements that reflect the highest order information requirements that supports the business strategy and which acts as the mandate for the Enterprise Architecture.

There are a number of business information requirements that arises from the Business Architecture, however the information requirement which relates specifically to information security is

Protect information and business continuity

This business requirement is to protect the information resource and provide for business continuity in the event of the loss of information.

The nature of the business environment in general and the increase in competitive forces, results in a need and business imperative to provide increased levels and more timeous access to the information resources to a wider audience, including outside parties like customers and business partners.
The advent and wide deployment of technologies, which grant such access itself, increases this need. These factors increase the risk of the loss of information, as well as the consequences of such loss and emphasise the need for the information requirement identified above. This business information requirement will be discussed further in the sections that follow.

Next we discuss the Business Information Architecture component of the Enterprise Architecture.

2.2.2 Business Information Architecture

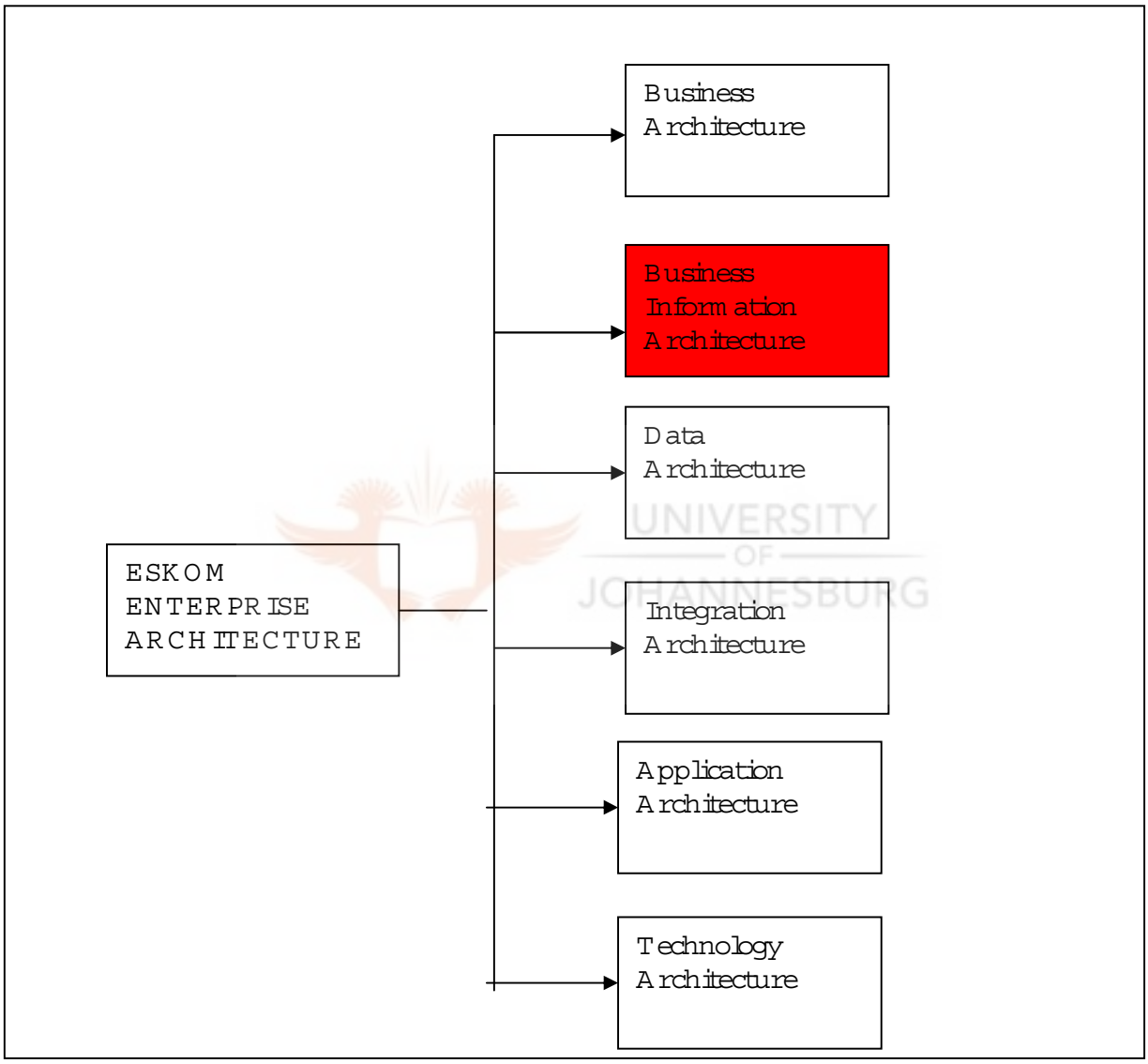


Figure 2.2.2

The Business Information Architecture of Eskom is a disciplined process that details the business information strategies, its extended information value chain, its information management principles, and their impact on technical architecture. It is informed and driven by the Business Architecture process with which it is closely integrated.
The Business Information Architecture presents a mechanism by which the availability, quality, governance and integrity of information can be discussed in business terms at the very highest levels of management in the organisation.
As discussed in the Business Architecture in the previous section, the Business Architecture provides the overarching guidelines and principles for Enterprise Architecture design. The Business Information Architecture is designed within those guidelines and principles and directly supports the following business information requirement as defined in the Business Architecture that relates specifically to information security:

Protect information and business continuity

The Business Information Architecture supports the above business information requirement through the establishment of principles that guide the Business Information Architecture design. A number of principles are stated in the Business Information Architecture of Eskom that support its business information requirements and specifically the one above. Below is a selection of those principles and its implications in the Business Information Architecture that relate specifically to supporting the information security requirement above:

2.2.2.1 Principle 1

Information is valued as an asset, which should be continuously maintained and shared to enhance and accelerate decision-making at all levels of the organisation.
The implication of this principle is that:

- **The data and information must be identified, authenticated and leveraged.**
- **An information custodianship must be established.**
- **Foster a culture that recognises the importance for and integrity of high quality data.**

2.2.2.2 Principle 2

Access to Eskom information and by its partners is the rule, not the exception, subject to security and confidentiality constraints.
The implication of this principle is that:

- **Pertinent information must be made available.**
- **Open sharing of information must be balanced against confidentiality of business strategies.**
- **Need for common definitions of information to simplify access and sharing.**

2.2.2.3 Principle 3

All information must derive from a known source that has been vetted by the responsible information custodian for accuracy and relevance.
The implications of this principle is that:

- **Existing and prospective information sources must be investigated for accuracy and reliability.**

2.2.2.4 Principle 4

All information, both structured and unstructured, must be recorded, named and classified according to agreed criteria.
The implications o this principle is that:

- **An Information Inventory must be created.**
- **An Information Confidentiality Register must be created.**
- **An Information Business Criticality Register must be created.**

2.2.2.5 Principle 5

Audit trails of changes to sensitive and critical information must be maintained.
The implications of this principle is that:

- **The security audit procedures around information changes must allow for many levels of security with a suitable level of granularity.**
- **An Information Confidentiality Register must be created.**
- **An Information Business Criticality Register must be created.**

2.2.2.6 Principle 6

Standard tools and applications must exist to format information for presentation to audiences with different needs and interests.
The implications of this principle is that:

- **Centralised data warehouses will increasingly supplant application databases as information sources for knowledge workers.**
- **Additional information manipulation and presentation tools will be needed to cater for new information formats.**

2.2.2.7 Principle 7

Information must be reviewed periodically to reassess its relevance and value.
The implications of this principle is that:

- **The uses and value of information must be assessed and measured according to pre-set targets.**

2.2.2.8 Principle 8

Explicit capturing and structuring of information
The implications of this principle is that:

- **The deployment or adaptation of technology, business structures and processes must explicitly capture unstructured and tacit intellectual capital in a secure, easily accessible and organised format.**
- **Intellectual capital pertaining to business processes must be catered for and captured into the information systems architecture.**

2.2.2.9 Principle 9

Explicit information custodianship

The implications of this principle is that:

- **Mechanisms must be acquired or adapted to support the increased focus on information security.**
- **Information ownership issues must be identified and resolved.**
- **Information must be classified in terms of the access to information act.**
- **The mechanisms necessary to support the access to information act and other legislation must be acquired.**

Next we discuss the Data Architecture component of the Enterprise Architecture.

2.2.3 Data Architecture

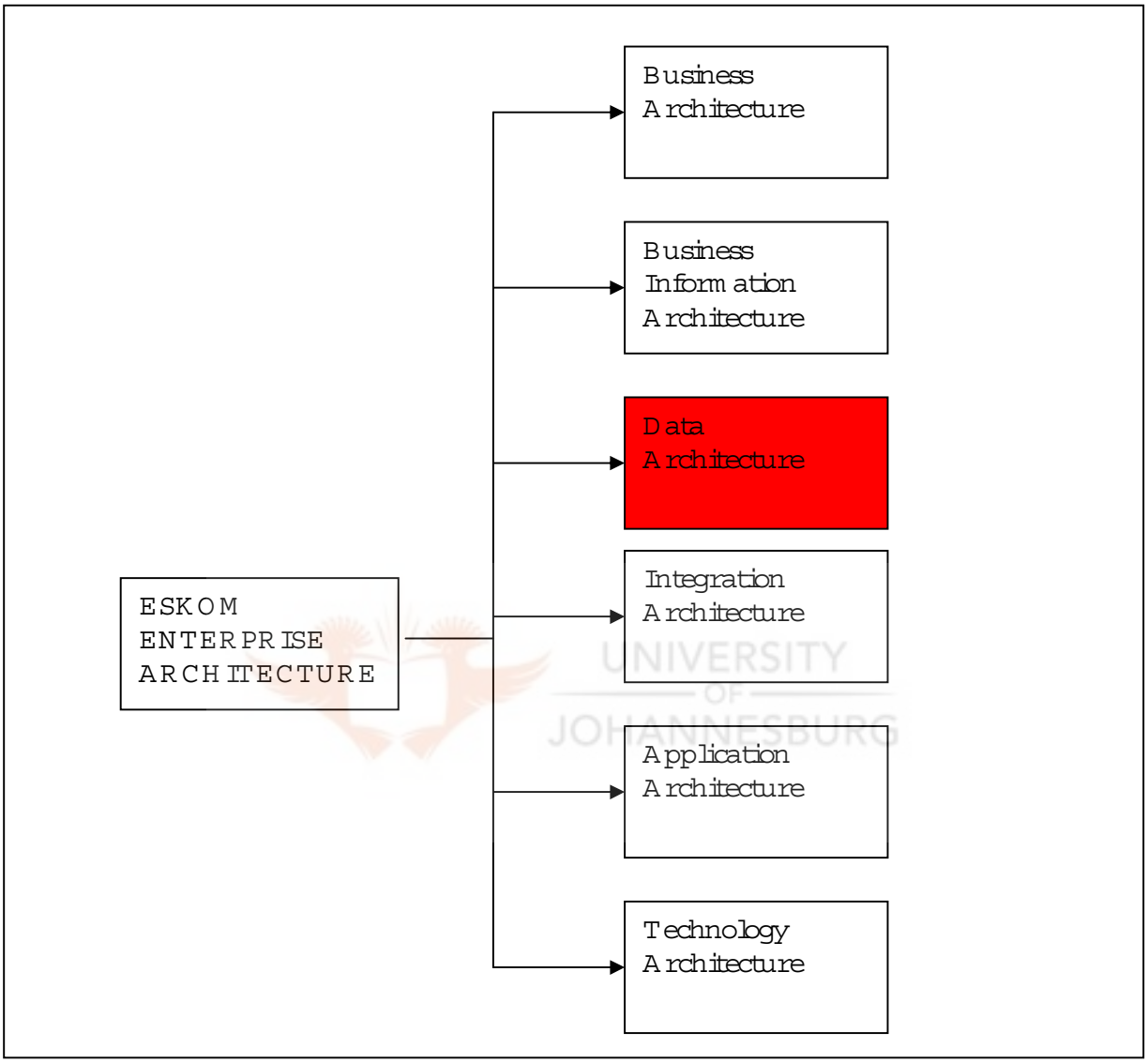


Figure 2.2.3

The Data Architecture defines a mechanism to achieve, regardless of technological platforms, effective management of data as a strategic resource in Eskom.

The Data Architecture considers the Data Architecture as promoting uniformity and standardisation of data elements, database construction, accessibility procedures, inter-system communication and maintenance to increase the effectiveness of systems and the sharing of data within and outside of Eskom.

As discussed in the Business Architecture in the previous section, the Business Architecture provides the overarching guidelines and principles for Enterprise Architecture design. The Data Architecture is designed within those guidelines and principles and directly supports the following business information requirement as defined in the Business Architecture that relates specifically to information security:

Protect information and business continuity

The Data Architecture supports the business information requirement above through the establishment of principles that guide the Data Architecture design. A number of principles are stated in the Data Architecture of Eskom that support its business information requirement. Below is a selection of those principles and its implications in the Data Architecture that relate specifically to supporting the information security requirement above:

2.2.3.1 Principle 1.

The data architecture is designed to be business driven, as opposed to technology driven, and aligned with business processes and the application architecture.
The implications of this principle is that:

- **Data analysis and design must be done before developing application software or purchasing packages.**

2.2.3.2 Principle 2.

Create roles and responsibilities to facilitate the management of data.
The implications of this principle is that:

- **Accurate business definitions of data must be provided.**
- **Security requirements for data must be defined.**
- **Jobs must be defined to include responsibility and tasks concerning data quality and management.**

2.2.3.3 Principle 3.

Centralise data that needs to be shared and must be current.
The implications of this principle is that:

- **Many users need access to latest changes in data**
- **A high volume of data is shared across locations and need to be consistent across all locations.**
- **Replicating frequent updates to distributed databases increases systems complexity and network traffic.**
- **Unintended redundancy of data must be reduced.**
- **Contents of databases must be regularly reviewed.**

2.2.3.4 Principle 4.

Design databases to be modular, not monolithic.
The implications of this principle is that:

- **Achieve better performance, availability, reliability and scalability.**
- **Facilitate data backup and recovery.**

2.2.3.5 Principle 5.

Design for all replicated copies of data to be read-only.
The implication of this principle is that:

- **Updates should occur through the source where the data originates to simplify data management.**

- **Data for public access should be put outside the firewall.**

2.2.3.6 Principle 6.

Use a common data dictionary to design and maintain all new databases.
The implications of this principle is that:

- **Data definitions and data models should be available and kept up-to-date.**
- **Consensus of stakeholders on data definitions will be required.**
- **Data design should be integrated in the appropriate stages of the application system development lifecycle.**

Next we discuss the Integration Architecture component of the Enterprise Architecture

2.2.4 Integration Architecture

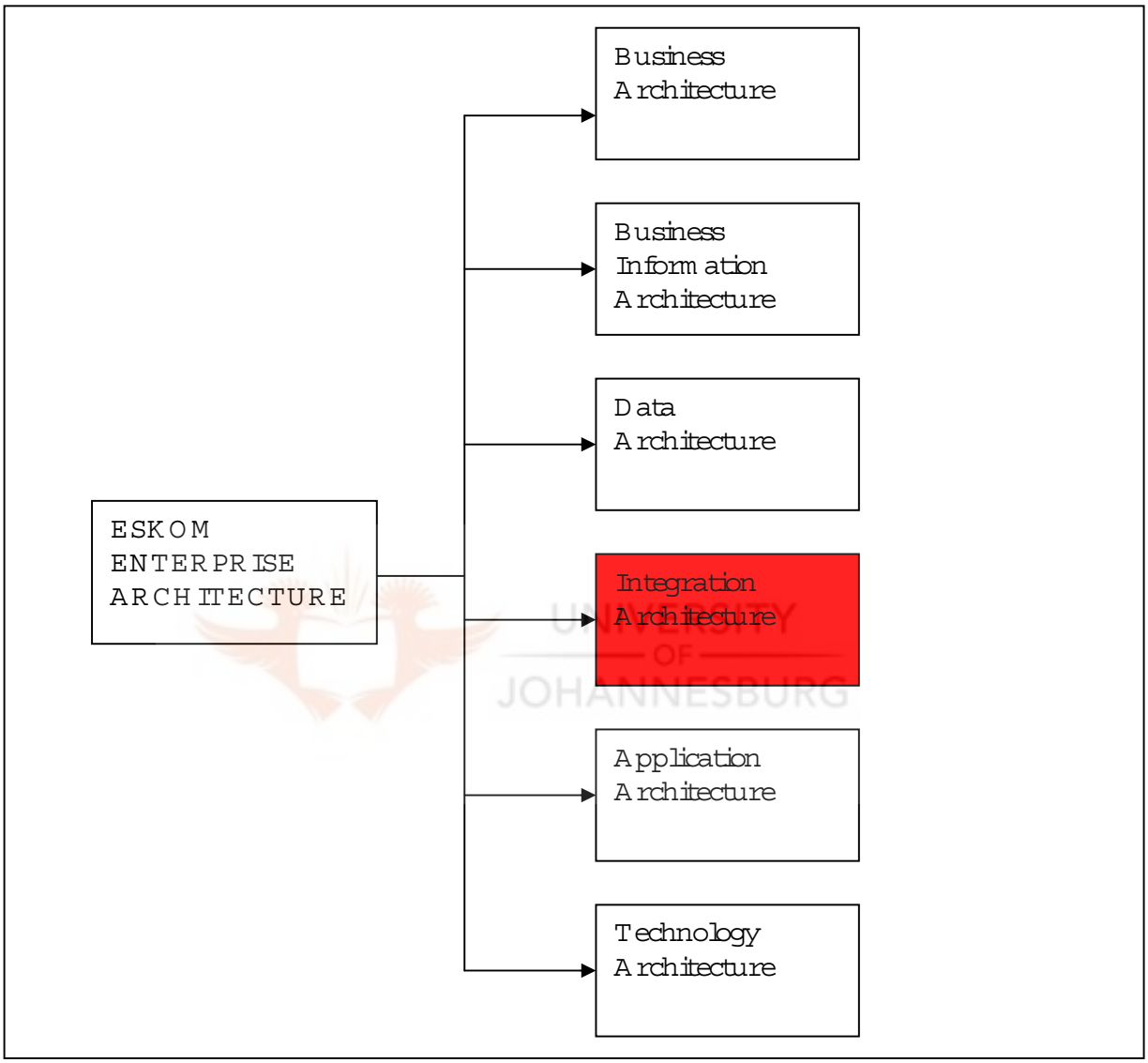


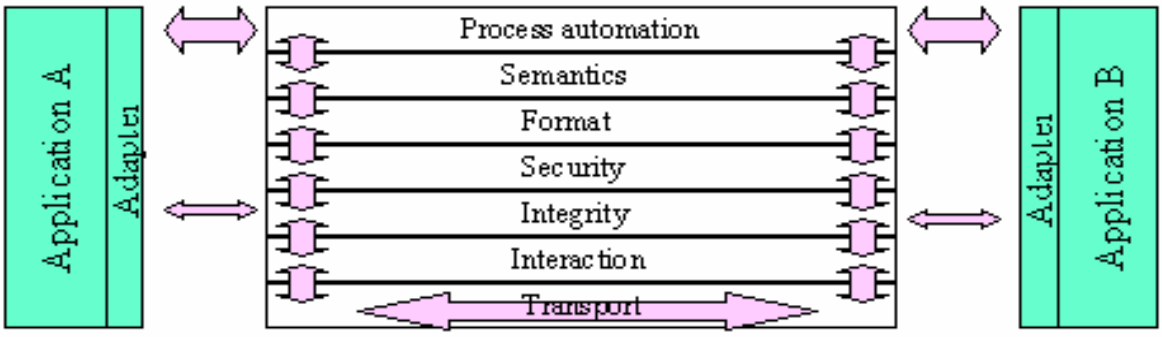
Figure 2.2.4

The Integration Architecture is that subset of the Enterprise Architecture which deals with integration and communications between individual business applications and services, across distributed heterogeneous or homogeneous platforms. The Integration Architecture focuses on inter-application integration, although intra-application integration is also included insofar as the same technology is used. The integration with applications outside of the organisation is included, as are generic user interface facilities.

As discussed in the Business Architecture in the previous section, the Business Architecture provides the overarching guidelines and principles for Enterprise Architecture design. The Integration Architecture is designed within those guidelines and principles and directly supports the following business information requirement as defined in the Business Architecture that relates specifically to information security:

Protect information and business continuity

The Integration Architecture supports the business information requirement above through the establishment of the application integration stack. Figure 2.2.4.1 is a description of the application integration stack.



The *Application Integration* stack

Figure 2.2.4.1

The integration between business applications is done by utilising the application adapter service interfaces. It handles the routing and integration logic for messages and services. Figure 2.2.4.1 above, extracted from the Eskom Integration Architecture specification, is used to describe the integration between business applications.
The integration stack is structured as a set of layers. The lowest layer provides a software interface to the various applications (via their application adapters) consisting of a set of standard functions via which the applications communicate with one another. Each additional layer interposes itself between the application and the previous layer, and provides a higher level set of standard functions to the application adapter. It implements these functions by accessing the lower level functions of the next layer down. By "higher level", it is implied that the functions provided allow the applications to access more powerful functions by performing only a minimum of work.

In the diagram, the security layer, for example, would enable an application to call a function to send an encrypted message. It would then encrypt the message (preventing the application from having to concern itself with the details of how this is done), and then send it by using the standard function from a lower layer for sending a message. Although information security requirements are not clearly specified in the Integration Architecture specification, the implication of the requirements for the Integration Architecture is that:

- **Security functions, example encryption, must be available.**
- **Authentication and authorisation for application to the application access is essential.**

Next we discuss the Application Architecture component of the Enterprise Architecture

2.2.5 Application Architecture

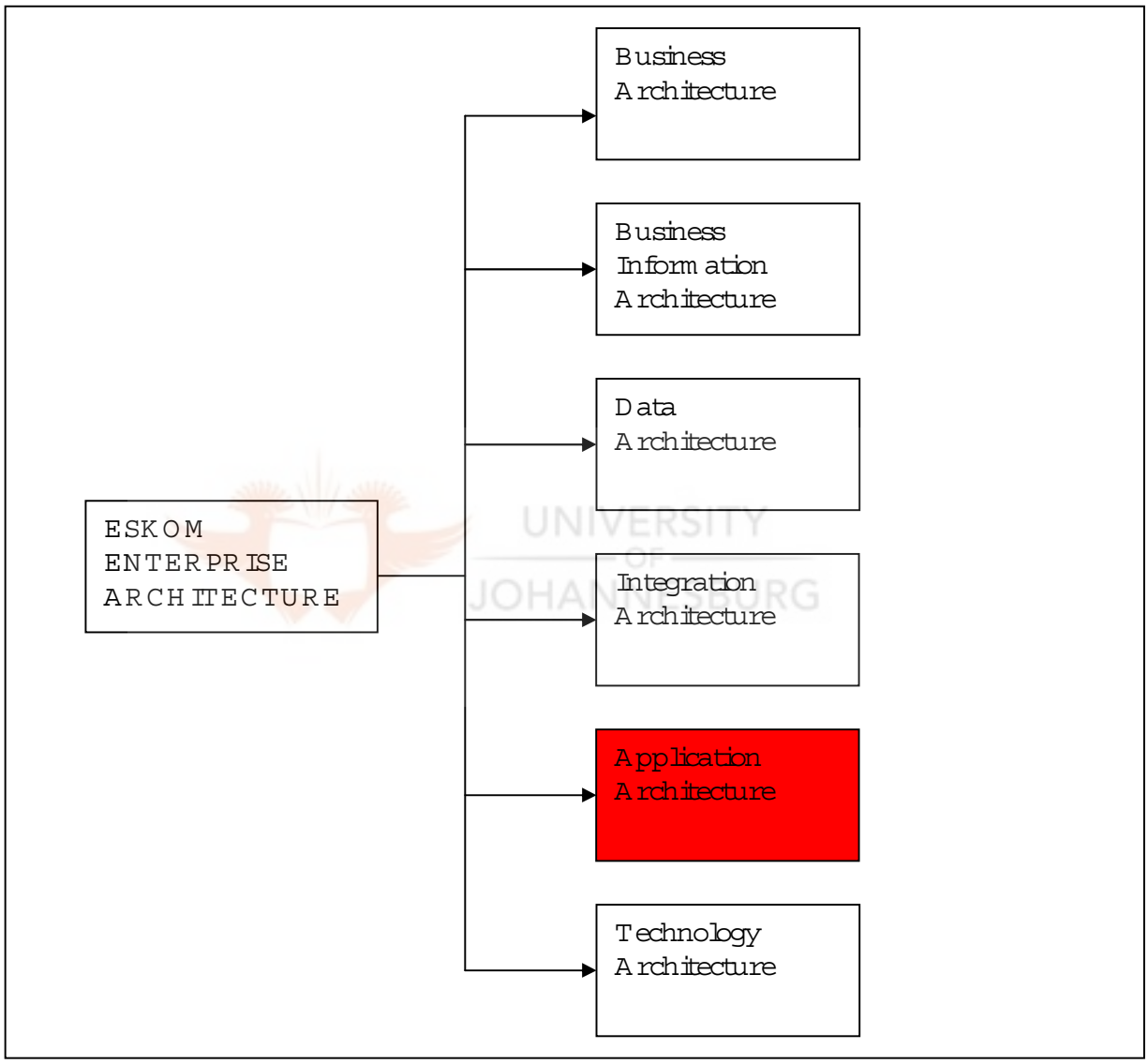


Figure 2.2.5

The Application Architecture is that subset of the Enterprise Architecture concerned with the acquisition and management of application systems to meet business needs.

As discussed in the Business Architecture in the previous section, the Business Architecture provides the overarching guidelines and principles for Enterprise Architecture design. The Application Architecture is designed within those guidelines and principles and directly supports the following business information requirement as defined in the Business Architecture that relates specifically to information security:

Protect information and business continuity

The Application Architecture is considered to be based on a layered application design model. It is a client-server design model that promotes the fact that client-server is not only a physical model. The model distinguishes between the different categories of components from which applications can be constructed, by using a layered application model. It starts off as a business model, breaking business processes into three main types of services (presentation services, business services and data/systems services) which highlights reusable services at a business level. This then gets expanded to include technical, security and system management services to complete the whole layered design model.

Figure 2.2.5.1 below is a graphical representation of the layered application model that is used by development projects, regardless of whether a bought or built solution is being implemented.

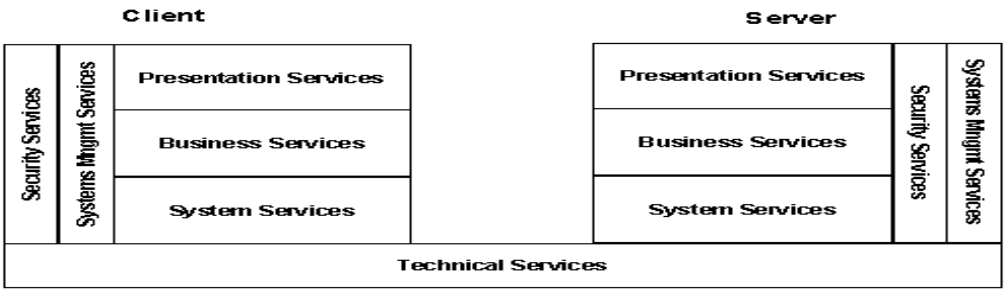


Figure 2.2.5.1

Figure 2.2.5.1 above indicates that all applications are divided into the following service layers:

- **Presentation services**
- **Business services**
- **System services**
- **Technical services**
- **Security services**
- **System Management services**

Of particular interest for the information security requirement is the Security services layer.

The Security services layer provide support services to all the other layers for security services, which is why it is drawn across all the layers.

The implication of this security services layer is that the following security services must be provided:

- **Security authentication**
- **Security authorisation**

This layered approach allows the organisation to change its security system without affecting the applications.

We will next discuss the Technology Architecture, which is the last component of the Enterprise Architecture.

2.2.6 Technology Architecture

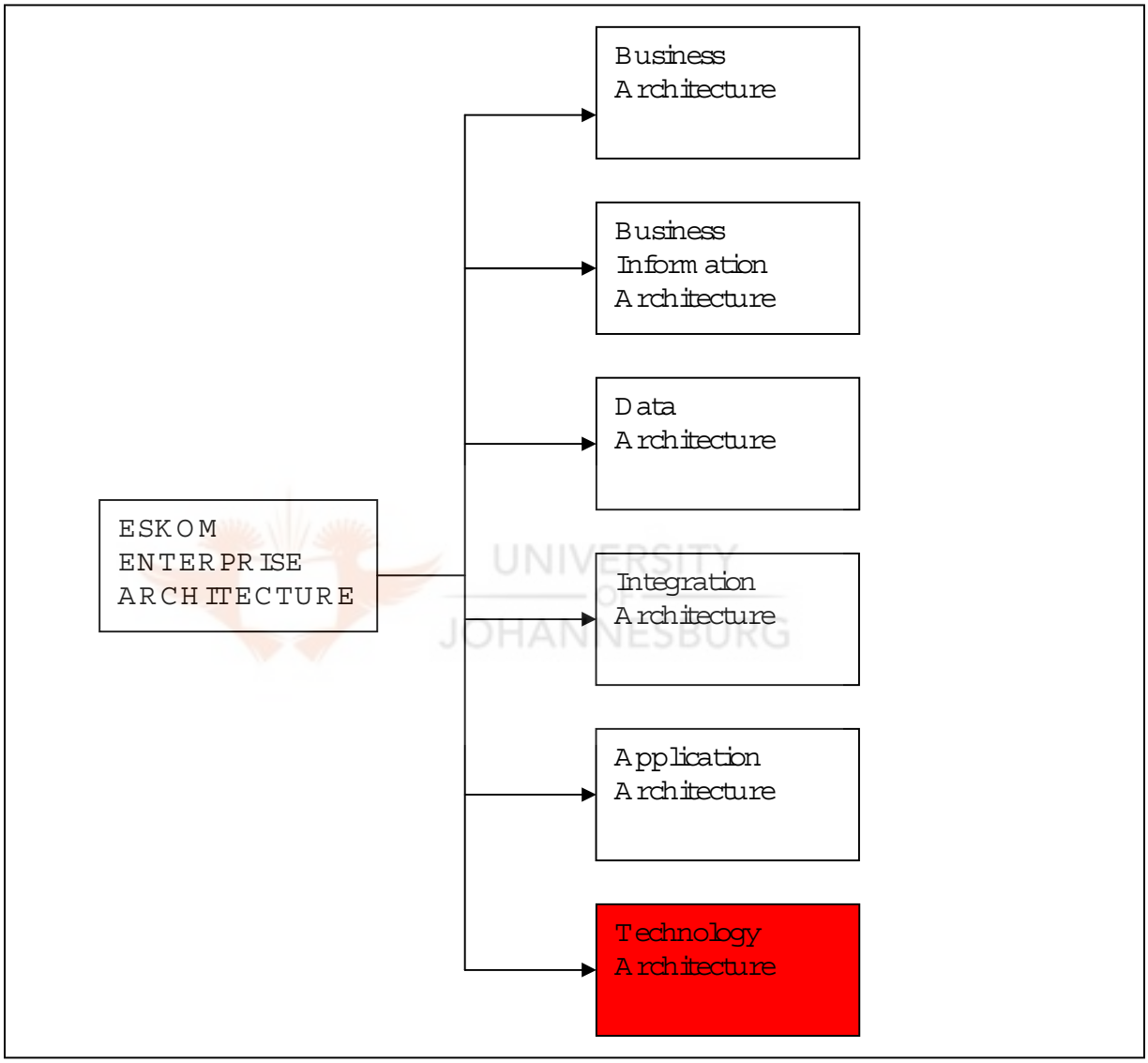


Figure 2.2.6

The Technology Architecture defines how the hardware and software components of the distributed environment will be implemented and managed. The planning, operation and management of an IT

infrastructure requires the combination of functions, standard methods, data, human resources and technology.

As discussed in the Business Architecture in the previous section, the Business Architecture provides the overarching guidelines and principles for Enterprise Architecture design. The Technology Architecture is designed within those guidelines and principles and directly supports the following business information requirement as defined in the Business Architecture that relates specifically to information security:

Protect information and business continuity

The Technology Architecture focuses on issues of configuration management, fault detection and isolation, testing, performance measurement, problem reporting, and software upgrades and control. It promotes uniformity and standardisation of hardware and software configurations, change control procedures, security measures, network and platform management, software distribution, asset management and performance management and capacity planning.

The Technology Architecture requirements are formulated in terms of the functions necessary to achieve the objectives of reliability, stability, accessibility and capacity of operations.

The functions are as follows:

- **Configuration management**
- **Operations**
- **Monitoring**
- **Administration services**
- **Planning**
- **Control**

The Technology Architecture specification lists a number of functional requirements under each of the above functions. However, only the information security related functional requirements will be extracted and presented below.

2.2.6.1 Configuration management

- **Ability to access and update the asset inventory system**
- **Ability to create and maintain profiles for user groups**
- **Ability to add, modify and delete users from the system**
- **User ID and password management**

2.2.6.2 Operations

- **Ability to manage sensitive data**
- **Ability to check authorisation**
- **Data encryption capability**
- **Ability to perform user security checking during start-up**
- **Ability to support virus checking**
- **Ability to determine the space available**
- **Ability to support all environments for backup and restore**
- **Ability to ensure that a file can be only backed up/restored by users with the right access level**
- **Ability to maintain security levels while performing backup/restore through encryption/decryption and validation of file security against the user's security level**
- **Ability to encrypt/decrypt information**
- **Ability to check security levels from remote operations**
- **Ability to restore system service(s) after a failure has occurred**
- **Disaster recovery**
- **Ability to provide secure physical access to equipment and media**
- **Ability to control user access to authorised applications and data**
- **Ability to protect data from operational negligence or virus infection**
- **Ability to keep security logs**
- **Ability to prevent theft/sabotage by users/hackers**

2.2.6.3 Monitoring

- **Ability to perform incident management**

2.2.6.4 Planning

- **Ability to determine physical data processing volumes for capacity modelling and planning**

2.2.6.5 Control

- **Ability to maintain a data model**
- **Ability to back up and archive the asset inventory system**

Section 2.2 discussed the components of the Enterprise Architecture. For each of the Enterprise Architecture components, principles and requirements related to information security were highlighted. While the Eskom Enterprise Architecture was used to discuss the components of the Enterprise Architecture, this mini dissertation is not motivating the Eskom Enterprise Architecture. Criticism of the Enterprise Architecture itself is therefore not relevant.

In the next section, the principles and requirements that were identified in Section 2.2 will be used to identify the information security implications and services that will be required to satisfy those principles.

2.3 Security requirements for the Enterprise Architecture

2.1	**Definition of Enterprise Architecture**
2.2	**Components of Enterprise Architecture for Eskom**
2.3	**Security requirement for the Enterprise Architecture**
2.4	**Alignment of an Information Security Architecture with an Enterprise Architecture**
2.5	**Conclusion**

The previous section discussed the components of the Eskom Enterprise Architecture and highlighted the principles relating to each of the components.

In this section the implications of the principles for each of the Eskom Enterprise Architecture components will be highlighted. The purpose of the implications is to assist in the identification of the security services.

2.3.1 Security implications based on the principles

This section summarises the relevant security implications as identified under each component of the Enterprise Architecture in Section 2.2.

The Business Architecture	
1	**Protect information and business continuity**
Business Information Architecture	
1	**The data users and information processes must be identified, authenticated and leveraged.**
2	**An information custodianship must be established.**
3	**Foster a culture that recognises the importance for and integrity of high quality data.**
4	**Pertinent information must be made available.**
5	**Open sharing of information must be balanced against confidentiality of business strategies.**
6	**Need for common definitions of information to simplify access and sharing.**
7	**Existing and prospective information sources must be investigated for accuracy and reliability.**
8	**An Information Inventory must be created.**
9	**An Information Confidentiality Register must be created.**
10	**An Information Business Criticality Register must be created.**
11	**The security audit procedures around information changes must allow for many levels of security with a suitable level of granularity.**
12	**Centralised data warehouses will increasingly supplant application databases as information sources for knowledge workers.**
13	**Additional information manipulation and presentation tools will be needed to cater for new information formats.**
14	**The uses and value of information must be assessed and measured according to pre-set targets.**
15	**The deployment or adaptation of technology, business structures and processes must explicitly capture unstructured and tacit intellectual capital in a secure, easily accessible and organised format.**
16	**Intellectual capital pertaining to business processes must be catered for and captured into the information systems architecture.**
17	**Mechanisms must be acquired or adapted to support the increased focus on information security.**
18	**Information ownership issues must be identified and resolved.**
19	**Information must be classified in terms of the access to information act.**
20	**The mechanisms necessary to support the access to information act and other legislation must be acquired.**

Data Architecture	
1	Data analysis and design must be done before developing application software or purchasing packages.
2	Accurate business definitions of data must be provided.
3	Security requirements for data must be defined.
4	Jobs must be defined to include responsibility and tasks concerning data quality and management.
5	Many users need access to latest changes in data
6	A high volume of data is shared across locations and need to be consistent across all locations.
7	Replicating frequent updates to distributed databases increases systems complexity and network traffic.
8	Contents of databases must be regularly reviewed.
9	Unintended redundancy of data must be reduced.
10	Achieve better performance, availability, reliability and scalability.
11	Facilitate data backup and recovery.
12	Updates should occur through the source where the data originates to simplify data management.
13	Data for public access should be put outside the firewall.
14	Data definitions and data models should be available and kept up-to-date.
15	Consensus of stakeholders on data definitions will be required.
16	Data design should be integrated in the appropriate stages of the application system development cycle.
Integration Architecture	
1	Security functions, example encryption must be available.
2	Authentication and authorisation for application to application access
Application Architecture	
1	Security authentication.
2	Security authorisation.
Technology Architecture	
1	Ability to access and update the asset inventory system.
2	Ability to create and maintain profiles for user groups.
3	Ability to add, modify and delete users from the system.
4	User ID and password management.
5	Ability to manage sensitive data.
6	Ability to check authorisation.
7	Data encryption capability.
8	Ability to perform user security checking during start-up.
9	Ability to support virus checking.
10	Ability to determine the space available.
11	Ability to support all environments for backup and

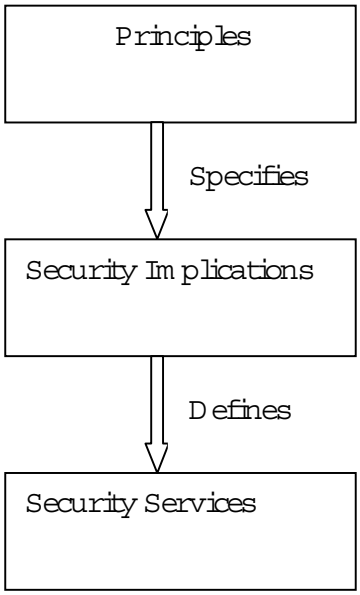
	restore.
12	**Ability to ensure that a file can be only backed up/restored by users with the right access level.**
13	**Ability to maintain security levels while performing backup/restore through encryption/decryption and validation of file security against the user's security level.**
14	**Ability to encrypt/decrypt information.**
15	**Ability to check security levels from remote operations.**
16	**Ability to restore system service(s) after a failure has occurred.**
17	**Disaster recovery.**
18	**Ability to provide secure physical access to equipment and media.**
19	**Ability to control user access to authorised applications and data.**
20	**Ability to protect data from operational negligence or virus infection.**
21	**Ability to keep security logs.**
22	**Ability to prevent theft/sabotage by users/hackers.**
23	**Ability to perform incident management.**
24	**Ability to determine physical data processing volumes for capacity modelling and planning.**
25	**Ability to maintain a data model.**
26	**Ability to back up and archive the asset inventory system.**

Figure 2.3.1

This section highlighted the security implications arising from the principles from the Business Architecture, Information Architecture, Data Architecture, Integration Architecture, Application Architecture and Technology Architecture components of the Eskom Enterprise Architecture.

In the next section, the author will identify the key information security services that will be required to address the security implications identified in Section 2.2 and summarised in Section 2.3.1.

The approach followed is described by the schematic below:



2.3.2 Identification of security services

This section will identify some of the key information security services that will be required to address the implications of the principles specified in the previous section. The identification of security services is necessary because according to the ISF [4], "Security services are typically used in the development of security architecture to indicate the type of security functionality required to protect the IT infrastructure components".

Using the security implications discussed in the previous section, the author has identified some of the information security services that will be required from an Information Security Architecture to address the security implications specified in the previous section. Table 2.3.3 lists these security services. It should be acknowledged that this is not necessarily a complete list of all possible security services that will be required by the Enterprise Architecture, but is as comprehensive as was possible within this investigation.

2.3.3 Security Services

The information security services that are listed below in Table 2.3.3 will be used in Chapter 5 as the basis to assess and identify an

Information Security Architecture framework that can best address the development and provision of the security services required by the Enterprise Architecture. The security services were derived from the implications that were summarised in Section 2.3.1. Table 2.3.3 lists the Security Services, which is based on the experience of the author, a description of the security services and a mapping to the implication that the security service is related to.

Security Services		Description	Implication
A	Identification and authentication services	This service deals with the identification and authentication of users and processes. The identification is concerned with assigning, managing and storing digital identities. The authentication is related to verifying the identity of a user or process.	The data users and information processes must be identified, authenticated and leveraged. (Implication 1 within the Business Information Architecture in Section 2.3.1)
B	Authorisation services	This service deals with granting and preventing access to resources. It is concerned with the process flow from beginning to end showing how a user requests access to the application, indicating the associated security controls and separation of duties.	Ability to control user access to authorised applications and data. (Implication 19 within the Technology Architecture in Section 2.3.1)
C	Access control services	This service addresses user registration and deregistration, issuing of user IDs, creating privileges or permissions based	Ability to create and maintain profiles for user groups. Ability to add, modify and delete users from the system. User Id and password

		upon the users job functions and responsibilities.	**management.** **(Implications 2, 3 and 4 within the Technology Architecture in Section 2.3.1)**
D	**Non-repudiation services**	**This service provides assurance that when a message is sent by a sending party to a recipient it is important to prevent the sender from later attempting to deny that the message was sent or the recipient later denying that the message was received.**	**Ability to manage sensitive information.** **(Implication 5 within the Technology Architecture in Section 2.3.1)**
E	**Security policy services**	**This service covers the creation and agreement of policies and standards. Policies can be of two types, technical and procedural.**	**An information custodianship must be established.** **(Implication 2 within the Business Information Architecture in Section 2.3.1)**
F	**Backup and recovery services**	**This service covers the backing up of business data and the ability to recover the business data following some type of failure or disaster.**	**Ability to support all environments for backup and restore.** **(Implication 11 within the Technology Architecture in Section 2.3.1)**
G	**Disaster recovery services**	**This service deals with recovery plans and procedures to ensure that a business system continues to function after a**	**Disaster recovery.** **(Implication 17 within the Technology Architecture in**

		failure or disaster. It is supported by data recovery and restoration procedures.	**Section 2.3.1)**
H	**Cryptographic services**	**This service plays a role in securing information through the implementation of cryptography in confidentiality, integrity, authentication and non-repudiation services.**	**Data encryption capability.** **(Implication 7 within the Technology Architecture in Section 2.3.1)**
I	**Audit services**	**This service ensures that there is historical evidence of activity for monitoring purposes or forensic examination purposes. It also includes the protection of the audit trail itself.**	**The security audit procedures around information changes must allow for many levels of security with a suitable level of granularity.** **(Implication 11 within the Business Information Architecture in Section 2.3.1)**
J	**Compliance services**	**This service ensures that there is regulatory and policy compliance, covering government and industry regulations and corporate policies.**	**Information must be classified in terms of the access to information act. The mechanisms necessary to support the access to information act and other legislation must be acquired.** **(Implication 19 within the Business Information Architecture in Section 2.3.1)**
K	**Security Awareness services**	**This service is concerned with**	**Foster a culture that recognises the**

		raising and developing ongoing awareness campaigns to create a strong information security culture across the organisation.	**importance for and integrity of high quality data.** **(Implication 3 within the Business Information Architecture in Section 2.3.1)**
L	**Security domain services**	**This service ensures that security elements belonging to a common group are subject to a common security policy.**	**Need for common definitions of information to simplify access and sharing.** **(Implication 6 within the Business Information Architecture in Section 2.3.1)**
M	**Middleware security services**	**This service deals with security issues in the integration layer of the infrastructure.**	**Security functions, example encryption must be available.** **(Implication 1 within the Integration Architecture in Section 2.3.1)**
N	**Data management security services**	**This service is concerned with the provision of security controls within the databases.**	**Ability to maintain a data model.** **(Implication 25 within the Technology Architecture in Section 2.3.1)**
O	**Network security services**	**This service is concerned with the provision of security controls within the network.**	**Ability to perform user security checking during start up.** **(Implication 8 within the Technology Architecture in Section 2.3.1)**

P	**Platform security services**	**This service is concerned with the provision of security controls within the individual physical platforms, example servers and workstations.**	**Ability to determine physical data processing volumes for capacity modelling and planning.** **(Implication 24 within the Technology Architecture in Section 2.3.1)**

Table 2.3.3

This section identified some key security services that should be included in an Information Security Architecture to address the security implications of the Enterprise Architecture components. Having identified the security services, the next section will discuss how an Information Security Architecture should align with an Enterprise Architecture

2.4 Alignment of Information Security Architecture with an Enterprise Architecture

2.1	**Definition of Enterprise Architecture**
2.2	**Components of Enterprise Architecture for Eskom**
2.3	**Security requirements for an Enterprise Architecture**
2.4	**Alignment of an Information Security Architecture with an Enterprise Architecture**
2.5	**Conclusion**

In section 2.2, the Enterprise Architecture of Eskom was discussed. The Enterprise Architecture was shown to comprise of the following architectures:

- **Business Architecture**
- **Information Architecture**
- **Data Architecture**
- **Integration Architecture**
- **Application Architecture**
- **Technology Architecture**

The security implications of the principles and requirements for each of the Enterprise Architecture components were also identified and specified.

In section 2.3, some of the security services were identified that would be required by an Information Security Architecture to address the security implications of the architecture components of the Enterprise Architecture.

This section discusses the author's view on how an Information Security Architecture should align with an Enterprise Architecture so that it will be able to provide the security services to the Enterprise Architecture.
No real literature as far as this aspect is concerned, could be identified. This section is therefore fully based on the author's experience and ideas.

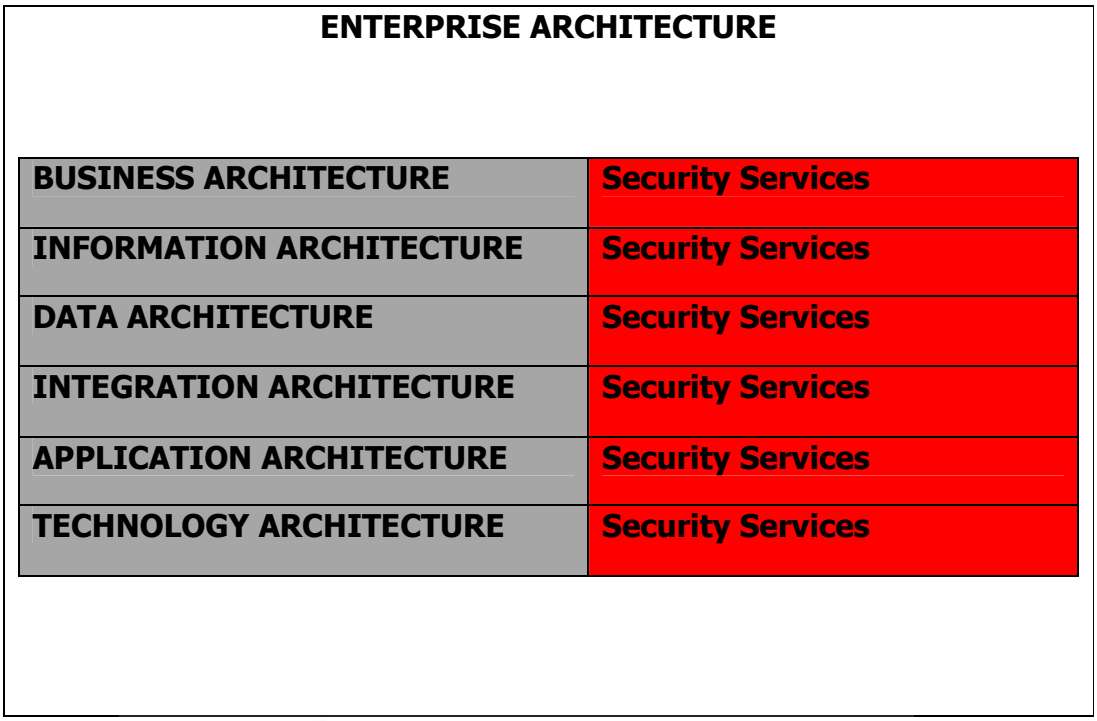


Figure 2.4.1

Figure 2.4.1 above illustrates that the Information Security Architecture must provide specific information security services to each of the Enterprise Architecture components, based on the principles and requirements of each component.

However, there are security services that are common to all the Enterprise Architecture components, example cryptography services and authentication services. This relationship is reflected in the Figure 2.4.2 below.

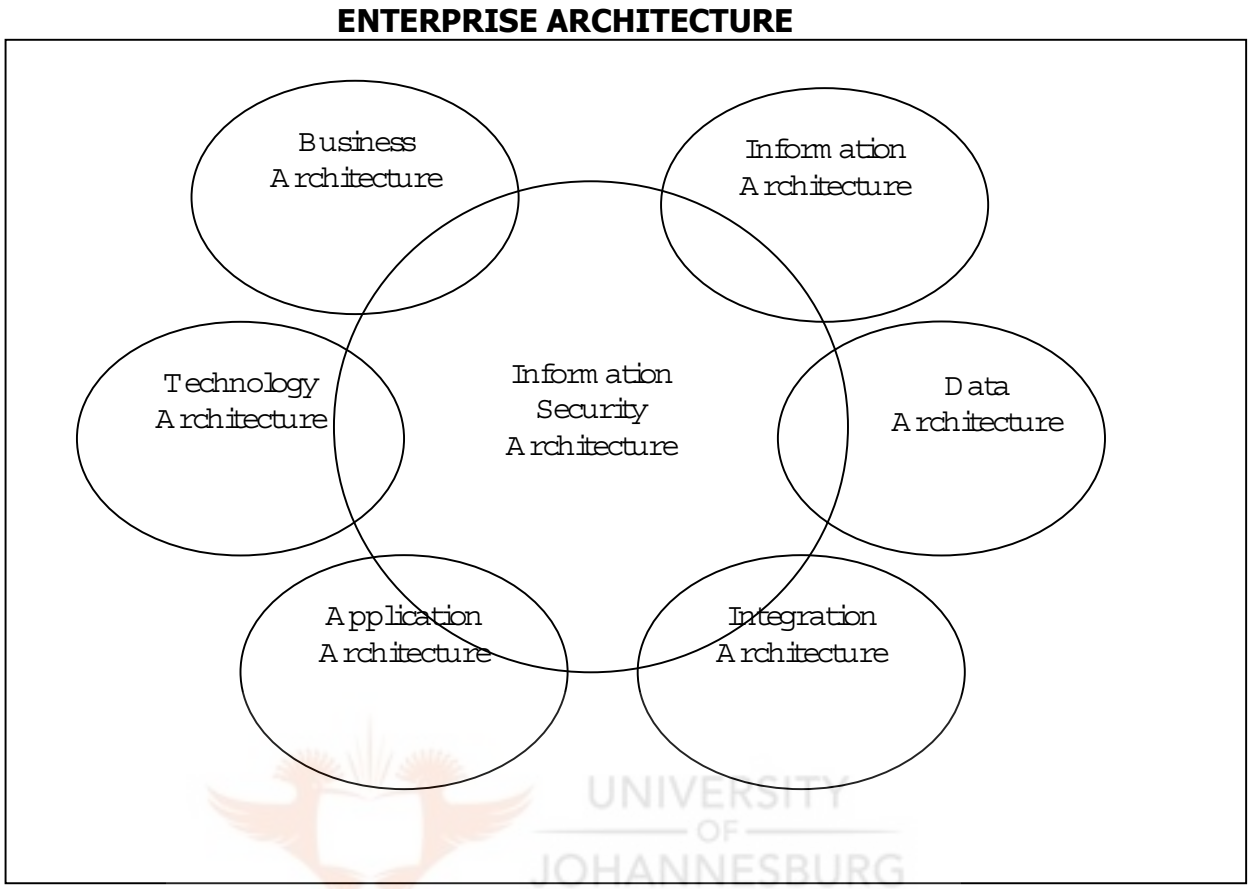


Figure 2.4.2

Figure 2.4.2 above reflects that while an Information Security Architecture must provide specific security services to each of the Enterprise Architecture components, an Information Security Architecture will also provide common security services that will be required by all the Enterprise Architecture components.

The above graphic also illustrates that the Enterprise Architecture will influence the development of an Information Security Architecture by providing the architecture direction, principles and standards. An Information Security Architecture should therefore fully align with the Enterprise Architecture.

2.5 Conclusion

2.1	**Definition of Enterprise Architecture**
2.2	**Components of Enterprise Architecture for Eskom**
2.3	**Definition of information security architecture**
2.4	**Alignment of an Information Security Architecture with an Enterprise Architecture**
2.5	**Conclusion**

This chapter provided the background for this dissertation by providing an overview of the Eskom Enterprise Architecture, in terms of its definition, its components, security requirements for each of the architecture components and security services to address the security requirements. The chapter also discussed how an Information Security Architecture should align with the Enterprise Architecture.

The next chapter, Chapter 3, will begin a discussion of some current Information Security Architecture models and frameworks.

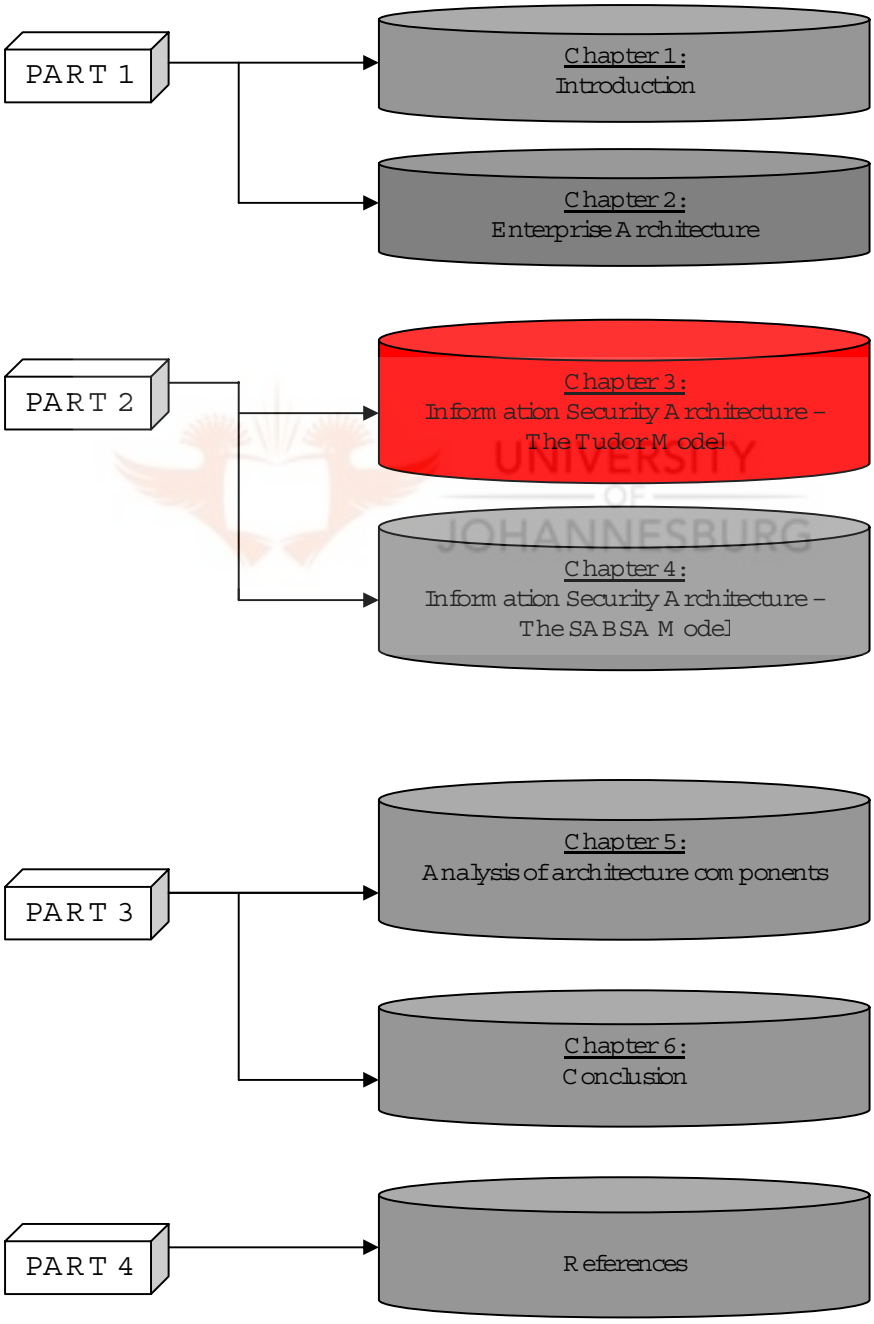
The purpose of this description is to identify the model or framework that best aligns with the Enterprise Architecture security requirements.

The next chapter, Chapter 3, will begin with a description of the Tudor Model.

PART 2

Chapter 3

THE TUDOR MODEL



Chapter 3

The objective of this chapter is to identify and describe the components in the Information Security Framework proposed by Tudor [1]. This chapter consists of the following headings:

3.1 Introduction

3.1	**Introduction**
3.2	**Components of the Tudor Framework**
3.3	**Tudor Model Component Security Activities**
3.4	**Conclusion**

The Tudor Framework proposes five components that are considered essential to an effective security architecture.

The components included in the Framework are:

Security organisation and infrastructure
Security Policies, Standards and Procedures
Security Baselines and Risk Assessments
Security Awareness and Training Programs
Compliance
Security Technology

Table 3.1

The Framework recommends that it is necessary to consider all of the components in order to develop an effective security plan. A deficiency or lack of emphasis in any one of these areas provides a weakness that can be exploited in the architecture and throughout the organisation.

3.2 Components of the Tudor Framework

3.1	Introduction
3.2	Components of the Framework
3.3	Tudor Model Component Security Activities
3.4	Conclusion

This section will provide a description of each component.

3.2.1 Security organisation and infrastructure

3.2.1	Security organisation and infrastructure
3.2.2	Security Policies, Standards and Procedures
3.2.3	Security Baselines and Risk Assessments
3.2.4	Security Awareness and Training Programs
3.2.5	Compliance
3.2.6	Security Technology

A strong, highly visible and flexible security organisation should be established, that is supported by executive management. This component will provide the framework for increasing security awareness, minimising information security risk and providing the management structure for implementing and supporting security solutions. The security organisation will be influenced by the size of the organisation, the systems environment, the organisational structure of the enterprise and the involvement of executive management.

3.2.2 Security Policies, Standards and Procedures

3.2.1	Security organisation and infrastructure
3.2.2	Security Policies, Standards and Procedures
3.2.3	Security Baselines and Risk Assessments
3.2.4	Security Awareness and Training Programs
3.2.5	Compliance
3.2.6	Security Technology

This section describes the security policies, standards and procedures component of the Framework.

3.2.2.1 Policies

Security policies are the foundation of the Enterprises Information Security Architecture. Their purpose is to inform all users about the expectations of management regarding the appropriate use of information, systems and resources throughout the enterprise. The information security policy should:

- **Describe in written format what executive management is trying to achieve, the policy objective.**
- **Include the policy scope, responsibilities, and management's intention for implementing it.**
- **Address security activities that include designing controls into application systems, establishing user access privileges, performing risk analysis, conducting investigations of computer crimes and disciplining workers for security violations.**

3.2.2.2 Standards

Security standards are designed for more efficient and consistent operation and should reflect industry best practices. Standards should:

- **Be a specific set of rules or conventions that are agreed upon between parties in order to operate more uniformly and effectively.**
- **Set a level of expectation that must be reached or exceeded in order to fulfil ones obligations or responsibilities.**

3.2.2.3 Procedures

Security procedures document the best way of performing a function. Procedures should:

- **Provide consistency of operations between individuals who perform the same job, and are most important when the primary administrator is unavailable and a backup must take over responsibilities.**
- **Allow for more knowledgeable and smoother transition during permanent changes of staff.**

3.2.3
Security Baselines and Risk Assessments

3.2.1	**Security organisation and infrastructure**
3.2.2	**Security Policies, Standards and Procedures**
3.2.3	**Security Baselines and Risk Assessments**
3.2.4	**Security Awareness and Training Programs**
3.2.5	**Compliance**
3.2.6	**Security Technology**

This section describes the Security Baselines and Risk Assessments component of the Framework.

A program for understanding and managing risk must be developed. For new systems or systems that have not been assessed, a preliminary assessment called a baseline is performed. Because the security posture is unknown, a baseline provides a starting point to measure changes in configurations and improvements to the system. From this baseline, periodic risk assessments provide the current state and effectiveness of controls within that system for a given period of time. Assessments are a mechanism to identify the strengths and implemented controls of a system, not just the weaknesses and risks.

Security baselines should be performed on all components of the operating environment. Initially, a high level assessment should be performed to gain an understanding of the management of the systems environment. The high-level overview provides an understanding of the level of effort and priority that has been placed on security within the organisation.

3.2.4 Security Awareness and Training Programs

3.2.1	**Security organisation and infrastructure**
3.2.2	**Security Policies, Standards and Procedures**
3.2.3	**Security Baselines and Risk Assessments**
3.2.4	**Security Awareness and Training Programs**
3.2.5	**Compliance**
3.2.6	**Security Technology**

This section describes the Security Awareness and Training Programs component of the Framework.

Awareness and training are the most significant elements in an information security program. The security awareness and training program is designed to help reduce the risk of losing intellectual property and processing resources. The program transfers the responsibility to protect these resources to each individual.
To be successful, the program needs to be multi-faceted and consistent with the predominant enterprise culture. It also has to be fun.
Awareness and training are two distinct methods of transferring knowledge about information security.
Training is more formalised, typically in a classroom or conference setting where the objective is to gain knowledge about a particular subject.
Awareness is a passive mechanism that occurs through less formal methods such as posters, themes, and objects such as key rings and cups.

3.2.5 Compliance

3.2.1	**Security organisation and infrastructure**
3.2.2	**Security Policies, Standards and Procedures**
3.2.3	**Security Baselines and Risk Assessments**
3.2.4	**Security Awareness and Training Programs**
3.2.5	**Compliance**
3.2.6	**Security Technology**

This section describes the Compliance component of the Framework.

Compliance measures the extent to which defined policies, standards and procedures are being followed. Compliance includes auditing, monitoring, and investigating at several levels of the enterprise. There are three levels of compliance, level 1 that involves the information owner or individual assigned responsibility for the component, level 2 that involves the audit function, level 3 that involves the security team or committee.

3.2.6 Security Technology

3.2.1	**Security organisation and infrastructure**
3.2.2	**Security Policies, Standards and Procedures**
3.2.3	**Security Baselines and Risk Assessments**
3.2.4	**Security Awareness and Training Programs**
3.2.5	**Compliance**
3.2.6	**Security Technology**

This section describes the Security Technology component of the Framework.

Organisations must rely on strong security technologies to preserve the integrity and confidentiality of business assets and processing resources. Some of these technologies include encryption, public key infrastructure, firewalls, virtual private networks, one time passwords and smartcards, remote access servers, and biometrics.

This section concludes the identification and description of the security components of the Tudor Model.

The next section identifies the security activities of each of the components in the Tudor Model. The security activities that are identified will be used in Chapter 5 to assess to what extent the Tudor Model meets the requirements of the Eskom Enterprise Architecture Model.

3.3 Tudor Model Component Security Activities

3.1	**Introduction**
3.2	**Components of the Tudor Framework**
3.3	**Tudor Model Component Security Activities**
3.4	**Conclusion**

In this section the author will define the security activities provided by each of the components of the Tudor Model. The author has derived the security activities from the operational outputs of each of the components of the Tudor Model. These security activities are therefore not in any way related to the security services defined for the Enterprise Architecture in Section 2.3.3. The purpose in defining these Tudor Model security activities is to be able to compare these security activities with the security services that were defined for the Enterprise Architecture in Section 2.3.3. This method was chosen by the author because it provides a platform to assess to what extent the Tudor Model fits the Enterprise Architecture, based on the security activities provided by the Model. The assessment of the Tudor Model against the Enterprise Architecture will be discussed in Chapter 5.

3.3.1 Information Security activities of the Tudor Security Organisation and Infrastructure component

Tudor Component	Tudor Component Security Activity	Description of activity
Security Organisation	**Management Structure**	**This activity will provide the management structure for implementing and supporting security solutions.**
	Trained security personnel	**This activity will ensure that trained personnel are used to carry out security.**
	Creating and maintaining an Information Security Architecture	**This activity provides for the creation and the maintaining of an Information Security Architecture.**
	Ownership of	**This activity defines and documents**

	system components.	**the responsibilities relating to ownership and custodianship of information assets.**
	Data Classification	**This activity uses a risk-based approach to classifying resources. It involves the system and information owners to identify what the enterprise views as important, crucial or sensitive. The classification determines the level of controls to be implemented.**
	Inventory of the operating environment.	**This activity produces an inventory of all applications, operating systems, databases and networks in the operating environment.**

Table 3.3.1

3.3.2 Information Security activities of the Tudor Security Policies, Standards, and Procedures component

Tudor Component	Tudor Component Security Activity	Description of activity
Security Policies, Standards, and Procedures	**Developing and implementing policies, standards and procedures.**	**This activity covers the development and implementation of information security policies, standards and procedures.**
	Updating of policies, standards and procedures.	**This activity reviews and updates the information security policies, standards and procedures on a regular basis.**
	Security Standards and Procedures Manual (SS&PM)	**This activity develops the SS&PM.**

Table 3.3.2

3.3.3 Information Security activities of the Security Baselines and Risk Assessments component.

Tudor Component	Tudor Component Security Activity	Description of activity

Security Baselines and Risk Assessments	**Performance of security risk assessments on the management of security programs developed and security responsibilities.**	**This activity performs high-level risk overviews to identify the areas of increased risk within and to understand the level of risk that exists within the operating environment. The areas covered in the workplan includes the following areas:**
		• **Assessing the Organisation of the Security Function includes:**
		  ○ **Individuals performing security functions**
		  ○ **Reporting lines and segregation of responsibility.**
		  ○ **Security mission and charter.**
		• **Assessing the Security Plan includes:**
		  ○ **Alignment to goals and objectives of the Strategic IT Plan.**
		• **Assessing Security Policies, Standards and Procedures includes:**
		  ○ **Security management and administration.**
		  ○ **Information access control.**
		  ○ **User identification and authentication.**
		  ○ **Data ownership.**
		  ○ **Security monitoring.**
		  ○ **Compliance testing.**
		  ○ **Software licensing.**
		  ○ **Physical security.**
		  ○ **Report storage, distribution and destruction procedures.**
		  ○ **Penalties and measures for non-compliance.**
		  ○ **Compliance enforcement mechanisms**
		• **Assessing Risk-related Programs includes:**
		  ○ **Classification methodologies.**

		○ **Business impact analysis(BIA).** ○ **Incident and emergency reporting and response.** ○ **Disaster Recovery planning(DRP)** ○ **Business continuity planning(BCP).**
	Performance of security risk assessments at the platform component level and develop Security baselines .	**This activity performs risk assessments of the operational security pograms. The areas covered are:** ○ **Security Monitoring includes:** ○ **Suspected Access violations.** ○ **Attempted system intrusions.** ○ **Audit trails** ○ **Computer Virus Controls includes:** ○ **Workstations.** ○ **Servers.** ○ **Firewalls.** ○ **Microcomputer Security includes:** ○ **Software licensing.** ○ **Physical and logical security.** ○ **Backup and contingency plans** ○ **Compliance with Legal and regulatory requirements includes:** ○ **Compliance with regulatory requirements .** ○ **Compliance with legislation protcting information.** ○ **Appropriate protection of classified data.** ○ **Guidelines on retention, storage, and handling of regulated information.**
	Performance of security risk assessments at the computer operations level and develop Security baselines .	**This activity performs risk assessments of the computer operations level. The areas covered are:** ○ **Physical and Environmental Security includes:** ○ **Physical access to computing facilities.** ○ **Pro-active measures against**

		natural disasters. **o Computer facilities location.** **o Environmental controls including UPS, air conditioning, fire detection and suppression.** **o Backup and Recovery includes:** **o Frequency of backups.** **o Off-site storage and security procedures for off-site backup.** **o Back-up processing locations.** **o Back-up Recovery plan testing.** **o Computer Systems Management includes:** **o Daily execution and maintaince of systems, applications and information.** **o Operational procedures.** **o Operational logs.** **o Operator access to pograms and source code.** **o Problem Management includes:** **o Problem resolution.** **o Reduction of failures.** **o Reduction of the impact on service.**
	Performance of security risk assessments at the application controls level and develop Security baselines .	**This activity performs risk assessments at the application controls level. The areas covered are:** **o Access Control** **o Role based access.** **o Access of users, administrators and programmers to application data, functionality, system files, program modules and hardware resources.** **o Access Control lists.** **o Authorisation of resources.** **o Identification and Authentication.** **o Availability.** **o Confidentiality.**

		○ **Integrity.** ○ **Segregation of Duties.** ○ **Audit Trails.** ○ **Application system utilities.** ○ **Application development and implementation.** ○ **Change Management.**
	Performance of security risk assessments at the Database security level and develop Security baselines .	**This activity performs risk assessments at the Database security level. The areas covered are:** ○ **Database type.** ○ **Database access.** ○ **Authorisation.** ○ **Inference.**
	Performance of security risk assessments at the Network level and develop Security baselines .	**This activity performs risk assessments at the Network level. The areas covered are:** ○ **Remote Acess.** ○ **Intranets.** ○ **Extranets.** ○ **Internet.** ○ **Local Area networks (LANs)** ○ **Metropolitan area networks (MANs)** ○ **Wide area networks (WANs)** ○ **Gateways separating the Corporate WAN and Lines of Business.** ○ **Internet gateways.** ○ **Virtual private Networks (VPNs)** ○ **Value added networks (VANs)**
	Performance of security risk assessments at the Operating System level and develop Security baselines .	**This activity performs risk assessments at the Operating System level. The areas covered are:** ○ **Security policies.** ○ **System configuration.** ○ **System change control.** ○ **Domains and trust relationships.** ○ **Networking.** ○ **Remote access.** ○ **Physical access.** ○ **Log-on and log-off controls.** ○ **User management.** ○ **Group management.** ○ **Password management.** ○ **Directory and file system security.**

		○ System privileges and utilities. ○ Maintenance and operations. ○ Auditing, logging and monitoring. ○ Backup and recovery. ○ Security administration.
	Performance of security risk assessments at the Telecommunications level and develop Security baselines .	This activiy performs risk assessments at the Telecommunications level. The areas covered are: ○ Voice networks. ○ PBX. ○ Mobile communications. ○ Teleconferencing. ○ Voice mail.
	Security baselines	This activity developes security baselines that provide the mechanism for understanding the lecel of risk that exists within an organisation.a starting point to measure changes in configurations and improvements.

Table 3.3.3

3.3.4 Information Security activities of the Security Awareness and Training Program component.

Tudor Component	Tudor Component Security Activity	Description of activities
Security Awareness and Training Program	Development and implementation of a security awareness and training program.	This activity covers the following areas: ○ Employees recognising their responsibility for protecting the organisation's information assets. ○ Employees understanding the value of information security. ○ Employees recognising potential violations and know who to contact. ○ The level of security awareness among existing employees remains high.

Table 3.3.4

3.3.5 Information Security activities of Compliance component.

Tudor Component	Tudor Component Security Activity	Description of activity
Compliance	Measure the extent to which policies, standards and procedures are being followed.	This activity covers the following areas: ○ Ensuring that the information owner or individual assigned responsibility for the component has put in place appropriate preventative and detective controls. ○ Conduct audits to ensure compliance with policies, standards and procedures. ○ Ensuring that the Security team is implementing security organisation-wide.

Table 3.3.5

3.3.6 Information Security activities of the Technology component

Tudor Component	Tudor Component Security Activity	Description of activity
Technology	Encryption Services	This activity is the process of making readable information unreadable through the use of mathematical conversion or processes.
	Public Key Infrastructure (PKI) services	This activity provides the infrastructure surrounding public key cryptography and it includes the management policies, programs, procedures, communications protocols, and processes for the creation, use, distribution, storage, and destruction of the key pairs.
	Firewall services	This activity provides the software or hardware necessary to validate and authenticate traffic and users

		against a security policy or set of rules to allow them to pass to the private or trusted side of a network.
	Virtual Private Networks (VPN) services	**This activity employs existing network components to create a secure communications channel over public networking facilities.**
	One-time Passwords and Smart Cards services	**This activity provides a secure method of authenticating a user through the use of a credit card type device that generates a password for a very short period. Smart cards can be used to generate the one-time passwords.**
	Remote Access services	**This activity provides the capability of assessing internal processing resources from a connection outside the processing environment.**
	Biometrics	**This activity provides methods for the identification of an individual using measurable physical characteristics of the human body as evidence of a user's identity.**

Table 3.3.6

3.4 Conclusion

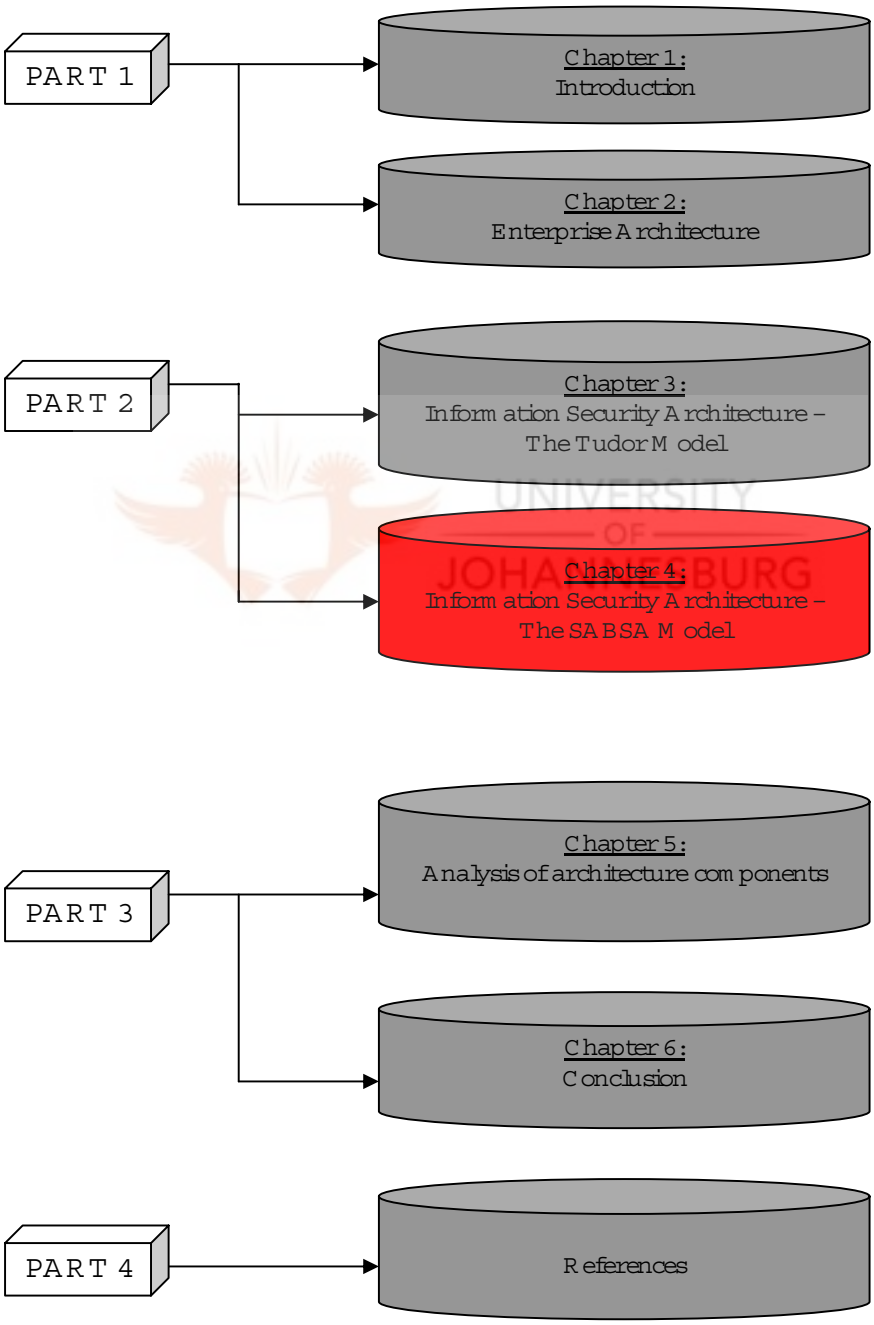
3.1	**Introduction**
3.2	**Components of the Tudor Framework**
3.3	**Tudor Model Security Services**
3.4	**Conclusion**

This chapter described the components of the Information Security Framework by J.K. Tudor. There are six components in the Framework. Each of the components was described. Based on each of the components, the security activities of each of the components were identified and described. These security activities will be used in Chapter 5 to assess whether the Tudor Model meets the security architecture requirements of the Eskom Architecture Model.

The next chapter, Chapter 4, will describe the Sherwood Applied Business Security Architecture (SABSA) model by Sherwood, Clark and Lynas.

CHAPTER 4

The Sherwood Applied Business Security Architecture Model (SABSA)



CHAPTER 4

The objective of the chapter is to identify and describe the components in the Sherwood Applied Business Security Architecture (SABSA) [2]

The chapter consists of the following headings:

4.1 Introduction

4.1	**Introduction**
4.2	**Components of the SABSA Framework**
4.3	**SABSA Framework Component Security Activities**
4.4	**Conclusion**

According to SABSA [2], it is a framework for an Information Security Architecture and Service Management used successfully by numerous high-profile organisations around the world. The Framework has evolved since 1995 as a holistic business-driven approach for delivering cohesive security solutions to business and government. SABSA ensures that the needs of an enterprise are met completely and that security services are designed, delivered and supported as an integral part of the business and IT management infrastructure.

SABSA is a model and a methodology for developing risk-driven Enterprise Information Security Architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.

The process analyses the business requirements at the outset, and creates a chain of traceability through the strategy and concept, design, implementation, and ongoing manage and measure phases of the lifecycle to ensure that the business mandate is preserved. Framework tools support the whole methodology.

The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction and detail is developed, going through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and finally at the lowest layer, the selection of technologies and products (component architecture).

The SABSA model itself is generic and can be the starting point for any organisation, but by going through the process of analysis and decision-making implied by its structure, it becomes specific to the enterprise, and is finally highly customised to a unique business model. It becomes in reality the enterprise security architecture, and it is central to the success of a strategic programme of information security management within the organisation.

4.2 Components of the Framework

4.1	**Introduction**
4.2	**Components of the SABSA Framework**
4.3	**SABSA Framework Component Security Activities**
4.4	**Conclusion**

The components of the SABSA architecture framework will be discussed under the following components:

The SABSA Model
The SABSA Matrix
SABSA Development Process
SABSA Lifecycle

4.2.1	**The SABSA Model**
4.2.2	**The SABSA Matrix**
4.2.3	**SABSA Development Process**
4.2.4	**SABSA Lifecycle**

4.2.1 The SABSA Model

The SABSA Model comprises six layers, which is highlighted in the table below. Each layer represents the view of a different player in the process of specifying, designing, constructing and using the business system.

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

Table 4.1 The SABSA Model for Security Architecture Development

Following is a description of each of these six architecture layers:

4.2.1.1 Contextual Security Architecture - The Business View

In the SABSA model, the business view is called the Contextual Security Architecture. It is a description of the business context in which the enterprise's secure systems must be designed, built and operated.

The Contextual Security Architecture is concerned with:

- **The business, its assets to be protected (brand, reputation etc) and the business needs for information security. It answers the question of what are the business requirements.**
- **The business risks expressed in terms of assets, goals, success factors and the threats, impacts and the vulnerabilities that put these at risk, driving the need for business security. It answers the question of why is the security necessary.**

- **The business processes that require security. It answers the question of how security will be integrated into the business processes.**
- **The organisational aspects of business security . It answers the question of who must be involved and impacted by the security.**
- **The business geography and location-related aspects of business security. It answers the question of where security will be necessary.**
- **The business time dependencies and time-related aspects of business security in terms of both performance and sequence. It answers the question of when security will be required.**

4.2.1.2 Conceptual Security Architecture - The Architect's Vew

The architect's view is the overall concept by which the business requirements of the enterprise may be met. Thus this layer of the architectural model is also referred to as the Conceptual Security Architecture. It defines principles and fundamental concepts that guide the selection and organisation of the logical and physical elements at the lower layers of abstraction.

The Conceptual Security Architecture is concerned with:

- **What you want to protect, expressed in the SABSA Model in terms of a SABSA Business Attributes Profile.**
- **Why the protection is important, in terms of control objectives.**
- **How you want to achieve the protection, in terms of high-level technical and management security strategies.**
- **Who is involved in security management, in terms of entity relationship models, and the trust framework within which entities interact with one another.**
- **Where you want to achieve the protection concepualised in terms of security domains.**
- **When is the protection relevant, in terms of both points in time and periods of time.**

4.2.1.3 Logical Security Architecture - The Designer's View

The designer's view involves the identification and specification of the logical architectural elements of an overall system. This view models the business as a system, with system components that are themselves sub-systems. It shows the major architectural security elements in terms of logical security services, and describes the logical flow of control and the relationship

between these logical elements. It is therefore also known as the Logical Security Architecture.

The Logical Security Architecture is concerned with:

- **Business information as a logical representation of the real business. It is this business information that needs to be secured. It answers the what.**
- **Specifying the security policy requirements for securing business information. It answers the why.**
- **Specifying the logical security services and how they fit together as common re-usable building blocks into a complex security system that meets the overall business requirements. It answers the how.**
- **Specifying the entities and their inter-relationships, attributes, authorised roles and privilege profiles in the form of a schema. It answers the who.**
- **Specifying the security domains and inter-domain relationships. It answers the where.**
- **Specifying the security processing cycle. It answers the when.**

4.2.1.4 Physical Security Architecture - The Builder's View

The builders view involves turning logical abstractions that describe the system to be built into a Physical Security Architecture model that describes the actual technology model and specifies the functional requirements of the various system components. The logical security services are now expressed in terms of the physical security mechanisms and machines that will be used to deliver these services.

The Physical Security Architecture is concerned with:

- **Specifying the business data model and the security-related data structures. It answers the what.**
- **Specifying rules that drive logical decision-making within the system. It answers the why.**
- **Specifying security mechanisms and the physical machines upon which these mechanisms will be hosted. It answers the how.**
- **Specifying the people dependency in the form of the users, the applications that they use and the security user interface. It answers the who.**
- **Specifying security technology infrastructure. It answers the where.**
- **Specifying the time dependency in the form of execution control structures .It answers the when.**

4.2.1.5 Component Security Architecture – The Tradesman's View

The tradesman view is one of an integrator that joins products together during an implementation of the design. Some of these products are hardware-related, some are software-related, and some are service oriented. The integrator works with a series of components that are hardware items, software items, and interface specifications and standards. Hence this layer of the architectural model is also called the Component Security Architecture.

The Component Security Architecture is concerned with:

- **Data field specifications, address specifications and other detailed data structure specifications. It answers the what.**
- **Security standards. It answers the why.**
- **Products and tools, both hardware and software. It answers the how.**
- **User identities, privileges, functions, actions and acces control lists. It answers the who.**
- **Computer processes, node addresses, and inter-process protocols. It answers the where.**
- **Security step timings and sequencing. It answers the when.**

4.2.1.6 Operational Security Architecture - The Facilities Manager's View

The facilities managers view is to deal with the operation of the system and its various services, maintaining it in good working order, and monitoring how well it is performing in meeting the requirements. The framework for doing this is called the Operational Security Architecture.

The Operational Security Architecture is concerned with the following:

- **Ensuring the operational continuity of the business systems and information processing, and maintaining the security of operational business data and information. It answers the what.**
- **To manage operational risks and hence to minimise operational failures and disruptions. It answers the why.**
- **Performing specialised security-related operations. It answers the how.**
- **Providing operational support for the security-related needs of all users and their applications. It answers the who.**
- **Maintaining the system integrity and security of all operational platforms and networks. It answers the where.**
- **Scheduling and executing a timetable of security-related operations. It answers the when.**

4.2.1.7 Configuration of the six layers

The figure below shows another configuration of the six layers provided by SABSA [2]. In the diagram, the operational security architecture has been placed vertically across the other five layers. This is because operational security issues arise at each and every one of the other five layers. Operational security has a meaning in the context of each of these other layers.

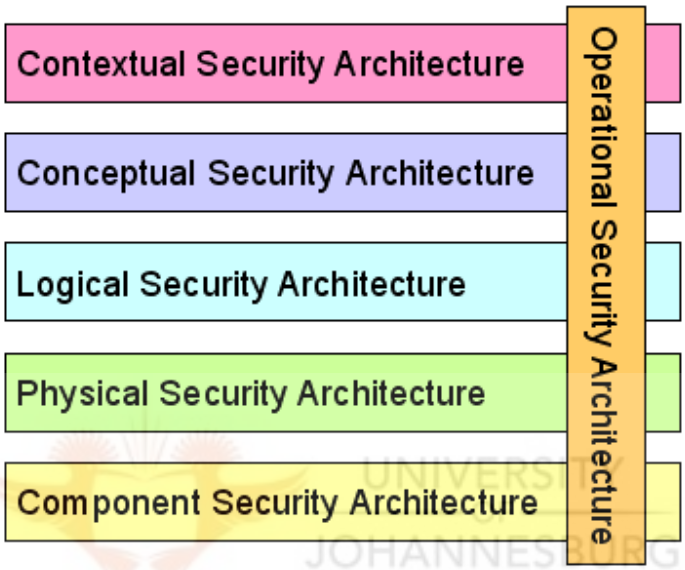


Table 4.2 The SABSA Model for Security Architecture Development

For each of the six layers above, SABSA provides a matrix, called The Sabsa Matrix, that can be used for detailed analysis of the six layers. Below is a description of the SABSA Matrix.

4.2.2 The SABSA Matrix

4.2.1	**The SABSA Model**
4.2.2	**The SABSA Matrix**
4.2.3	**SABSA Development Process**
4.2.4	**SABSA Lifecycle**

For detailed analysis of each of the six layers, the SABSA Matrix uses What, Why, When, How, Where and Who? For each horizontal layer there is a vertical analysis as follows:

- ***What*** **are you trying to do at this layer? – The assets to be protected by your security architecture.**
- ***Why*** **are you doing it? – The motivation for wanting to apply security, expressed in the terms of this layer.**
- ***How*** **are you trying to do it? – The functions needed to achieve security at this layer.**
- ***Who*** **is involved? – The people and organisational aspects of security at this layer.**
- ***Where*** **are you doing it? – The locations where you apply your security, relevant to this layer.**
- ***When*** **are you doing it? – The time-related aspects of security relevant to this layer.**

These six vertical architectural elements are summarised for all six horizontal layers. This gives a 6 x 6 matrix of cells, which represents the whole model for the enterprise security architecture. It is called the SABSA Matrix (see Table 4.3 below). If the issues raised by each and every one of these cells can be addressed, then the entire range of questions to be answered will be covered, and there will be a high level of confidence that the security architecture is complete. The process of developing an enterprise security architecture is a process of populating all of these thirty-six cells.

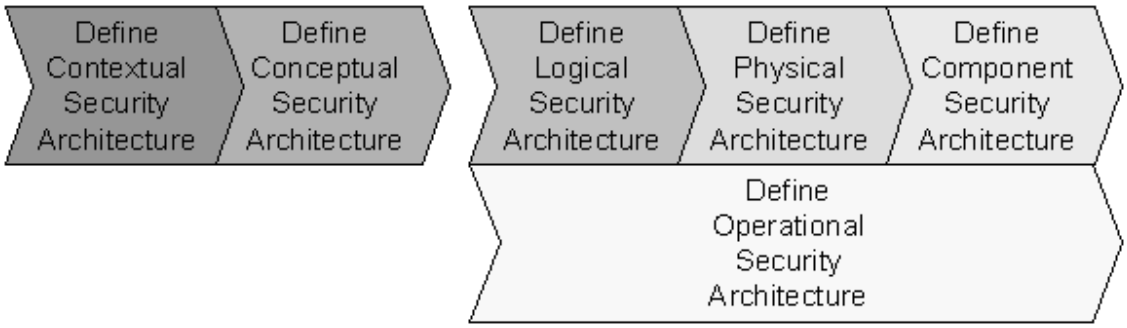
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Table 4.3 The SABSA Matrix for Security Architecture Development

4.2.3 SABSA Development Process

4.2.1	**The SABSA Model**
4.2.2	**The SABSA Matrix**
4.2.3	**SABSA Development Process**
4.2.4	**SABSA Lifecycle**

The SABSA Model provides the basis for an architecture development process, since it is clear that through understanding the business requirements, the architect can create the initial vision. This is used by the designers to create the detailed design, which in turn is used by the builder to construct the systems, with components of various sorts provided by specialists. Finally, the facilities manager operates the finished system, but unless the earlier phases take account of the operational needs, this phase in the lifetime of the system will be fraught with difficulty. The development process itself is shown, at a high level, in the following diagram.



The SABSA Development Process

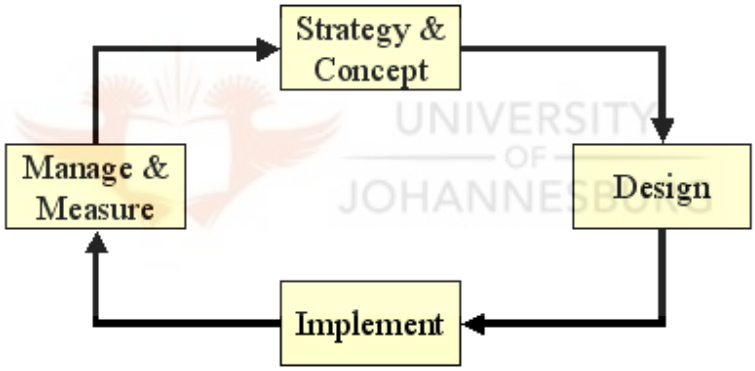
The high-level development process (see diagram above) indicates that there is a natural break after the first two phases. Once the Contextual Architecture and the Conceptual Architecture are agreed and signed off, then work on the later phases can begin, with considerable parallel working. However, it is difficult to make useful progress on the later stages until these first two are fairly fully defined. The temptation to go straight to an implementation of certain products and tools should be avoided, since this is the source of so many severe problems during the operational phase.

It is also important not to be confused by the positioning of the sub-process 'Define Operational Security Architecture'. The Operational Security Architecture itself cuts across all of the other five layers, but the development process for that Operational Security Architecture is best delayed until after the Contextual and Conceptual Security Architectures have been defined and signed off.

4.2.4 SABSA Lifecycle

4.2.1	**The SABSA Model**
4.2.2	**The SABSA Matrix**
4.2.3	**SABSA Development Process**
4.2.4	**SABSA Lifecycle**

The SABSA Lifecycle is designed to align with the IT Lifecycle. Whatever the scope, the SABSA Framework provides a structured approach for successful delivery. Whether the challenges of service management, enterprise-wide architecture, designing the infrastructure for a new business initiative, implementing a single IT project, or complying with governance and compliance directives, the SABSA Lifecycle will provide the roadmap for success.



The SABSA Lifecycle

In the SABSA Lifecycle, the first two phases of the SABSA Development Process are grouped into an activity called 'Strategy & Concept'. This is followed by an activity called 'Design', which embraces the design of the logical, physical, component and operational architectures. The third activity is 'Implement', followed by 'Manage and Measure'. The significance of the 'Measure' activity is that early in the process the target performance metrics is set. Once the system is operational, it is essential to measure actual performance against targets, and to manage any deviations observed. Such management may simply involve the manipulation of operational parameters, but it may also feed back into a new cycle of development.

This section concludes the identification and description of the security components of the SABSA Framework.

The next section identifies the security services that are provided by each of the components in the SABSA Framework. The security services that are identified will be used in Chapter 5 to assess to what extent the SABSA Framework meets the requirements of the Eskom Enterprise Architecture Model.

4.3 SABSA Framework Component Security Activities

4.1	Introduction
4.2	Components of the Framework
4.3	SABSA Framework Component Security Activities
4.4	Conclusion

In this section the author will define the security activities provided by each of the components of the SABSA Framework. The author has derived the security activities from the Contextual, Conceptual, Logical, Physical and Component Architecture layers as outlined in Table 4.3 of The SABSA Matrix. The security activities that are introduced have been extracted by the author from the description provided of each of the architecture layers from the SABSA Framework for all 36 cells. The reason for choosing the cells of the SABSA Matrix is that it provides a representation of the whole model for the SABSA Framework.

These security activities are therefore not in any way related to the security services defined for the Enterprise Architecture in Section 2.3.3. The purpose in defining these SABSA Framework security activities is to be able to compare these security activities with the security services that were defined for the Enterprise Architecture in Section 2.3.3. This method was chosen by the author because it provides a platform to assess to what extent the SABSA Framework fits the Enterprise Architecture, based on the security activities provided by the Framework. The assessment of the SABSA Framework will be discussed in Chapter 5.

Tables 4.3.1 – 4.3.5 have three columns. The first column consists of the SABSA output obtained from the SABSA Matrix in table 4.3. Column two

consists of the security activities associated with the SABSA output. The security activities have been extracted by the author from the description provided of each of the architecture layers from the SABSA Matrix in table 4.3 for all 36 cells. Column three consists of a description of the security activity.

4.3.1 Information Security activities at the SABSA Contextual Security Architecture layer

SABSA Matrix output	SABSA Component Security Activity	Description of activity
The Business	**Business requirements collection**	**This activity provides for:** • **Identifying the business needs for information security.** • **Identifying new business activities enabled by information and communications technology.** • **Leveraging the value of information.** • **Security implications for doing electronic business.** • **Security requirements for ensuring operational continuity and stability.** • **Identifying security requirements for safety-critical systems where failure may cause injury or death to human beings.** • **Idntifying security requirements for systems assurance.**

Business Risk Model	**Business Risk Assessment**	**This activity provides for:**
		• **Risk assesments that looks at the following key areas where the organisation faces risk and a security response should be developed:**
		  ○ **Brand protection;**
		  ○ **Fraud prevention;**
		  ○ **Loss prevention;**
		  ○ **Business continuity;**
		  ○ **Legal obligations;**
		  ○ **Confidence of stakeholders;**
		  ○ **Operational risk that covers the loss resulting from inadequate or failed internal processes, people and systems.**

Business Process Model	**Security for business processes**	**This activity provides for:**
		• **Identifying the security requirements that are driven by business processes. This will include:**
		  ○ **Business interactions where entity identification and authentication is required.**
		  ○ **Business communications.**

Business Organisation and Relationships	**Organisation and relationships affecting business security needs**	**This activity will provide for:**
		• **Examining the following to derive the business drivers and business requirements:**
		  ○ **Management hierarchies and their effect on authorisation, governance and control.**
		  ○ **Integration of supply chains to determine the trusted interactions between suppliers and customers.**
		  ○ **3rd Party service providers.**
		  ○ **Strategic partnerships.**
		  ○ **Joint ventures.**
		  ○ **Mergers, acquisitions and divestments.**

Business Geography	**Location dependence of business security needs**	**This activity will provide for:** • **Identifying the locations of the business, its customers and suppliers.** • **Identifying remote working modes.**

Business Time Dependencies	**Time dependency of business security needs**	**This activity will provide for:**
		• **Identifying the time related business drivers, eg.:**
		  • **Business transaction turnaround times.**
		  • **Business transaction lifetime.**
		  • **Business deadlines.**
		  • **Record retention times.**
		  • **Response to customers.**
		  • **Time to market.**

Table 4.3.1

4.3.2 Information Security activties at the SABSA Conceptual Security Architecture layer

SABSA Matrix output	SABSA Component Security Activity	Description of activities
Business Attributes Profile	**Conceptualising business assets that need protection.**	**This activity provides for:** • **Identifying business drivers** • **Mapping business attributes to business drivers** • **Setting up metrics framework for measurement**
Control Objectives	**Security Audits & assurance Levels.**	**This activity provides for:** • **Using control objectives to conceptualise mitigation strategies to address business risks.**
Architectural layering	**Multi-layered security.**	**This activity provides for:** • **Examining conceptual multi-layered models for security.** • **Examining multi-tiered incident handling models.** • **Providing for a security infrastructure layered architecture that caters for:** o **Security services in the Application layer.** o **Security services in the Middleware layer.** o **Data management security services.** o **Security services in the Network layer.** o **Security services in the Processing Platform layer.**
Security Strategies	**Security Service Management Strategy**	**This activity provides for:** • **Managing security services strategy, including:** o **Provisioning of security parameters for user privileges, application systems, embedded systems.** o **Security operations.** o **Security monitoring.** o **Security incident**

		management. ○ Security vulnerability management. • Securing management services strategy, including: ○ Authorisations. ○ Segregation of duties. ○ Authentication. ○ Access Control. ○ System assurance strategy. ○ Directory services strategy.
Security Entity Model and Trust Framework	**Security entities and security entity relationships.**	**This activity provides for:** • **Identifying security entities.** • **Identifying security entity relationships.** • **Understanding and modelling trust.**
Security Domain Model	**Security Domain Management**	**This activity provides for:** • **Identifying scurity elements that are subject to a common security policy.**
Security-Related Lifetimes and Deadlines	**Security Operation Schedule Management**	**This activity provides for:** • **Identifying lifetimes and deadlines, including:** ○ **Registration lifetimes.** ○ **Certification lifetimes.** ○ **Cryptographic key lifetimes.** ○ **Policy lifetimes.** ○ **Password lifetimes.** ○ **Token lifetimes.**

Table 4.3.2

4.3.3 Information Security activities at the SABSA Logical Security Architecture layer

SABSA Matrix output	SABSA Component Security Activity	Description of activities
Business Informational Model	**Business information and transaction protection.**	**This activity provides for:** **Using the Business Attributes Profile and identifying the protection required for business information, including:** o **Confidentiality protection.** o **Integrity protection.** o **Availability protection.** o **Authentication of source.** o **Non-repudiation.** **Identifying the special security needs for transaction processing, including:** o **Business user identification.** o **Business user authentication.** o **Business user authorisation.** o **Business entity authentication.** o **Business transaction integrity protection.** o **Business transaction authentication.** o **Business transaction non-repudiation.**
Security Policies	**Security Policy architecture**	**This activity provides for:** **The definition of the security policies and the security policy architecture.**
Security Services	**Layered model of security services**	**This activity provides for:** **The identification of security services within the following categories of services:** o **Prevention services:** o **Entity Security Services:** ▪ **Directory services** ▪ **Authentication** ▪ **Authorisation** o **Communication Security Services:** ▪ **Authentication** ▪ **Message Integrity**

		▪ Message Confidentiality ▪ Privilege management ▪ Physical security ▪ Environmental security ▪ Non-repudiation o Application and System Security Services ▪ Authorisation ▪ Access Control ▪ Data integrity ▪ Data confidentiality ▪ Software integrity ▪ Data replication & backup ▪ User interface o Security Management Services. ▪ Policy management ▪ Training & awareness ▪ Security Operations ▪ Security provisioning ▪ Security monitoring o Containment services. o Entity authorisation o Stored data confidentiality o Software integrity o Physical security o Training and awareness o Detection and notification services. o Intrusion detection o Event collection and event tracking services. o Recovery and restoration services. o Incident response o Data backup o Software backup o Disaster Recovery o Assurance services. o Audit trails o Security audit o Security monitoring
Entity Schema & Privilege Profiles	**Data rules directory**	**This activity provides for: Identification and specification of rules that determine what data can be stored in databases.**
Security	**Security domain**	**This activity provides for:**

Domain Definitions & Associations	**definition**	**The definition of the security domains that will include:** ○ **Network Domains** ○ **Middleware Domains** ○ **Application Domains** ○ **Security Service Management Domains**
Security Processing Cycle	**Security processing cycles**	**This activity provides for :** **The documentation of security management activities, including manual and automated processes.**

Table 4.3.3

4.3.4 Information Security activities at the SABSA Physical Security Architecture layer

SABSA Matrix output	SABSA Component Security Activity	Description of activities
Business Data Model	**Physical organisation and management of data.**	**This activity considers the security of the following:** **o File structures, including record structures and field structures.** **o File management tools, including directory management.** **o Database structures.** **o Database management systems.**
Security Rules, Practices and procedures	**Rules, practices and procedures.**	**This activity turns the security policies identified in the Logical Security Architecture into sets of rules, into practices and procedures.**
Security Mechanisms	**Mapping of Physical Security Mechanisms to Security Services.**	**This activity provides for:** **The mapping of the physical security mechanisms to the Security Services that was established in the Logical Security Architecture.**
Users, Applications, and User Interface	**Security mechanisms to implement application-level securuty services.**	**This activity maps the security mechanisms related to user and application security. The mechanisms include:** **Directory Mechanisms.** **Central Access Manager Mechanisms.** **Database Mechanisms.** **File System Mechanisms.** **Operating System Mechanisms.** **Application Mechanisms.** **User Authentication Mechanism.** **Password Management.**
Platform and Network Infrastructure	**Security mechanisms used to provide security within the platform and network infrastructure.**	**This activity maps the security mechanisms related to platfom and network security. In includes:** **Resilient configurations.** **Performance and Capacity Planning.** **Platform Security.** **Hardware Security.** **Network topology.** **Directory Topology.**

Control Structure Execution	**Security mechanisms for implementing control points.**	**This activity looks at the security mechanisms to implement control points in security processes to enforce the security related time constraints and sequence constraints.**

Table 4.3.4

4.3.5 Information Security activities at the SABSA Component Security Architecture layer

SABSA Matrix output	SABSA Component Security Activity	Description of activities
Detailed Data Structures	Syntax rules and protocols	This activity ensures that data structures are standardised to ensure that components from different vendors have the capability of being plugged together to build integrated structures.
Security Standards	Standardisation	This activity ensures that standards are adopted to enable component integration.
Security Products and Tools	Listing of features of security products and tools.	This activity provides a listing of the features of security products and tools.
Identities, Functions, Actions and ACL's	Functional protocol standards and their applications.	This activity identifies the protocol standards used to build the infrastructure.
Process, Modes, Addresses and Protocols	Security related protocols.	This activity provides the security related protocols and describes how they fit into the hierarchical protocol stack.
Security Step Timing and Sequencing	Timing and sequencing of security steps.	This activity describes how the timing and sequencing steps relating to the business requirements will be met in practice, eg user expectations, business deadlines and volume throughput frequirements.

Table 4.3.5

4.4 Conclusion

4.1	**Introduction**
4.2	**Components of the Framework**
4.3	**SABSA Framework Component Security Activities**
4.4	**Conclusion**

This chapter described the components of the SABSA model. The components included:
The SABSA Model
The SABSA Matrix
SABSA Development Process
SABSA Lifecycle

The SABSA Matrix was used to identify security activities for each of the architecture layers and their components. These security activities will be used in Chapter 5 to assess whether and to what extent the SABSA Framework fits the security services requirements of the Eskom Enterprise Architecture.

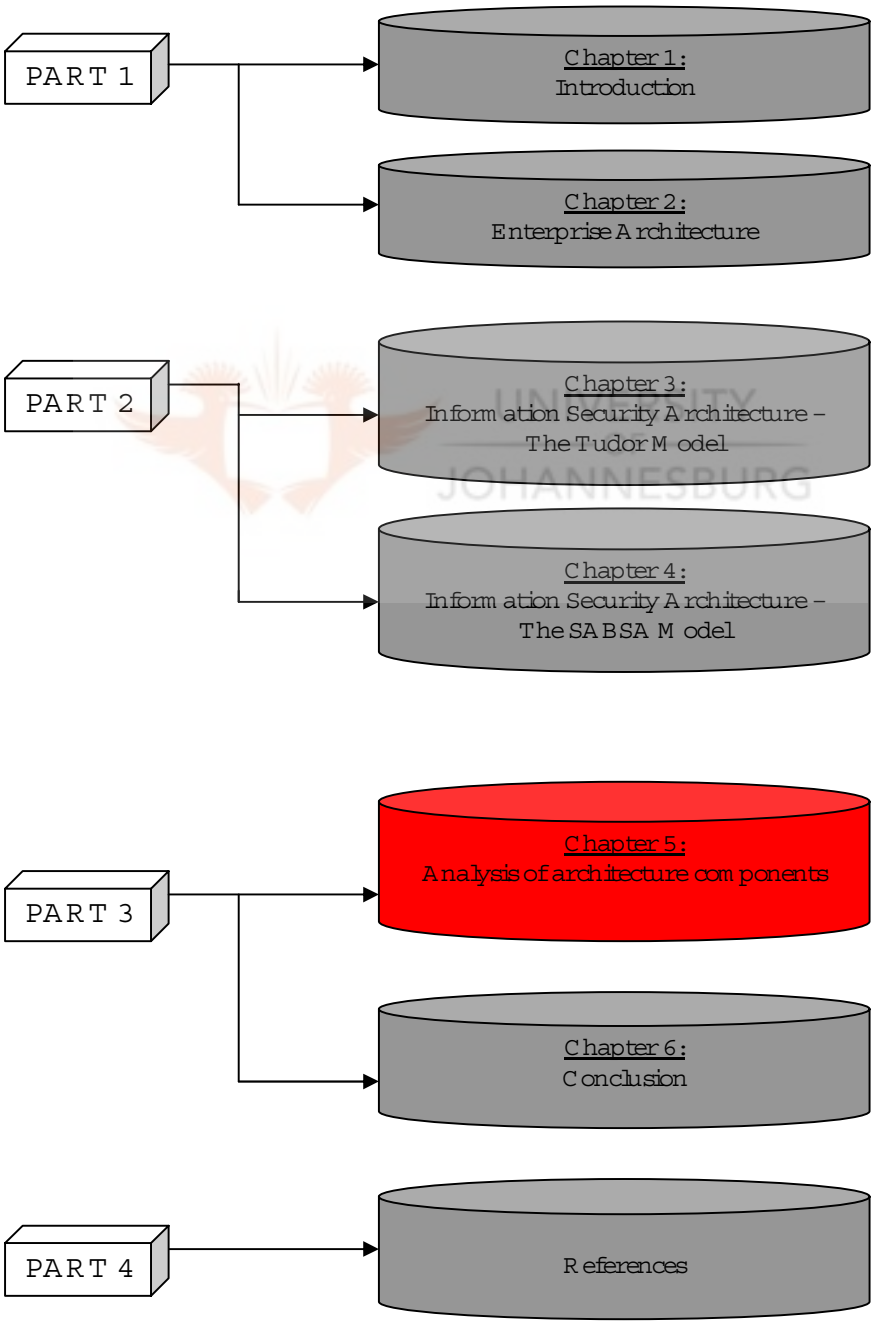
In Chapter 2, security services were extracted from the principles and implications of the Enterprise Architecture. In Chapter 3, security activities were extracted from the components of the TUDOR Architecture Model. In Chapter 4, security activities were extracted from the components of the SABSA Architecture Model.

The next Chapter, Chapter 5, is part of PART 3. In this Chapter, a comparison will be made between the security activities provided by the two Architecture Models and the security services of the Enterprise Architecture. This is where the real "mapping" takes place.

Part 3

Chapter 5

ANALYSIS OF ARCHITECTURE SECURITY SERVICES



Chapter 5

The chapter consists of the following headings:

5.1 Introduction

5.1	**Introduction**
5.2	**Assessment of the Tudor Model**
5.3	**Assessment of the SABSA Framework**
5.4	**Conclusion**

This chapter will assess to what extent the Information Security Architecture frameworks and models introduced in Chapters 3 and 4 meet the security services requirements of the Enterprise Architecture, introduced in Chapter 2.

The approach that will be followed is the security services requirements from the Enterprise Architecture, introduced in Chapter 2 will be used as a basis to assess the security activities of the Information Security Architectures discussed in Chapter 3 and Chapter 4. The assessment will identify the extent to which the Information Security Architecture component security activities are able to meet the security requirements of the Enterprise Architecture. The result of the assessment will inform Eskom as to which of the Information Security Architecture frameworks fits the best.

5.1.1 Rating Scale

A three point rating scale will be used for the assessment, as described below:

0	**The security requirement is not met**
1	**The security requirement is partly met**
2	**The security requirement is fully met**

5.1.2 Security Services required by the Enterprise Architecture

The security requirements introduced in Paragraph 2.3.3 in Chapter 2 will be used to assess the Tudor Model.

5.2 Assessment of the Tudor Model

5.1	**Introduction**
5.2	**Assessment of the Tudor Model**
5.3	**Assessment of the SABSA Framework**
5.4	**Conclusion**

This section will assess to what extent the security services required by the Enterprise Architecture model, introduced in Table 2.3.3 in Chapter 2, is met by the security activities provided by the Tudor Model security components, introduced in Table 3.3.1, Table 3.3.2, Table 3.3.3, Table 3.3.4, Table 3.3.5, and Table 3.3.6 in Paragraph 3.3, in Chapter 3. The security activities of each component in the Tudor Model will be ranked according to the rating scale to reflect to what extent the component security activities address the security services of the Enterprise Architecture. A motivation will be provided to justify the ranking for each of the component security activities.

5.2.1 Ranking of the Tudor Model component security activities against the Enterprise Architecture security services.

The table below uses the security services required by the Enterprise Architecture to rank the security activities of the Tudor Model components. Table 3.3.1 reflects the security activities associated with the Tudor Security Organisation and Infrastructure component, Table 3.3.2 reflects the security activities associated with the Tudor Security Policies, Standards, and Procedures component, Table 3.3.3 reflects the security activities associated with the Tudor Security Baselines and Risk Assessments component, Table 3.3.4 reflects the security activities associated with the Tudor Security Awareness and Training Program component, Table 3.3.5 reflects the security activities associated with the Tudor Compliance component and Table 3.3.6 reflects the security activities associated with the Tudor Technology component.

Enterprise Architecture		TUDOR Architecture Components security activities					
SECURITY SERVICES		TABLE 3.3.1	TABLE 3.3.2	TABLE 3.3.3	TABLE 3.3.4	TABLE 3.3.5	TABLE 3.3.6
A	Identification and authentication services	0	0	2	0	0	0
B	Authorisation services	0	0	2	0	0	0
C	Access control services	0	0	2	0	0	0
D	Non-repudiation services	0	0	0	0	0	2
E	Security Policy services	0	2	0	0	0	0
F	Trusted recovery services	0	0	2	0	0	0
G	Disaster recovery services	0	0	2	0	0	0
H	Encryption services	0	0	0	0	0	2
I	Audit services	0	0	0	0	2	0
J	Compliance services	0	0	0	0	2	0
K	Security Awareness services	0	0	0	2	0	0
L	Security domain services	0	0	1	0	0	0
M	Middleware security	0	0	0	0	0	0

	services						
N	**Data management security services**	**0**	**0**	**2**	**0**	**0**	**0**
O	**Network security services**	**0**	**0**	**2**	**0**	**0**	**0**
P	**Platform security services**	**0**	**0**	**2**	**0**	**0**	**0**

Table 5.2.1

The total score for the Tudor Model is 29. This is obtained by adding the scores for each of the components.

5.2.2 Motivation for the rankings of each of the services.

A) Identification and Authentication services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Identification and Authentication services at the application controls, operating systems and network levels.

B) Authorisation services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Authorisation services at the application controls and database security levels.

C) Access Control services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Access Control services at the application controls, database and operating system security levels.

D) Non-repudiation services

This service is covered under the Technology component. It is ranked as 2 because the model provides for Non-repudiation services through the Public Key Infrastructure (PKI) services.

E) Security Policy services

The Security Policy services is referenced by the Security Policies, Standards and Procedures architecture component. The ranking for this component is 2

because the model addresses the areas of Security policies, standards and procedures and considers security policies as the foundation of an Enterprise Security Architecture.

F) Trusted recovery services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Trusted recovery services at the computer operations and operating system security levels.

G) Disaster recovery services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Disaster recovery services as part of the management of security programs and security responsibilities.

H) Encryption services

This service is covered under the Technology component. It is ranked as 2 because the model provides for Encryption services at the Technology encryption services level.

I) Audit services

This service is covered under Compliance. It is ranked as 2 because the model provides for Audit services to measure the extent to which policies, standards and procedures are being followed.

J) Compliance services

This service is covered under Compliance. It is ranked as 2 because the model provides for Compliance services that includes:

- **Ensuring that the information owner or individual assigned responsibility for the component has put in place appropriate preventative and detective controls.**
- **Conducting audits to ensure compliance with policies, standards and procedures.**
- **Ensuring that the Security team is implementing security organisation-wide.**

K) Security Awareness services

This service is covered under the Security Awareness and Training Program component. This component is ranked as 2 because the

component describes the elements for a security awareness program and a procedure for developing an awareness program.

L) Security domain services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 1 because the model provides Security domain services only at the operating system level.

M) Middleware security services

The Tudor model does not cover Middleware security services in any of the components.

N) Data management security services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Data management security services at the Database security level.

O) Network security services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Network security services at the Network security level.

P) Platform security services

This service is covered under Security Baselines and Risk Assessments. It is ranked as 2 because the model provides for Platform security services at the platform component security level.

5.2.3 Summary

In summary, the Tudor model, had a score of 29. This is obtained by adding the scores for each of the components.

The Tudor Model does provide for all the services required by the Enterprise Architecture, except for the Middleware services. The Tudor Model also includes security services that are not considered by the Enterprise Architecture.

5.3 Assessment of the SABSA Framework

5.1	**Introduction**
5.2	**Assessment of the Tudor Model**
5.3	**Assessment of the SABSA Framework**
5.4	**Conclusion**

This section will assess to what extent the security services required by the Enterprise Architecture model, introduced in Paragraph 2.3.3 in Chapter 2 is met by the security activities provided by the SABSA Framework architecture components security activities, introduced in Table 4.3.1, Table 4.3.2, Table 4.3.3, Table 4.3.4 and Table 4.3.5, in Paragraph 4.3 in Chapter 4. Each component security activity in the SABSA Framework will be ranked according to the ranking scale to reflect to what extent the component security activities address the security services of the Enterprise Architecture. A motivation will be provided to justify the ranking for each of the component security activities.

5.3.1 Ranking of the SABSA Model architecture components security activities against Enterprise Architecture security services.

The table below uses the security services required by the Enterprise Architecture to rank the security activities of the SABSA Model components.

Table 4.3.1 reflects the security activities associated with the SABSA Contextual security layer, Table 4.3.2 reflects the security activities associated with the SABSA Conceptual security layer, Table 4.3.3 reflects the security activities associated with the SABSA Logical security layer, Table 4.3.4 reflects the security activities associated with the SABSA Physical security layer and Table 4.3.5 reflects the security activities associated with the SABSA Component security layer.

Enterprise Architecture		SABSA architecture components security activities				
Security Services		TABLE 431	TABLE 432	TABLE 433	TABLE 434	TABLE 435
A	Identification and Authentication services	1	1	2	1	1
B	Authorisation services	1	1	2	1	1
C	Access control services	1	1	2	1	1
D	Non-repudiation services	1	1	2	1	1
E	Security Policy services	1	1	2	1	1
F	Backup and recovery services	1	0	2	0	0
G	Disaster recovery services	1	1	2	1	1
H	Cryptographic services	1	1	2	1	1
I	Audit services	0	0	2	1	1
J	Compliance services	1	1	2	1	0
K	Security Awareness	0	0	1	1	0

	services					
L	**Security domain services**	**0**	**0**	**1**	**2**	**1**
M	**Middleware security services**	**1**	**1**	**2**	**1**	**1**
N	**Data management security services**	**0**	**0**	**1**	**2**	**1**
O	**Network security services**	**0**	**0**	**1**	**2**	**1**
P	**Platform security services**	**0**	**0**	**1**	**2**	**1**

Table 5.3.1

The total score for the SABSA framework is 78. This is obtained by adding the scores for each of the components.

5.3.2 Motivation for the rankings of each of the services.

A) Identification and Authentication services

In the SABSA framework, Identification is the process of ensuring that each entity is uniquely identified and Authentication is the process of verifying identity.

This service is ranked as 1 in the SABSA Contextual Security Architecture component because the Business Process Model help to identify the security requirements relating to Identification and Authentication services.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because the Security Strategies and Architectural Layering help to examine the strategies and possibilities for Identification and Authentication services at a conceptual level.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services help to specify Identification and Authentication services independently of the physical mechanisms that might be used to deliver them. The specification is guided by the contextual and conceptual security architectures.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms help to map the Identification and Authentication services to the security mechanisms. A security mechanism is

a physical means by which the Identification and Authentication services are implemented.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provides a description of the security products used in the implementation of the Identification and Authentication services.

B) Authorisation services

In the SABSA framework, Authorisation refers to the process of granting a privilege.

This service is ranked as 1 in the SABSA Contextual Security Architecture component because Business Process Model help to identify the security requirements relating to Authorisation services.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Security Strategies and Architectural Layering help to examine the strategies and possibilities for Authorisation at a conceptual level.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services help to specify Authorisation services independently of the physical mechanisms that might be used to deliver them. The specification is guided by the contextual and conceptual security architectures.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms help to map the Authorisation services to the security mechanisms. A security mechanism is a physical means by which the Authorisation services are implemented.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the security products used in the implementation of the Authorisation services.

C) Access Control services

In the SABSA framework, Access Control is the process of making access decisions based on checking Authorisations and Authenticating identity.

This service is ranked as 1 in the SABSA Contextual Security Architecture component because Business Process Model help to identify the security requirements relating to Access Control services.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Security Strategies and Architectural Layering help to examine the strategies and possibilities for Access Control at a conceptual level.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services help to specify Access Control services independently of the physical mechanisms that might be used to deliver them. The specification is guided by the contextual and conceptual security architectures.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms help to map the Access Control services to the security mechanisms. A security mechanism is a physical means by which the Access Control services are implemented.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provides a description of the security products used in the implementation of the Access Control services.

D) Non-repudiation services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because Business Organisation and Relationships help to identify the security requirements relating to non-repudiation services that included trusted interactions between suppliers and customers, the trust model that represents them and the risk model associated with these relationship.

This service is ranked 1 in the SABSA Conceptual Security Architecture component because Security Entity Model and Trust Framework help to examine the strategies and possibilities for non-repudiation services at a conceptual level. A security entity is something or someone that can take actions in a business environment.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Entity Schema and Privilege Profiles help to specify non-repudiation services independently of the physical mechanisms that might be used to deliver them. The specification is guided by the contextual and conceptual security architectures.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Users, Applications and User Interface help to map the

non-repudiation services to the security mechanisms. A security mechanism is a physical means by which the non-repudiation services are implemented, example the directory mechanism.

This service is ranked as 1 in the SABSA Component Security Architecture component because Identities, Functions, Actions and ACL's provides a description of the security products used in the implementation of the non-repudiation services, example web services.

E) Security Policy services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because Business Risk Model help to identify the security requirements relating to security policy services that includes looking at some of the key areas where the enterprise faces risk and is motivated to develop an information security response.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Controlled Objectives help to examine the strategies and possibilities for security policy services at a conceptual level. It explains in detail how the control objectives are used as the key tool for conceptualising the mitigation strategy to address the identified business risks. Controls are implemented through policies, organisational structures, processes, practices and procedures and through technical systems.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Policies help to specify security policy services independently of the physical mechanisms that might be used to deliver them. The specification is guided by the contextual and conceptual security architectures. Security policies are statements of what type of security and how much should be applied to protect the business.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Rules, Practices and Procedures help to map the Security policy services to sets of rules, practices and procedures.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Standards provides a description of the security standards available.

F) Backup and recovery services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because in the collection of Business requirements, Security requirements for ensuring operational continuity and stability help to describe the set of business requirements for Backup and recovery services.

This service is ranked as 2 in the SABSA Logical Security Architecture component because included in the Layered model of security services, recovery and restoration services are considered. This service covers data backup, software backup and disaster recovery.

G) Disaster recovery services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because Business Risk Model help to describe the set of business requirements for business continuity at a high level.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Security Related Lifetimes and Deadlines help to partially explain the business needs and justifications to assist with the disaster recovery planning that will become part of the business continuity program.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services describes the mechanisms that support disaster recovery.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to disaster recovery.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of disaster recovery planning tools and products.

H) Cryptographic services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because in the collection of Business requirements, security requirements for security implications for doing electronic business help to describe the set of business requirements for Cryptographic services.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Security Related Lifetimes and Deadlines help to describe the business needs and justifications to assist with the Cryptographic key lifetimes.

This service is ranked as 2 in the SABSA Logical Security Architecture component because as part of the Layered model of security services, stored data confidentiality is described.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to Cryptographic services.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of Cryptographic services tools and products.

I) Audit services

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services describes the assurance services that include Audit trails, Security audit and Security monitoring.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security mechanisms for implementing control point looks at the security mechanisms to implement control points in security processes to enforce the security related time constraints and sequence constraints.

This service is ranked as 1 in the SABSA Component Security Architecture component because Timing and sequencing of security steps describes how the timing and sequencing steps relating to the business requirements will be met in practice, eg user expectations, business deadlines and volume throughput frequirements.

J) Compliance services

This service is ranked as 1 in the SABSA Contextual Security Architecture component because as part of the Business requirements collection, the security requirements for systems assurance are identified.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Security Strategies help to examine the System assurance strategy at a conceptual level.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Services describes the assurance services that include Audit trails, Security audit and Security monitoring.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security mechanisms for implementing control point looks at the security mechanisms to implement control points in security processes to enforce the security related time constraints and sequence constraints.

K) Security Awareness services

The Security Awareness services in the SABSA Logical Security Architecture is ranked as 1 because Security Services describes Security Training and Awareness as part of the defensive strategy.

The Security Awareness services in the SABSA Physical Security Architecture is ranked as 1 because Security Mechanisms maps the physical security mechanisms to security training and awareness.

L) Security domain services

This service is ranked as 1 in the SABSA Logical Security Architecture component because Security Domain Definitions & Associations defines the security domains that will include Network Domains, Middleware Domains, Application Domains and Security Service Management Domains.

This service is ranked as 2 in the SABSA Physical Security Architecture component because Security Rules, Practices and procedures turns the

security policies identified in the Logical Security Architecture into sets of rules, practices and procedures.

This service is ranked as 1 in the SABSA Component Security Architecture component because Security mechanisms used to provide security within the platform and network infrastructure.

M) Middleware security services

This service is ranked as 1 in the Contextual Security Architecture component because Business Process Model identifies the security requirements that are driven by business processes.

This service is ranked as 1 in the SABSA Conceptual Security Architecture component because Architectural layering provides for a security infrastructure layered architecture that caters for Security services in the Middleware layer.

This service is ranked as 2 in the SABSA Logical Security Architecture component because Security Domain Definitions & Associations defines the security domains that will include Middleware Domains.

This service is ranked as 1 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to Middleware security services

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of Middleware security services tools and products.

N) Data management security services

This service is ranked as 1 in the SABSA Logical Security Architecture component because Security Domain Definitions & Associations defines the security domains that will include Data management Domains.

This service is ranked as 2 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to Data management security services

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of Data management services tools and products.

O) Network security services

This service is ranked as 1 in the SABSA Logical Security Architecture component because Security Domain Definitions & Associations defines the security domains that will include Network security Domains.

This service is ranked as 2 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to Network security services

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of Network security services tools and products.

P) Platform security services

This service is ranked as 1 in the SABSA Logical Security Architecture component because Security Domain Definitions & Associations defines the security domains that will include Platform Domains.

This service is ranked as 2 in the SABSA Physical Security Architecture component because Security Mechanisms maps the physical security mechanisms to Platform security services

This service is ranked as 1 in the SABSA Component Security Architecture component because Security Products and Tools provide a description of the features of Platform services tools and products.

5.3.3 Summary

In summary, the SABSA Framework, had a total score of 78. This is obtained by adding the scores for each of the components.

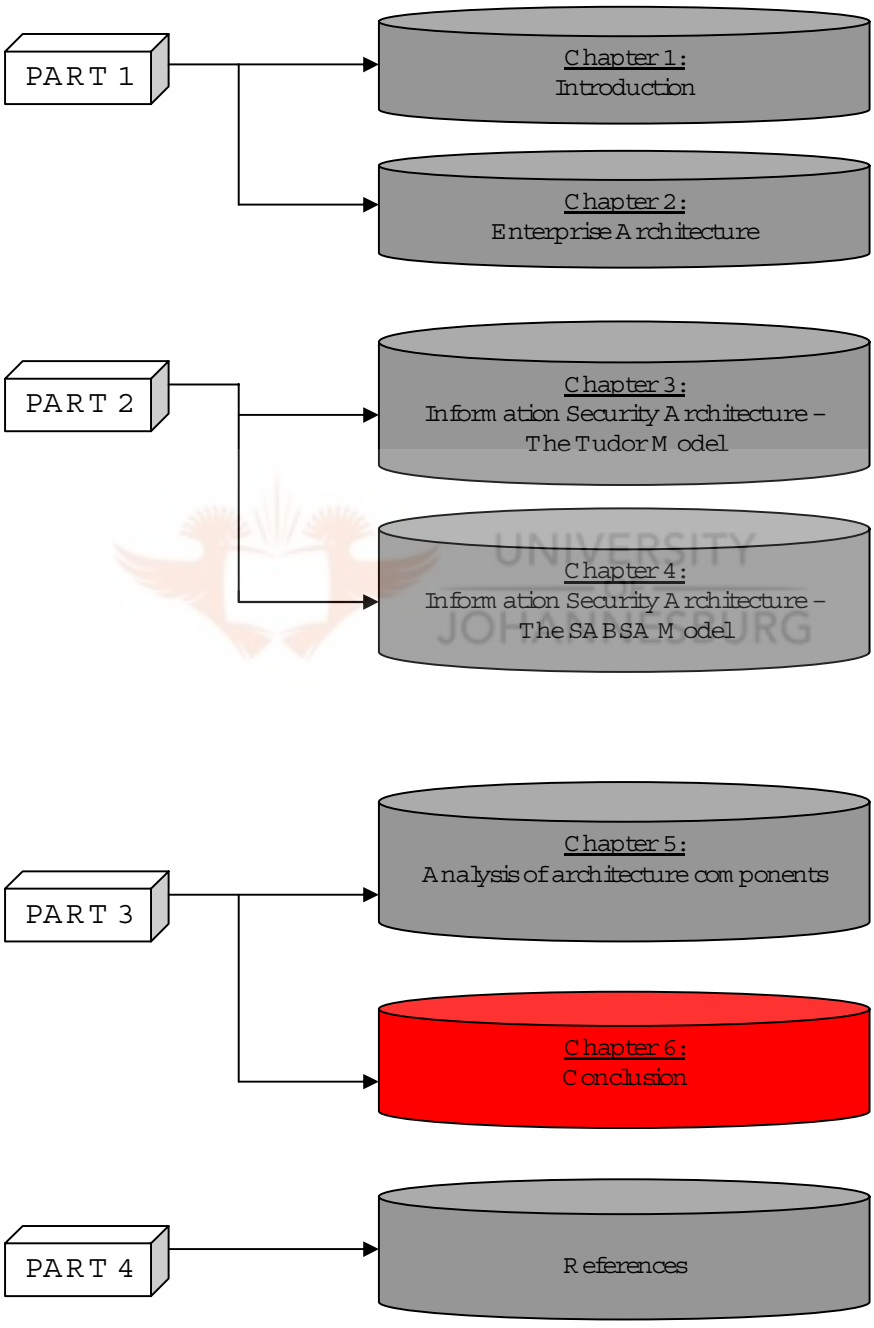
The SABSA Framework provides for most of the security services required by the Enterprise Architecture. The SABSA Framework also includes security services that are not considered by the Enterprise Architecture.

The next chapter, Chapter 6 is the last chapter of this mini dissertation. The chapter will provide a recommendation on which Information Security Architecture model or framework is the best fit.

However, it should be noted that in terms of the objectiveness of the scoring for the Tudor Model and the SABSA Framework, we are not comparing "apples" with "apples' because the two Architectures are not defined the same way. Nevertheless, in Chapter 6, a recommendation will be submitted based on the author's self evaluation.

CHAPTER 6

CONCLUSION



CHAPTER 6

This chapter will conclude the dissertation. The chapter will be discussed under the following headings:

6.1 Restatement of the objective of this dissertation
6.2 Summary of the analysis of the Information Security Models and Frameworks
6.3 Recommendation

6.1 Restatement of the objective of this dissertation

6.1	**Restatement of the objective of this dissertation**
6.2	**Summary of the analysis of the Information Security Models and Frameworks**
6.3	**Recommendation**

The objective of this mini dissertation was to identify an Information Security Architecture that aligns with the principles and security requirements of the Enterprise Architecture of a large energy utility, Eskom.

The approach used a literature survey to identify two possible Information Security Architecture models and frameworks. Each of the identified frameworks and models were analysed to understand the components that make up the framework. Information security activities were compiled from each of the components, based on the author's knowledge and experience. The information security activities were used to assess the extent to which the Information Security Architecture frameworks aligned with the security services required by the Enterprise Architecture of Eskom. Based on this alignment, a recommendation would be submitted on which Information Security Architecture is the best fit for Eskom.

6.2 Summary of the analysis of the Information Security Models and Frameworks

6.1	**Restatement of the objective of this dissertation**
6.2	**Summary of the analysis of the Information Security Models and Frameworks**
6.3	**Recommendation**

The Tudor Model had a total score of 29. Except for the Middleware services, The Tudor Model does provide for all the services required by the Enterprise Architecture. The Tudor Model also includes security services that are not considered by the Enterprise Architecture.

The SABSA Framework had a total score of 78. The SABSA Framework provides for most of the services required by the Enterprise Architecture. The SABSA Framework also includes security services that are not considered by the Enterprise Architecture.

The primary difference between the two Information Security Architectures is that the SABSA Framework is based on a six layer model of information security. The layers correspond closely to the layers of an Enterprise Architecture used by Eskom. Therefore the SABSA Framework provides security services at all layers, with each layer providing a greater level of detail regarding the security service.

In the discussion in Chapter 2 regarding the alignment of an Information Security Architecture with an Enterprise Architecture as was depicted in Figure 2.4.1 and Figure 2.4.2, the SABSA Framework aligns closely with an Enterprise Architecture.

6.3 Recommendation

6.1	**Restatement of the objective of this dissertation**
6.2	**Summary of analysis of the Tudor Model**
6.3	**Summary of analysis of the SABSA Framework**
6.4	**Recommendation**

Based on the results of this dissertation, it is recommended that the SABSA Framework is the best fit Information Security Architecture for Eskom. Another recommendation is that further research be conducted after the implementation of the SABSA Framework to assess the alignment.

Part 4

References (Referred in the dissertation)

[1] Tudor, JK 2001, Information Security Architecture: An Integrated approach to Security in the Organisation, CRC Press LLC, Florida

[2] Sherwood, J, Clark, A, Lynas, D 2005, Enterprise Security Architecture: A Business-Driven Approach, CMP Books, San Francisco

[3] Berinato, S 2005, The Global State of Information Security, http://www.cio.com/article/11691/the_global_state_of_information_security_

[4] Information Security Forum (ISF) 2006, Security Architecture: Workshop Report, London

[5] Eskom Common Understanding IS Architecture Model v3.0 2002, Eskom, Johannesburg

[6] The Open Group 2007, The Open Group Architecture Framework (TOGAF), http://www.opengroup.org/architecture

References (Read but not directly referred in the dissertation)

[1] **Zackman Institute for Framework Advancement (ZIFA) 2007, Zackman Framework, www.zifa.com**

[2] **Network,Analysis,Collaboration (NAC) 2004, Enterprise Security Architecture: A Framework and Template for Policy Driven Security, www.netapps.org/techpubs.htm#positionpapers**

[3] **Jhingram,AD, Mattos,N, Pirakesh,H 2002, Information Integration: A research agenda, http://www.research.ibm.com/journal/jj/414/jhingram.html**

[4] **BCC Security Strategy 2005, http://www.bcc.ctc.edu**

[5] **Microsoft 2007, Best practices for Enterprise Security, www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.mspx**

[6] **CSO 2003, Security Immaturity, http://www.csoonline.com/read/040103/survey.html**

[7] **Telstra Corporation Limited 2006, Information Security Strategy, http://www.telstra.com/hosting/products/security**

[8] **IBM 2002, Security in a WEB Services World: A Proposed Architecture and Roadmap, http://www.ibm.com/developerworks/webservices/library/specification/ws-secmap/**

[9] **Feigenbaum, J 2002, Towards Realistic Assumptions, Models and Goals for Security Research, http://www.cs.yale.edu/homes/jf/nsf-security-wp.pdf**

[10] **US Whitehouse 2003, The National Strategy to Secure Cyberspace, http://www.uscert.gov/reading_room/cyberspace_strategy.pdf**

[11] **OECD 2003, Implementation Plan for the OECD guidelines for the security of Information Systems and Networks: Towards a culture of security, http://www.oecd.org/dataoecd/23/11/31670189.pdf**

[12] **Malhorta, Y 1996, Enterprise Architecture: An Overview, http://www. kmbook.com/enterarch.htm**

[13] Tasmania Government 2005, Information Security Framework, http://www.egovernment.tas.gov.au/themes/information_security_and_management/information_security_framework

[14] Creswick, BP 2005, Enterprise Architecture Definition and Automation: A Basis for IT Strategic Planning and Executive Decision Making http://www.ppc.com/modules/knowledgecenter/eadefinition.pdf

[15] Schekkerman, J 2005, Another View at Extended Enterprise Architecture Viewpoints, http:// www.enterprise-architecture.info/images/extended enterprise/extended enterprise architecture4.htm