Managing Information Confidentiality Using the Chinese Wall Model to Reduce Fraud in Government Tenders

By

Sobhana Rama

Managing Information Confidentiality Using the Chinese Wall Model to Reduce Fraud in Government Tenders

By

Sobhana Rama

200402862

Dissertation

Submitted in fulfilment of the requirements for the degree

Masters of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: **Prof Stephen Flowerday**

January 2013

Abstract

Instances of fraudulent acts are often headline news in the popular press in South Africa. Increasingly, these press reports point to the government tender process as being the main enabler used by the perpetrators committing the fraud. The cause of the tender fraud problem is confidentiality breach of information. This is accomplished, in part, by compromising the tender information contained in the government information system. This results in the biased award of a tender. Typically, the information in the tender process should be used to make decisions about a tender's specifications, solicitation, evaluation and adjudication. The sharing of said information to unauthorised persons can be used to manipulate and corrupt the process. This in turn corrupts the tender process by awarding a tender to an unworthy recipient.

This research studies the generic steps in the tender process to understand how information is used to corrupt the tender process. It proposes that conflict of interest, together with a lack of information confidentiality in the information system, paves the way for possible tender fraud. Thereafter, a system of internal controls is examined within the South African government as well as in foreign countries to investigate measures taken to reduce the breach of confidential information in the tender process. By referring to the Common Criteria Security Model, various critical security areas within the tender process are identified. This measure is assisted with the ISO/IEC 27002 (2005) standard which has guiding principles for the management of confidential information. Thereafter, an information security policy,the Chinese Wall Model will be discussed as a means of reducing instances where conflict of interest may occur. Finally, an adapted Chinese Wall Model, which includes elements of the tender process, is presented as a way of reducing fraud in the government tender process.

Finally, the research objective of this study is presented in the form of Critical Success Factors that aid in reducing the breach of confidential information in the tender process. As a consequence, tender fraud is reduced. These success factors have a direct and serious impact on the effectiveness of the Chinese Wall Model to secure the confidentiality of tender information. The proposed Critical Success Factors include: the Sanitisation Policy Document, an Electronic Document Management System, the Tender Evaluation Ethics Document, the Audit Trail Log and the Chinese Wall Model Prosecution Register.

Keywords: Chinese Wall Model; information confidentiality; conflict of interest; government tender fraud

Declaration

I, Ms Sobhana Rama, 200402862, hereby declare that:

- The work in this dissertation is my own work.
- I am fully aware of the University of Fort Hare's policy on plagiarism and I have taken every precaution to comply with the regulations.
- I am fully aware of the University of Fort Hare's policy on research ethics and I have taken every precaution to comply with the regulations.

Signature : .....

Date : .....

Acknowledgements

I would like to express my sincere gratitude and appreciation to my supervisor, Prof. Stephen Flowerday, for his valued advice, guidance, teaching, and encouragement towards the finalisation of my dissertation. I appreciate the constructive feedback from Duane Boucher who assisted on this Master's, whilst being mentored by Prof. Flowerday.

I also want to thank the proofreader, for all her time and effort in providing her language editing and proofreading skills. Their contribution is much appreciated.

I would like to express further gratitude to my friends and family for all their endless support, love and understanding throughout the dissertation process, and for all their help in ensuring the submission of the final dissertation.

I am grateful to the experts and reviewers who participated in this study, and who contributed to the achievement of its objectives.

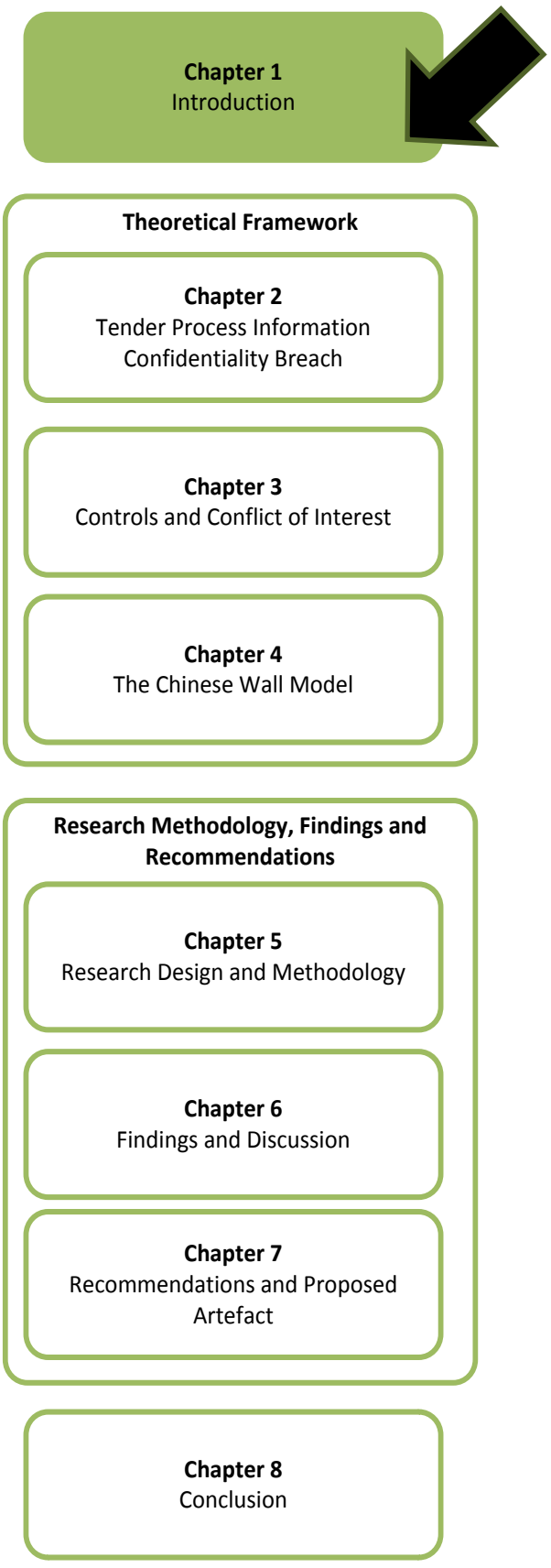
Finally, I would like to thank my Lord Shiva, who has been my strength and perseverance, and who has helped me every step of the way to complete this dissertation.

Table of Contents

List of figures

List of tables

CHAPTER 1 : INTRODUCTION



Chapter 1

"Confidential information in the government tender process is often not secure, exposing it to possible fraud".

(Rama, Flowerday & Boucher, 2012)

1.1 Background to the Study

Information plays an important role in the tender process. With such reliance on information, its security should be of the utmost importance to government. According to NIST Publication (2010) and ISO/IEC 27002 (2005), information security guards the *availability*, *confidentiality* and *integrity* of the information. Thus, information is used to make decisions about tender specifications, solicitation, evaluation and adjudication. Information in the tender process is contained in committee meeting minutes, score sheets completed for each bidder's document received, and a declaration of interest signed by each member of the committee. Sharing this information with unauthorized persons can cause irregularities and disruptions in the tender process (Tomlinson, 2010).

The Chinese Wall Model has emerged as a means of restricting the flow of information to unauthorised persons (Brewer & Nash, 1989). Information is the key to decision-making in the government tender process (Kaisara & Pather, 2011). The unauthorised disclosure of information is due to a conflict of interest which can lead to corruption of the government tender process (Tomlinson, 2010). Conflict of interest is defined as a public servant acting, or failing to act, on a matter where the public servant or another person or entity that stands in a relationship with the public servant, has an interest (Bertino, 2010). The Chinese Wall Model is an information barrier designed to reduce the conflict of interest problem in the organisation (Slay & Koronios, 2006; TechTarget Corporation, 2011). Therefore, a conceptual wall is constructed to prevent the breach of insider information.

There are a number of acts, policies, regulations and standards, such as the Preferential Procurement Policy Framework Act (PPPFA), 2000 (Republic of South Africa, 2000a) and National Treasury Supply Chain Management Regulations, 2003 (Republic of South Africa, 2003b) which are intended to safeguard information and to improve confidentiality in the government tender process. However, even with these acts, policies, regulations and standards in place, the conflict of interest problem is still a growing issue in the South African government tender process (Gordhan, 2011).

An example of conflict of interest in the tender process is at the Department of Correctional Services and at the Company and Intellectual Property Registration Office (Cipro). As

acknowledged by Paton (2010), the tender for the Information Technology (IT) data management system at Cipro was worth R153-million and was awarded to a company which, at the time, was only three months old and had no track record. No SARS tax clearance certificate was provided. The composition of the evaluation committee was manipulated. The above is in conflict with at least one of the regulations, namely the PPPFA (2000). This example is noteworthy because it is one of the numerous, occurring conflict of interest problems encountered in the government tender process. The tender process is depicted in Appendix A. The use of the Chinese Wall Model in organisations such as investment banks was researched and applied in the context of the tender process for this study.

The Chinese Wall Model has been applied in investment banks between the corporate-advisory area and the brokering department. Individuals, who will give corporate advice about takeovers, are not allowed to disclose information to individuals advising clients to buy shares (TechTarget Corporation, 2011). The unauthorized disclosure of this information could influence the advice given to clients making investments, thus allowing staff to take advantage of facts not yet known to the general public.

1.2 Statement of the Problem

In the past few years, research into tender process risk management has gained considerable attention (Kaynak & Hartley, 2008). This study will consider the problem of the unauthorised disclosure of confidential information caused by the conflict of interest problem in the tender process. This problem arises from intentional human interference in information disclosure and is illegal according to the Prevention and Combating Corruption Activities Act (2004).

Paton (2010, p.1) states “It has been estimated unofficially, that R30-billion per year, 20% of the overall government procurement budget of R150-billion, is being lost or is disappearing into a black hole of corruption”. Much of this loss is due to conflict of interest in the tender process, overpricing, and the failure of contractors to deliver on their promises (Paton, 2010). She further states that the Special Investigating Unit (SIU) has noted that supply chain corruption is on the increase despite the recent, increased political focus on the issue. This is further confirmed by the South African Budget Speech (2011).

According to the 2011 Budget Speech by Minister of Finance Pravin Gordhan, “…public procurement plays a significant part in the economy and is central to government service delivery” (Gordhan, 2011, p. 21). He further adds that citizens and taxpayers do not receive full value for money, because the tender process is vulnerable to waste and corruption (Gordhan, 2011). It is clear that there is failure to manage the confidentiality of information

and that there is a breach of this confidential information with the intention of manipulating the tender process. The next section will consider the research questions.

1.3 Primary Research Question

How can the application of the Chinese Wall Model reduce the use of information in corrupting the tender process in the South African government?

1.4 Secondary Research Questions

In answering the main research question, the following secondary questions are addressed.

1.4.1 *How is information used to corrupt the government tender process in South Africa?*

Corruption poses a threat to the government tenders (Gordhan, 2011; IBM, 2008). While corruption arises from human activities, lack of information system security can hamper and subvert the confidentiality of information (Common Criteria Security Model, 2009). This research question will explain the tender process and the concept of corruption in government. An explanation will be provided on how corruption is committed in this context.

1.4.2 *What controls are in place to reduce the information breach and improve confidentiality in the government tender process?*

The effective management of the supply chain process requires that controls are put in place. Controls are necessary to avoid risk and identify the strengths and weaknesses of a process (Ko, Lee & Lee, 2009). Within government organisations, the major controls identified are policies and procedures, and laws and regulations. These controls will be compared and contrasted with the Common Criteria Model (Common Criteria Security Model, 2009) and ISO/IEC 27002 (2005) to evaluate the security of information in the tender process.

1.4.3 *How can the Chinese Wall Model be used to improve information confidentiality in the government tender process?*

There are three levels of information security control: preventative, detective and corrective (GTAG1, 2012). The Chinese Wall Model will be applied at the preventative level as it aims to prevent the breach of confidential information. Critical Success Factors (CSFs) will be developed based on the Chinese Wall Model.

1.5 Objective of the Study

This study investigates and explains the current controls in place to reduce the use of information used to corrupt the tender process. Gaps in these controls will be identified. Consequently, the objective of this study is to produce an artefact, comprising a set of Critical Success Factors (CSF), incorporating the Chinese Wall Model in order to reduce the breach of information confidentiality. These CSFs will be used to improve information confidentiality and reduce the use of information used to corrupt the tender process.

1.6 Significance of the Study

This research project is undertaken in response to a call by Gordhan (2011), who states that all citizens have a shared responsibility to prevent corruption in the government tender process. This study also adds to the emerging, yet growing literature on government tender fraud, and contributes to improving confidentiality in the government tender process.

This study will contribute to the body of knowledge by extending the examination of the use of information which may corrupt the tender process. Firstly, it identifies gaps in information systems which control the government supply chain tender process. Secondly, it proposes a solution to avoid the conflict of interest problems with the application of the Chinese Wall Model. Finally, an artefact comprising Critical Success Factors (CSFs) will be formalised.

In addition, individuals will find this study useful when implementing strategic decisions in government with regard to tender management. These include individuals involved in contract, commercial and supplier management and also project and programme managers.

1.7 Literature Review

This section introduces literature from other studies concerning the research problem. It also notes the relevant legislation applicable to this study. The review is divided into three sections aligned to the research questions.

1.7.1 The use of information with regard to the corruption of the tender process

The tender process is an aspect of the government supply chain (Republic of South Africa, 2003b). An important aspect of the tender process is risk management. Risk can be detrimental not only to the department, but to the public it serves. Corruption is defined as a type of supply chain risk (IBM, 2008) and is defined by Department of Human Settlements (2009) as “the offering, giving, receiving or soliciting of anything of value to influence the action of a department official in the selection process or in the execution of contracts”.

If information in the tender process is not safeguarded from unauthorised individuals, it can be used to negatively influence individuals who make procurement decisions in the tender

process. Information in the tender process is used to make decisions about the procurement of suppliers who will provide goods or services to a department (Mutula & Wamukoya, 2009). Also, information that is not known to the public can be abused by the unauthorised individual. This abuse of information is in most cases, due to a conflict of interest (Tomlinson, 2010).

It was stated in the South African Budget Speech on the 23 February 2011, that there are currently 53 investigations involving procurement irregularities, involving contracts worth R3 billion (Gordhan, 2011). Consequently, the Minister of Finance, Pravin Gordhan, has undertaken a project to tackle corruption in the government supply chain by using the Special Investigationing Unit (SIU) resources and involving each government agency that reports to him. He clearly notes that corruption in the supply chain is a risk that every practitioner in the procurement environment needs to identify, manage and eliminate. Thus, it is important that the confidentiality of information is safeguarded and available only to authorised persons. However, reliance is placed on practitioners following an honour system. In other words, the information is only restricted by the judgment of the parties involved and this is in alignment with the Chinese Wall Model. This theory states that information should only be available to persons who have authorised access (Bertino, 2010).

According to TechTarget Corporation (2011), the term '*Chinese Wall'* is said to have originated after the catastrophic stock market crash of 1929, when the largely unregulated United States market suffered a 40% drop in the price of shares between September and October. The crash is said to have resulted from inflated stock values created by price manipulation and insider trading. After the crash, a law was passed mandating the separation of commercial and investment banks, in an attempt to prevent conflict of interest. However, rather than enforcing physical or corporate separation, the law only mandated that policies must be in place to create a logical division between these segments.

In addition to the Chinese Wall Model, legislation specifies legal requirements for information security as highlighted in the next section, to help control corruption and improve information confidentiality in the tender process.

1.7.2 Controls to reduce unauthorised information disclosure in the tender process

Legislation, acts, policies and procedures include but are not limited to; Public Finance Management Act (PFMA) (Republic of South Africa, 1999), the National Treasury Supply Chain Management Regulations (Republic of South Africa, 2003b), the Preferential Procurement Policy Framework Act (PPPFA) (Republic of South Africa, 2000a), the Promotion of Administrative Justice Act (Republic of South Africa, 2000b) and the Promotion of Access to Information Act (Republic of South Africa, 2000). Furthermore, regarding

procedures and administrative actions, a government official is bound to comply with the directives and limitations contained in the Supply Chain Management Procedure Manual Framework (SCMPFM) (Department of Human Settlements, 2009). This compliance will lessen the breach of information to unauthorised officials.

Barham (2010) points out that an information security breach includes denial of access, unauthorised disclosure and unauthorized destruction or modification of information. It is further stated that information confidentiality means preserving authorized restrictions on access and disclosure, including the means for protecting personal privacy and proprietary information (ISO/IEC 27002, 2005). This means restricting the flow of information which is in agreement with the advocated Chinese Wall Model.

In addition to legislation, there are eight principles which have been adopted by the South African government, known as the Batho Pele framework (Department of Public Services and Administration (2011). The Batho Pele policy framework is an approach to conducting service quality evaluations. It is an approach which puts pressure on systems, procedures, attitudes and behaviour within the public service and reorients them in the customer's favour. It is an approach that puts *people first*. Three key principles of the Batho Pele framework are relevant to this study. These are listed below with an example given applicable to this study.

- Information –
    - Persons from the public should have access to information they are entitled to receive. For example, the bidders should be aware of a government tender, but information such as the bidder's price of the different bidders should not be revealed before the tender closes.
- Openness and transparency –
    - The supply chain process and especially the tender process, should be clear, non-biased and made available to the public.
- Value for money –
    - Taxpayers should receive full value for their money. Poor delivery by a government organisation due to poorly chosen contractors is unacceptable.

These principles align with tender legislation. The accounting officer for a department, trading entity or constitutional institution must ensure that the department has and maintains an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective (Republic of South Africa, 1999). Additionally, these controls should manage the behaviour of employees to ensure information confidentiality (Da Veiga &

Eloff, 2010). This leads to the next section on the application of the Chinese Wall Model to improve the confidentiality of information in the tender process.

1.7.3 Information confidentiality and the Chinese Wall Model

Information confidentiality is attained through controls that management creates and maintains within a company (Da Veiga & Eloff, 2010; Huntley, 2010; Flowerday & von Solms, 2007). The management board of government should consider performing a tender process risk assessment against the ISO/IEC 27002 (2005) to explore their information security risks and apply suitable controls.

There are models constructed to provide information security controls which are discussed in this section. The goal of Clark and Wilson's approach is to prevent information corruption and error in the commercial environment (Chen, Shing, Lee, & Shing, 2007). On the other hand, Biba's Integrity Model prevents possible data corruption by limiting information flow among data objects (Byun, Sohn, & Bertino, 2006). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information (Chen *et al*., 2007). To summarise, the Clark and Wilson's model, Biba's Integrity Model and Bell–La Padula Model are based on a set of access control rules for information, which already exist in the database. The Chinese Wall Model however explains that information cannot flow between the subjects and objects in a way that would create a conflict of interest (Bertino, 2010). Policies in the Chinese Wall Model group objects into conflict of Interest classes and individual users are not allowed to access information from two or more objects in a conflict of interest class (Brewer & Nash, 1989). In particular, the semantics of Chinese Wall Model allow an individual to access any one dataset in a conflict of interest class, and prevents further accesses to other datasets in that class (Brewer & Nash, 1989).

When the above models are compared and contrasted, the Chinese Wall Model is more relevant for this research project as it addresses the problem of conflict of interest (Bertino, 2010), rather than the modification of information in the database, which can be addressed by the above mentioned theories, other than the Chinese Wall Model. In other words, the Chinese Wall Model is directed to the flow of information, rather than access control.

To refer to the Batho Pele framework, an example of how the Chinese Wall Model can be applied to the three key principles is addressed below.

Table 1.1 Batho Pele principles

Batho Pele Principle	Application of the Chinese Wall Model
Information	A departmental official who is unauthorised to view sensitive information of tender documents received, should not have access to such information.
Openness and transparency	If a supply chain official has a business interest in a contract to be awarded by the Department, that official must withdraw from participating in any manner of the tender award process relating to the contract.
Value for money	A Chinese Wall can be employed to separate information made available during the bid specification committee meetings, from bidders and other departmental staff, who could potentially influence the value (price) of the bid submitted.

The research methodology in the next section briefly describes how the research project was be conducted.

1.8 Research Design and Methodology

The research methodology is tailored to address the research problem. The focus of this study is directed towards the improvement of information confidentiality and the reduction of the threat of corruption in the government supply chain tender process with the development of Critical Success Factors (CSF's). The CSFs will be validated by an expert panel.

The artefact will be created by using the Design Science Guidelines. The Information Systems (IS) Design Science Guidelines can be based on positivism, traditional realism or pragmatism (Carlsson, Keller, Henningsson & Hrastinski, 2011). For the purpose of this study, the pragmatism research paradigm is followed. The figure that follows, summarises the research process adopted in this study.

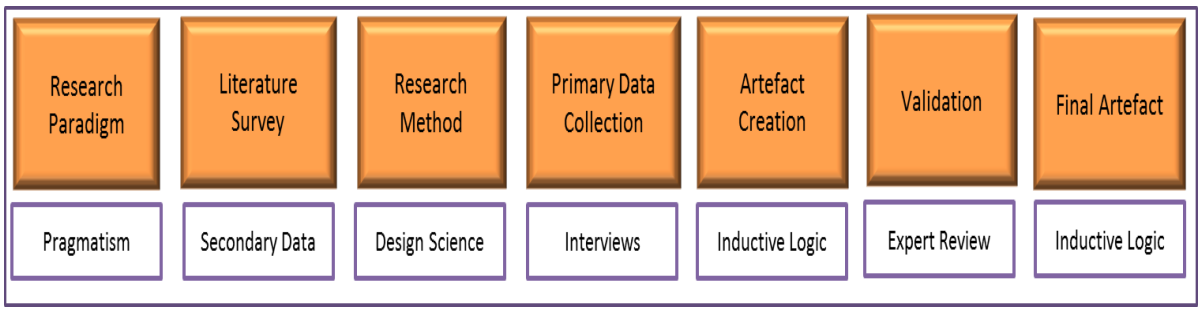


Figure 1.1 Research process

1.9 Research Paradigm

Pragmatism includes subjectivity as it assumes that reality is a contextual field of information (Cavana, Delahaye & Sekaran, 2001 in Andrade, 2009). Social reality is defined by people's actions and interaction. The researcher's interpretation is substantiated by quality arguments rather than by exact statistics (Andrade, 2009). In other words, theory is extracted from practice and applied back to practice. Pragmatism is the ability to think about external things and to improve understanding of them (Hookway, 2008). This will be done using the Design Science Guidelines.

1.10 Methods

Design Science is a comprehensive problem-solving process characterized by a detailed evaluation of a project or system to create an artefact (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007). Information Systems (IS) Design Science research is aimed at developing practical design knowledge and theory to solve IS problems (Carlsson, Keller, Henningsson & Hrastinski, 2011). For this study, the proposed artefact is Critical Success Factors. The Design Science methodology has seven guidelines namely: design as an artefact, problem relevance, design evaluation, research contributions, research rigor, design as a search process and communications of research (Hevner, March, Park & Ram, 2004). In order to apply the Design Science methodology, these seven guidelines will be followed.

1.11 Data collection

Primary data collection in this study includes the use of the Expert Review Process. This process will be used to obtain feedback from ten senior individuals to gain their expert opinion concerning the research question, the proposed solution, the critical success factors, and any other relevant questions that have to be asked for this research project. Furthermore, experts will be presented with the research findings and will be asked to critique these findings as a validation step in the process of refining the proposed artefact. This is in compliance with the Design Science research and is explained below in the validation section (Hevner *et al*., 2004).

Secondary data includes other studies of the tender process, that is risk management, corruption, controls, information security, information confidentiality and the Chinese Wall Model. Theories and models pertinent to this research project will also be sourced. Legislation, policies and procedures used to govern the tender process, will be collected. The evaluation of this research will now be presented.

1.12 Research Evaluation

The proposed artefact (CSFs) will be presented for evaluation to an expert review panel of twelve practitioners who are knowledgeable about information security and the tender process. It is essential to verify and validate the proposed artefact (CSFs) in order for it to be adopted and tested in the real world (Lambert, Knemeyer & Gardner, 2011). Design Science notes that the goal of validating the proposed artefact is to ensure that the artefact addresses the research question and fits with the research project context (Hevner *et al*., 2004). In summary, once an artefact is put through a validation process, it has a higher degree of credibility and quality. The delimitation of this study follows.

1.13 Delimitation of the Study

The application of the Chinese Wall Model together with the government tender process in South Africa and information confidentiality will be the focus of this study. Supply chain risk includes operational/technological, social, natural/hazard, economy/competition, legal/political categories (IBM, 2008). This research project focuses only on the social category of supply chains and the misuse of information to corrupt the tender process. See Appendix B for categories. This research focuses on the government environment and not on the private sector. Also the focus is narrowed down to the tender process which is part of the broader context of the entire supply chain. The term government referred to throughout this study is a South African government department.

Information security in this study focuses on controls, including policies, procedures and processes and information system controls. Attention is placed on the confidentiality aspect of information security throughout this study. The following paragraph describes the ethical consideration.

1.14 Ethical Considerations

Due to the nature of information collected during this study, the researcher is bound by a strict confidentiality code. No government officials, whom the supplier identifies or expert reviewers, will be disclosed for any reason outside the scope of this study. Approval has been obtained from a particular department, to gain access to the necessary individuals and documents needed for this study. The government entity prefers to be anonymous and therefore will be referred to as Department A. Any information deemed confidential that cannot be disclosed, will be at the discretion of the necessary government officials. The researcher is bound by a research code of ethics (Resnik, 2010). The researcher will adhere to ethical norms in this research. Research ethics are explained in detail in the research methodology chapter. The next section highlights the findings of this research.

1.15 Research Findings

Based on the theoretical framework of this study, it was found that the application of the Chinese Wall Model can be used to reduce conflict of interest and thus reduce the breach of confidential information in the tender process (Rama *et al*., 2012). The proposed design artefact of this research project is a set of critical success factors incorporating the Chinese Wall Model to manage information confidentiality in the tender process. A paper was prese ted at the ISSA 2012 conference and published on the IEEE database. See Appendix G. A second paper is under review. This research and the proposed artefact were validated during the expert review process. Consensus from the experts was obtained for this research project. The next section will introduce all the chapters.

1.16 Outline of Chapters

Chapter one denotes and describes the background for this study including the relevance of this research project. The problem statement and research questions are introduced, followed by the research scope and significance of the study. The research design and methodology is explained and concludes with the delimitations to the study and ethical considerations.

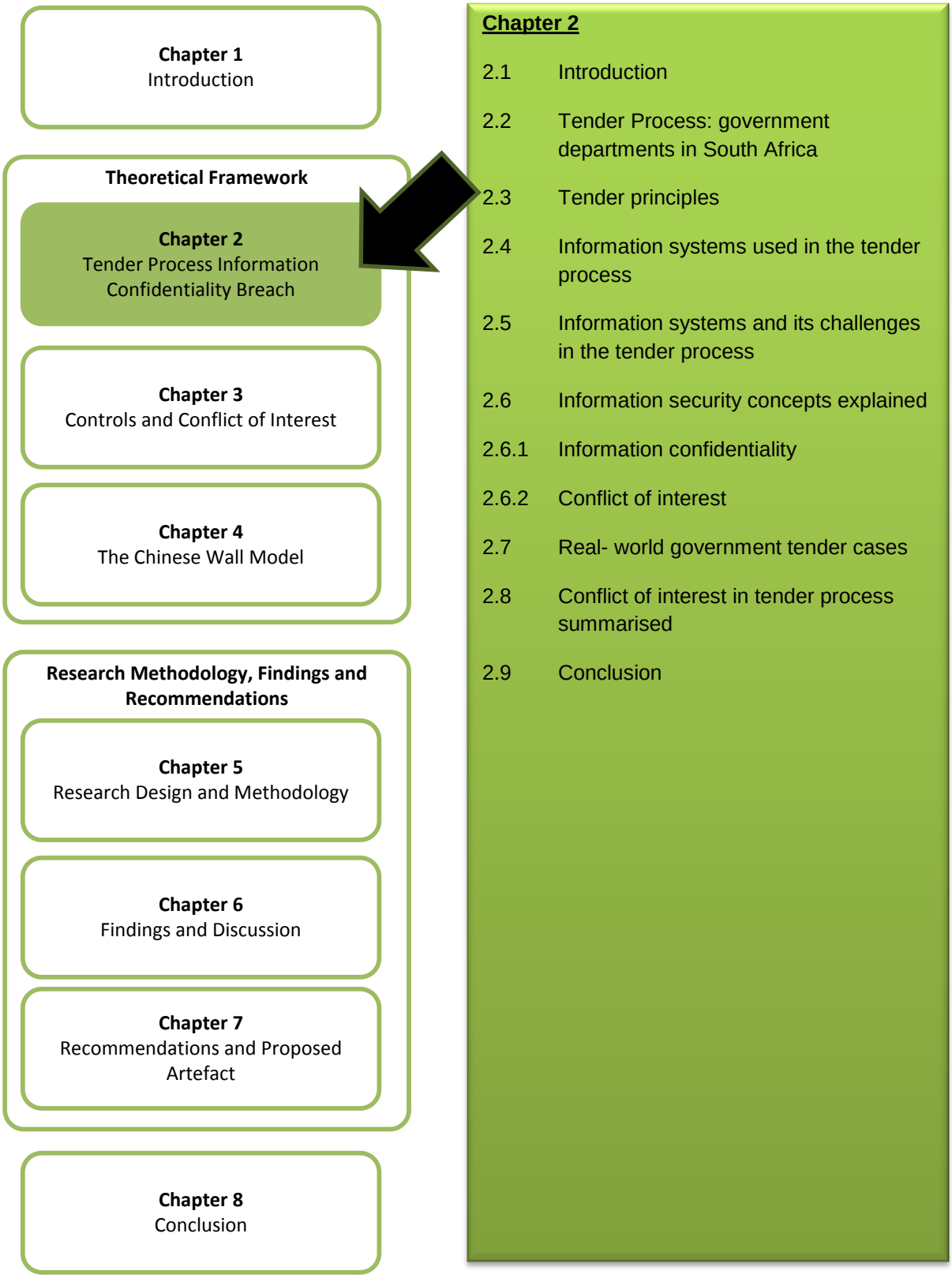
Chapter two introduces the concept of corruption in the government tender process process. It explains how information is used to corrupt the tender process. Chapter three examines the checks and controls in place to lessen information breaches which lead to corruption of the tender process. This includes regulations, policies and procedures; system of internal controls as well as controls identified in foreign governments including developing and developed countries. Controls from an information security perspective will be thoroughly analysed.

Chapter four examines various information access control models to manage the flow of information in the tender process. It incorporates the application of the Chinese Wall Model to improve information confidentiality issues relating to conflict of interest.

Chapter five describes the research design and methodology. It explains how the research process takes place as well as how the data is obtained and analysed. The validation process of the proposed artefact is reflected. Chapter six discusses the empirical findings.

Chapter seven reflects the proposed artefact, which meets the objective of this study. Here, the researcher discusses critical thought in the development of the artefact. Validation and credibility of the research findings is also discussed. Chapter eight presents a conclusion and provide suggestions for future research.

CHAPTER 2 : TENDER PROCESS INFORMATION CONFIDENTIALITY BREACH



> "Corruption hurts the poor disproportionately by diverting funds intended for development, undermining a government's ability to provide basic services, feeding inequality and injustice, and discouraging foreign investment and aid".
>
> Previous Secretary-General of the United Nations (Kofi Anan, 2006)

2.1 Introduction

In the current environment, the South African government has embarked on investing in major information systems in an attempt to take advantage of the benefits of information technology (Department of Communications, 2010). This allows government to extend the channels by which services are delivered to the public. To assist government departments to provide services to the public, the departments outsource the required work and services to suppliers (Republic of South Africa, 2003; Tomlinson, 2010).

Therefore, departments are obliged to follow a set of rules concerning tender solicitation, specification, evaluation and adjudication, when procuring goods/services. This is to ensure that systems are equitable, consistent and that transparent processes are followed in the tender process.

Inadequate application of procurement policies, weak information security, inappropriate influence in carrying out the appointment of project managers and suppliers, accepting personal gain from suppliers, all lead to corruption of the tender process. Based on research done by Mutula and Wamukoya (2009), Tomlinson (2010) and Gordhan (2011), corruption of government tenders is mainly due to the unauthorised disclosure of information or a breach of information confidentiality. This breach of information confidentiality is due to a conflict of interest which can arise between government officials and external stakeholders (Gordhan, 2011). The purpose of this chapter is, therefore, to critique the tender process and investigate a few of its failures by placing corruption of the tender process in context. To assist the understanding of this research problem, this chapter will focus on exploring the problem steps in the tender process. It will introduce the concept of information confidentiality and conflict of interest. Thereafter it will seek to understand how information is used to corrupt the tender process by an information breach. This will be done by analysing various case studies associated with conflict of interest and tender fraud.

2.2 Tender Process: government departments in South Africa

The terms, public sector or government are used in this study to refer to agencies, institutions, organisations under state control that are recognised as serving the needs of the general public. The term private sector, on the other hand, refers to institutions and/or organisations or business enterprises whose activities are usually financed through private shareholding equity. Government covers the civil service, state and quasi-public or state corporations (Mutula & Wamukoya, 2009). The government is the largest organisation in South Africa and spends billions of Rands on infrastructure, amoungst others, projects related to buildings, port works, roads, water works and technology (Gordhan, 2011).

According to South Africa's Preferential Procurement Policy Framework Act, PPPFA (2000), the government may outsource required work and services by various methods. These include bidding through: Request for Quotation (RFQ), Request for Proposal (RFP) or Agreement through Negotiation. The competitive tendering process through RFP is the most frequently used for tenders above R500 000. However, irrespective of the method used, there is the need to follow a set procedure to ensure that the tender process is transparent, so that instances of conflict of interest can be avoided. The essential requirements for the tender process as per National Treasury's Supply Chain Management (Republic of South Africa, 2003b) are as follows:

- Accounting officers of the departments must ensure that the tender process is competitive for potential service providers.
- The tenders should be advertised in the government tender bulletin and in any other appropriate media to ensure that potential bidders are aware of the required work or service needed.
- Should it be impractical to invite competitive bids for specific procurement, e.g. in emergency cases or in the case of a sole proprietor, the accounting officer may procure the required goods or services by other means, such as by price quotations or negotiations in accordance with Treasury Regulations. The reasons for deviating from inviting competitive bids should be recorded and approved by the accounting officer. This ensures that officials do not abuse the deviation from the standard tender process.
- The accounting officer must report within ten working days to the relevant treasury as well as to the Auditor-General all cases where goods and services above the value of R1 million (VAT inclusive) are procured in terms of Treasury Regulation 16A6.4. The report must include, amid other requirements, the reasons for dispensing with the prescribed competitive bidding process.

- The selection of supplier(s) for the outsourced worked is based on an overall value for money. Whilst the bidders' price is important, the departments must prioritise economic factors such as the quality, reliability, safety, good design, timely delivery, maintenance and after- sales support when recommending a supplier. This ensures that the tender is not awarded to an unworthy supplier taking into account the bidder's price before economic factors can lead to a biased decision when recommending a supplier.

The above tender requirements feed into the tender process. In order to understand how a conflict of interest might occur in the tender process, it is necessary to review the tender process as applied in the departments. The section below reflects a high-level process and is generic across the departments in South Africa (Republic of South Africa, 2003b).

Step 1: Submission of an approved requisition

The first step in the tender process is to ensure that the department has budgeted for the procurement of the work. The requisition form stipulates that funds will have to be committed and approved for the required goods or services to be outsourced.

Step 2: Specification approved by Bid Specification Committee (BSC) and Bid Adjudication Committee (BAC)

The specifications and evaluation criteria for the required work must be included in the tender document and must be completed together with the assistance of the end user and the BSC. The tender document must include, but is not limited to, invitation to bid, tax clearance certificate, pricing specifications, technical specifications, and if needs be any special conditions. The BAC must confirm and approve the specifications.

Step 3: Public invitation of bid in the Government Gazette and other media

Tenders should be advertised in the Gazette. A tender briefing session may be held with prospective suppliers. Tender documents are issued to interested bidders. A reasonable fee may be charged for the tender documents.

Step 4: Submission of standard Bid documents by bidders

Prospective bidders/ tenderers will submit bids/ proposals with the completed tender documents to the Department.

Step 5: Bid closure process

The receipt of bids/proposals from suppliers will close on a specified date and time indicated in the tender document. No bids will be accepted after the closing date and time. The

bids/proposals are opened to the public only after the bid has closed. The supply chain management (SCM) practitioners and a witness will observe the bid closing process. The bid register is updated.

Step 6: Evaluation process based on price, functionality & preferential procurement objectives

The BEC will evaluate the bids in terms of the criteria stipulated in the bid documents. The BEC consists of five senior officials, two members from the BSC, SCM practitioners and individuals from the end user. It is important to note that the evaluation criteria may not be amended after the closure of bids. If amendments take place after the bid has closed then it is considered fraudulent. Completeness of documents must be checked in terms of SARS tax clearance certificate, company registration, legitimate signatures and any other necessary requirements as stipulated in the tender document.

The scoring for each bid document must be completed in accordance with the preference point system. In other words, the points calculated for *price* and *functionality* must be added to the points calculated for *goals*.

In terms of *functionality* points the following must be followed:

- Obtain criteria, values, weighing from specifications and the score each bid response obtained to each criteria. If the bids do not pass minimum passing score as stipulated in specification, the bid document is eliminated. It is considered fraud if unsuccessful documents are not eliminated.

The *price* points are calculated using the lowest price as the benchmark score. In addition, the calculations on scoring for *preference*/Black Econimic Empowernment (BEE) points must be done. The scores calculated for **functionality, price** and **preference** must be added. This must be done for each bid/proposal received and which has passed the functionality points. The bid/proposal document with the highest score must be recommended. A report with the recommendations from the BEC must be submitted to the BAC for approval.

The bidder / suppliers, who did not meet the criteria and were not recommended to provide the service/goods, must be notified by the department. The minutes taken at the bid meetings must be recorded. Also the necessary meeting documents such as oath of secrecy, delegation of authority and meeting agenda must be completed and filed in the SCM unit.

Step 7: Awarding of bid to highest scoring bidder by BAC

The BAC must confirm that all disqualified bids are justified. The unjustified bids must be submitted to the Bid Evaluation Committee (BEC) for re-evaluation. The bid documents above the departmental delegation are forwarded to a final approval committee such as the Interim Bid Adjudication Committee (IBAC). The supply chain manager (SCM) must ensure that the document format for the recommendations is in accordance with the IBAC requirements.

The Chief Financial Officer (CFO) must provide the submissions to IBAC. IBAC will decide to support the BAC's decision or ask for a re-evaluation for the scoring of the bids. If the IBAC proposes that the bids be re-evaluated, then this will be forwarded to the BEC and BAC. BEC will re-evaluate the bids and the re-evaluation will be forwarded to the BAC again.

Step 8: Publish award in government gazette and other media

The recommended bidder must be made known to the public. The recommended bidder should be published in the government gazette and or appropriate media.

Step 9: Notify bidders on the outcome of their bid proposal submitted

Unsuccessful bidders should be notified in writing. A letter of award should be signed by CFO or HOD and forwarded to successful bidder.

Step 10: Appeals process is finalised

A member of the SCM must follow up with the provincial Department of Treasury and with the department's legal section if any appeals have been lodged for the tender.

Step 11: Sign contract with the successful bidder

The SCM practitioner(s) and necessary individuals from the department must meet with the successful bidder/supplier to confirm scope of work and sign the contractual agreement(s).

Step 12: Issue purchase order

The last step in the tender process is for the department to issue a purchase order to the successful bidder/supplier.

These tender steps are summarised in a process diagram which is available in Appendix A. A summation of these steps is the high level overview of the tender process to which these steps must comply. No step should be compromised in any way. Compromising these steps is illegal and leads to tender fraud. Having said this, these steps are still compromised by certain government officials where a conflict of interest exists. This is linked to the study's

problem where information is used to corrupt the tender process. The steps in the tender process must be aligned with a number of principles as mentioned in the Batho Pele principles (Department of Public Services and Administration, 2011) and the PPPFA, 2000 (Republic of South Africa, 2000a). The tender principles will now be examined.

2.3 Tender principles

These principles play an integral part in ensuring that instances of fraud arising from a conflict of interest are avoided. The combination of tender principles has been adapted with a brief description of each principle. These are listed in no particular order of importance (Department of Human Settlements, 2009; Department of Public Services and Administration, 2011).

- Transparency Principle:
  - Implies that the procurement process must be open and must afford prospective bidders timely access to the same and accurate information.
- Effectiveness Principle:
  - To strive for effectiveness and cost-effectiveness in the procurement process.
- Efficiency Principle:
  - Seeks to ensure standards are met by simplifying procedures.
  - To build good relationships with suppliers and ensure good working practice.
- Competitiveness Principle:
  - Requires the need for competitiveness in bidding during the tender process.
- Fairness Principle:
  - Requires that no bidders should be discriminated against and fairness is upheld when dealing with any bidder. This entails that all proposals be evaluated fairly.
- Ethics Principle:
  - Necessitates that all stakeholders shall conduct business and themselves professionally, fairly, reasonably and with integrity. All interests shall be disclosed and any breach of information confidentiality and security requirements shall be reported.

- Proportionality Principle:
    - The product/service requirements stipulated in the specification / terms of reference must be appropriate, necessary and in reasonable proportion to the product / service being procured.

- Uniformity Principle:
    - To ensure tender procedures, policies, control measures and contract documentation are uniform, simple and adaptable to advances in modern technology.

- Accountability Principle:
    - The accounting officer and its management are accountable for their decisions and actions relative to their procurement responsibilities, the procurement process as well as the implementation of contracts.

- Openness Principle:
    - Must ensure procurement process is in line with best practice principles.

- Monetary Worth Principle:
    - Requires money to be spent in conjunction with cost and quality measures, to maximise efficiency, effectiveness and flexibility.

These principles are important to improve information confidentiality and decrease conflict of interest among tender officials. Therefore appropriate information security must be in place. The information security model known as the Chinese Wall Model, will be applied to these tender principles in Chapter Four. The Chinese Wall Model will be applied to assist in ensuring that tender principles exist in the tender process. In order to appreciate the relevance of these tender principles, it is necessary to explain the systems used for storing information in the tender process.

2.4 Information systems used in the tender process

For a number of years, government departments have captured and stored information using tools such as Microsoft Word, Excel and PowerPoint. To elaborate, tender- related information such as the scoring points calculated for each bid document are stored in physical files or on the departmental server (Department of Human Settlements, 2009). This information is often not safeguarded from unauthorised access (Cerrillo-i-Martínez, 2011). The decisions taken at bid committee meetings (steps two, six and seven) on tender specification, solicitation, evaluation and adjudication are available to all members of the BSC, BEC and BAC. The decisions made at the bid committee meeting are confidential, but

are often not kept secure from unauthorised persons. These unauthorised persons include members of the bid committees as well as non-bid committee members (Special Investigating Unit, 2011).

A lack of information confidentiality together with a government official knowingly possessing a conflict of interest, allows the official to derive personal gain by influencing decisions made on the award of a tender (Wagner & Bode, 2007). This in turn corrupts the tender process. Confidential information stored in paper trails or in the department's information system are easily accessible to unauthorised individuals and are at times compromised, leading to tender fraud (Cerrillo-i-Martínez, 2011). The reliance on uncompromised information during the tender process, points to the need to ensure that there is information confidentiality.

Also, the supplier database systems are not integrated across the departments in the Province. Each department in the province maintains its own supplier database. This result in suppliers having to register their company with numerous departments in the province, should they wish to do business with any department (Department of Human Settlements, 2009). This allows departments to follow their own supplier vetting process, which might not necessarily be thorough. Incorrect information relating to a supplier may be intentionally and incorrectly captured. This weakness is enhanced as there is no reliable audit trail for "read" and "write" access to information stored in a department's server.

Recently, late 2010, the Provincial Treasury implemented a centralised supplier database (CSD) in the Eastern Cape Province. The CSD contributes towards establishing an integrated and streamlined supply chain management system in the Eastern Cape Province. The CSD is web-based and is accessible to all departments as well as to the public. Obviously, information accessible to the users of the system is dependent on their security level. Therefore, access control is very important. Additionally, the intention of the CSD is to ensure that suppliers are vetted thoroughly as per statutory guidelines. Furthermore, the suppliers need to only register their company once on the CSD to tender across all departments (Eastern Cape Provincial Treasury, 2008).

The CSD allows for all necessary supplier registration and tender documentation to be stored electronically. Such documents include, but are not limited to, supplier registration forms such as an application for registration form, company registration forms, tax clearance certificates, the Broad-Based Black Economic Empowernmet (B-BBEE) certificates and tender award information for the tender. The system allows for a full audit log of all user interactions with the system. Thus, access to confidential information can be controlled. While certain information on the system must remain confidential, department officials will only have access to information which they have permission to view and modify (Eastern Cape Provincial Treasury, 2008).

2.5 Information systems and its challenges in the tender process

There are a number of challenges facing government in the information systems society. These include but are not limited to, managing information confidentilaity, unauthorised access to information and transparency of the tender process (Gordhan, 2011).

Mutula and Wamukoya (2009) note that one reason for unauthorised disclosure of information may be due to poor records' management in electronic formats. They added that when records become missing, altered, inaccessible or poorly managed, the process of tender governance becomes unclear. Weak records systems can be a barrier to information confidentiality and thus can encourage corruption of the government tenders (Mutula & Wamukoya, 2009).

While information confidentiality is key to reducing unauthorised disclosure of information, Mutula and Wamukoya (2009) add that effective access to government information and Freedom of Information (FOI) legislation impose responsibilities on the public authorities to provide access to information. They further add that effective electronic records management allows for an environment of increase transparency, accountability, integrity in the use of public resources and exposure to corruption. In the 2010 Budget Vote Speech, the Minister of Communications, Siphiwe Nyanda, stated that government must use information technology to improve its efficiency, improve administration of processes and streamline its operations (Department of Communications, 2010). Thus, with the increasing reliance on information systems, one of the challenges facing managers in government is the management of confidential information in information systems (Kaisara & Pather, 2011).

Cerrillo-i-Martínez (2011) adds that transparency in the tender process can be improved by electronic means. However, it is important to note that electronic means can limit transparency if citizens are not empowered and if the technological infrastructure does not deal with the needs of the system user. Furthermore, due to limitations of the transparency principle, Cerrillo-i-Martínez, (2011), suggests that sociological, economical, political and legal arguments exist against the spread of transparency. Furthermore, transparency depends on the types of technology used, access to the technology, and the institutional and political, organisational frameworks that support the technology infrastructure (Cerrillo-i-Martínez, 2011). This points to the need for an appropriate regulation of government information via electronic means.

The tender process must be fair, equitable, transparent, competitive and cost-effective according to the PFMA (Republic of South Africa, 1999). However, this is not always the case as there is often corruption of the tender process. In order to understand the corruption problem in tenders, it is necessary to explain the information security concepts of information confidentiality and conflict of interest. This will be discussed in the next section.

2.6 Information security concepts explained

The section will examine the key information security concepts represented in this study. It is essential that in this research project, these concepts are explained thoroughly because they concepts are not adequately managed in the tender process, and therefore continue to be a problem. Information confidentiality and conflict of interest will now be clarified.

2.6.1 Information confidentiality

Confidentiality assures that access is confined to those who have authority (Barham, 2010). The term refers to the protection of information so that it cannot be used against the interest of the government. The information system used in the tender process has to ensure that information is not made available to any official other than those involved in the process. Furthermore, information which is available to those who should not have access is an information security breach (ISO/IEC 27002, 2005; Flowerday & von Solms, 2007). A loss of confidential information is at times, considered to be present in the tender process (Paton, 2010; Cerrillo-i-Martínez, 2011; Gordhan, 2012).

This leads to information manipulation and biased decisions are made on the awarding of a tender (Gordhan, 2011). Slay and Koronios (2006) add that confidentiality can be compromised by one or more of the three methods of interception: Interception through direct observation of data in an office environment. For example, an official who provides the system logon details to a colleague to access the tender information system. Network interception refers to data which is read as it is transmitted on the network. For example, some officials can access information on the department's network, due to a number of reasons, even though they are not privy to the information. Electromagnetic interception refers to wireless networks. For example, an official's laptop uses a wireless connection to the network and this connection is intercepted by a second unauthorised laptop which also uses a wireless connection. This interception will allow the second laptop to read information stored in the first laptop.

While confidentiality is an obligation of the officials to protect government information, it must be noted that a lack of information confidentiality encourages certain officials to take advantage of the system's security weakness. This results in tender fraud which is a growing concern in South Africa. Tender fraud is committed when there is a conflict of interest and a weakness in the information security mechanisms in the government can be exploited. Conflict of interest will now be discussed in the next section.

2.6.2 Conflict of interest

A *conflict of interest* within the government context is defined as a public servant acting or failing to act on a matter in which he or she has an interest or where another person or entity that stands in a relationship with them, has a vested interest (Department of Human Settlements, 2009). Public servants or departmental officials who do not disclose any business, commercial, and financial interest undertaken for financial gain contribute to the corruption of the tender process. Furthermore, departmental officials who place themselves under any financial obligation to individuals or organisations that influence the performance of their duties will also aid corruption of the tender process (Huntley, 2010).

However, the presence of a conflict of interest is independent from the execution of the improper act. Therefore, a conflict of interest can be discovered and voluntarily defused before any corruption occurs (Hellriegel et al., 2007). The existence of a conflict of interest may not, in and of itself, be evidence of wrongdoing. It is sometimes impossible to avoid having a conflict of interest (Hellriegel *et al*., 2007). A conflict of interest can, however, become a legal matter, for example when an individual tries and/or succeeds in influencing the outcome of a decision, for personal gain (Hellriegel et al., 2007). Otherwise the conflict of interest should be declared, although this is not always done in South Africa (Special Investigating Unit, 2011).

The Auditor General of South Africa reports that three quarters of government tenders in the Eastern Cape Province are awarded to companies owned by government officials and their families (George, 2011). The ANC legislator, Zolile Mrara, stated that a disturbing 74% of tenders were secured by government officials who conduct business with government (George, 2011). It is clear that conflict of interest is a growing problem in the tender process. Furthermore, the audit outcomes by the Auditor General for the fiscal year 2009/10 reflect that R5 Billion of government's expenditure in the Eastern Cape was lost to irregular, unauthorised, fruitless and wasteful expenditure (George, 2011). Most of the money misspent amounted to the value of R4.8 billion which was in the Department of Education (George, 2011). This raises concerns as to whether the tender principles highlighted earlier actually exist and whether the conflict of interest within the department is minimised.

Conflict of interest occurs when an organisation or an individual is in a position to exploit a decision in some way for their personal or corporate benefit. Officials will find themselves in such a position if they have access to confidential information which they are not privy to read. A prohibited or undisclosed representation involving a conflict of interest can subject a person to disciplinary hearings, or criminal proceedings in a case where there is a failure to make mandatory disclosure of an interest.

One such information security model to manage conflict of interest is the Chinese Wall Model. The theory features a mix of free choice and mandatory access. For example, a person can choose what unit of the department to work for, but once that choice has been made, the user is restrained from accessing another dataset which is in conflict with it. The theory also introduces the concept of separation of duty into access control which is vital for upholding confidentiality in the tender process.

A conflict of interest may exist as described above. For example, a member of an organisation from the private sector provides services/goods to the government. This member is related to a government official who makes decisions on the awarding a tender. The official has access to all proposals submitted for tender. This allows the official to compare and contrast information in the proposals. This paves the way for manipulation of information in such a way that it influences the recommendation of an unworthy supplier. The concept, conflict of interest, is often associated with fraudulent actions which corrupt the tender process. This is explained in the next section.

This section makes the link between information confidentiality and conflict of interest. Conflict of interest exists among the government officials in the department. An official may personally benefit by manipulating information not adequately secured. In addition, although certain officials have authority to access confidential tender information, the security thereof still needs to be properly managed. The next section will demonstrate cases where information is used to corrupt the tender process as a result of conflict of interest.

2.7 Real- world government tender cases

This section will review real- world cases to understand where and when a conflict of interest occurs in the tender process. These cases are specific to South Africa and relate to 2010 and 2011.

A. National Department of Housing (DOH)

Tomlinson (2010) pointed out in their case study, based on interviews held with departmental officials, that there is political interference in the appointment of project managers and suppliers. This case study is specific to the delivery of houses to the poor by the government. Local officials were responsible for developing a demand database, managing housing lists, accepting applications for housing subsidies and carrying out a needs assessment to match households to houses. The provincial officials were expected to verify the applications and approve the subsidies. At times the provincial officials would override

the list of beneficiaries approved on the Housing Subsidy System and approve beneficiaries who would normally have been rejected by the system. This system was audited by the Auditor General, and it was proven that the system was overridden during the approval process in order to bypass the national verification process (Tomlinson, 2010).

B. State Information Technology Agency (SITA)

Three cases for SITA were referred to the Special Investigating Unit (SIU). SITA requested the SIU to investigate accusations of procurement irregularities relating to the awarding of a contract and misconduct by a senior government official. The allegations also pertain to the supplier and a third party. A report indicated that there were prima facie indications of contraventions of the Companies Act, corruption, that the Board was misled, and that SITA were now bound to a three-year agreement where they did not have the opportunity to explore all the recommendations made regarding the contract (Special Investigating Unit, 2011). Corruption occurred at steps five, six and seven and the tender process was compromised. The mimimum number of bid committee members required was not present for the bid evaluation and adjudication.

A second SITA case refers to an investigation pertaining to allegations which were levelled against a former Senior Manager in the Limpopo Province, involving procurement irregularities. It was alleged that the former official concluded contracts on behalf of SITA without following the required procurement processes. Nine contracts were involved, with a total value of around R30 million (Special Investigating Unit, 2011). It is possible that most steps of the tender process were exposed to corruption.

A third SITA case refers to an investigation pertaining to various allegations of non-compliance with policies and legislation of a former SITA Senior Manager. This manager had a relationship with certain suppliers and he received personal benefits for resources deployed from those suppliers to specific government departments. Thirteen incidents appear to have occurred amounting to R35 million (Special Investigating Unit, 2011). Steps six and seven were exposed to corruption as the official did not acknowledge interest in the supplier entity who was recommended by the Department.

C. Department of Arts and Culture (DoAC)

There was a need to identify gaps in the department's systems, and to assist with the quantifying of losses suffered, especially the recovery of money. The SIU established the level of legislative compliance at the department, and assisted with the institution of disciplinary, civil and criminal charges against those officials responsible for non - compliance and losses.

The SIU investigated possible conflict of interests where a senior official had an interest in three supplier entities who conducted business with the department. The SIU confirmed a number of conflicts of interest on the part of the official (Special Investigating Unit, 2011). Steps six and seven were exposed to corruption. The suppliers VAT registration details were not vetted by the Department and the senior official did not disclose his/her interest in the supplier entities.

D. National Department of Public Works (NDoPW)

There were 19 cases under investigation in the abuse of emergency delegations. There were deviations from SCM policies and procedures, inflation of bills of quantity, fruitless and wasteful expenditure, corruption and conspiracy between Department of Public Works (DPW) officials and contractors, non-disclosure of outside interests and irregular payments (Special Investigating Unit, 2011). Step two was exposed to corruption as the specifications for the goods/services required from the supplier were not clear and this resulted in the inflation of the bill of quantities. Steps six and seven were exposed to corruption as there was influence on the decisions taken by the bid committees on the recommendation of suppliers/contractors for the emergency tender.

E. Ekurhuleni Metropolitan Municipality

The cases referred to here relate to municipalities, instead of a specific department. It is worth mentioning as the scenario depicted here can occur also at department level.

A supplier to the municipality admitted that he did not complete the tender document presented to him on which the contract was awarded. He admitted that the signature on the tender document did not belong to him. The BEE status as indicated on the document was also incorrect. He is the sole owner and director; however, 70% BEE status was claimed on the bid document. The supply chain management policy was contravened. No needs analysis was conducted prior to implementation of the project. This led to the procurement of unnecessary equipment. The description of equipment, in this case, cameras as specified on the bid specification documents were different to the cameras that had been installed. No variation order was issued and approved for the change in specifications (Special Investigating Unit, 2011).

Another case depicts that an electricity contract of R100 million was awarded to a service provider who did not have the capacity nor the resources to perform in terms of the contract.

If these cases haad occurred in a government department, corruption would be evident in the following steps in the tender process. Corruption was identified at steps one and two as no needs assessment was conducted prior to government's committing funds to the project. Step four was corrupt as the bidder's document submitted to the department was inaccurate

and not checked. Steps six and seven were corrupt as the BEC and BAC did not check for completeness, capability and accuracy of information supplied in the bidder's document. Also the goods supplied by the supplier did not meet the Department's specifications and this was not documented nor was a variation order issued. This is in contradiction of the supply chain policy and procedures.

F. Mpumalanga Department of Education:

A thorough analysis of all documentation (tender submissions, appointment letters, contract extension letters, invoices and supporting vouchers) was conducted by SIU. It was noted that documents, including minutes of meetings for the BSC, BAC and BEC were not available and could not be traced (Special Investigating Unit, 2011). This is highly disturbing as there is no audit trail of decisions taken at the bid committees on the procurement of suppliers. Steps two, six and seven of the tender process were affected. This points to a lack of responsibility and accountability of behalf of the official. Also the official cannot be prosecuted if there is no audit trail pointing to specific users.

G. North West Department of Local Government and Traditional Affairs

A service provider, who was not registered for VAT, was awarded a tender valued at R5.4 million for the cutting of grass at cemeteries. A condition for submitting a proposal for a tender is that the supplier must be registered for VAT (Republic of South Africa, 2003b). Another supplier was paid R432 000 and claimed for VAT despite the fact that the company was not registered for VAT and no SARS certificate was presented (Special Investigating Unit, 2011). The Department did not check for compliance and completeness of the supplier's documentation which was submitted for the tender. Fraudulent activities occurred at steps six and seven.

The number of cases presented here to show the magnitude of the problem of conflict of interest. The cases reflect that easy access to confidential information corrupts the tenders. Together with a poor system of internal controls, officials are not always held accountable for their doing wrong. Also, there is little compliance with the law. The next section summarises the conflict of interest problem.

2.8 Conflict of interest in tender process summarised

Figure 2.1 summaries the essence of this chapter. The process starts with the consumer paying tax to the government. The government uses tax money to provide services to the country via various means. In this case, the service is provided via a government

department. The government provides the department with a budget to manage its organisation and to provide a service(s) to the citizens of the country.

The department will, when needs be, outsource the required work to a service provider via various methods. In this case through a tender process. The tender process in South Africa is weak in terms of information security. The diagram depicts a lack of information confidentiality, unauthorised access to information, tender principles are compromised and that all or most of the members of the bid committees have access to supplier related information. The diagram illustrated that a bid committee member in this case, had a vested conflict of interest in a particular supplier. Since the tender information security is weak, it allows for information to be manipulated. The official takes advantage of this weakness and therefore manipulates the tender information, resulting in a biased decision in the awarding of the tender. This is tender corruption and results in the awarding of a tender to an unworthy supplier. In many instances, the supplier is not competent to deliver the required work to the department. This causes irregular, unauthorised, fruitless and wasteful expenditure. This in turn impedes the delivery of service to the citizens of the country. Consumers who pay tax to the government questioned the value for money. And so the cycle continues.

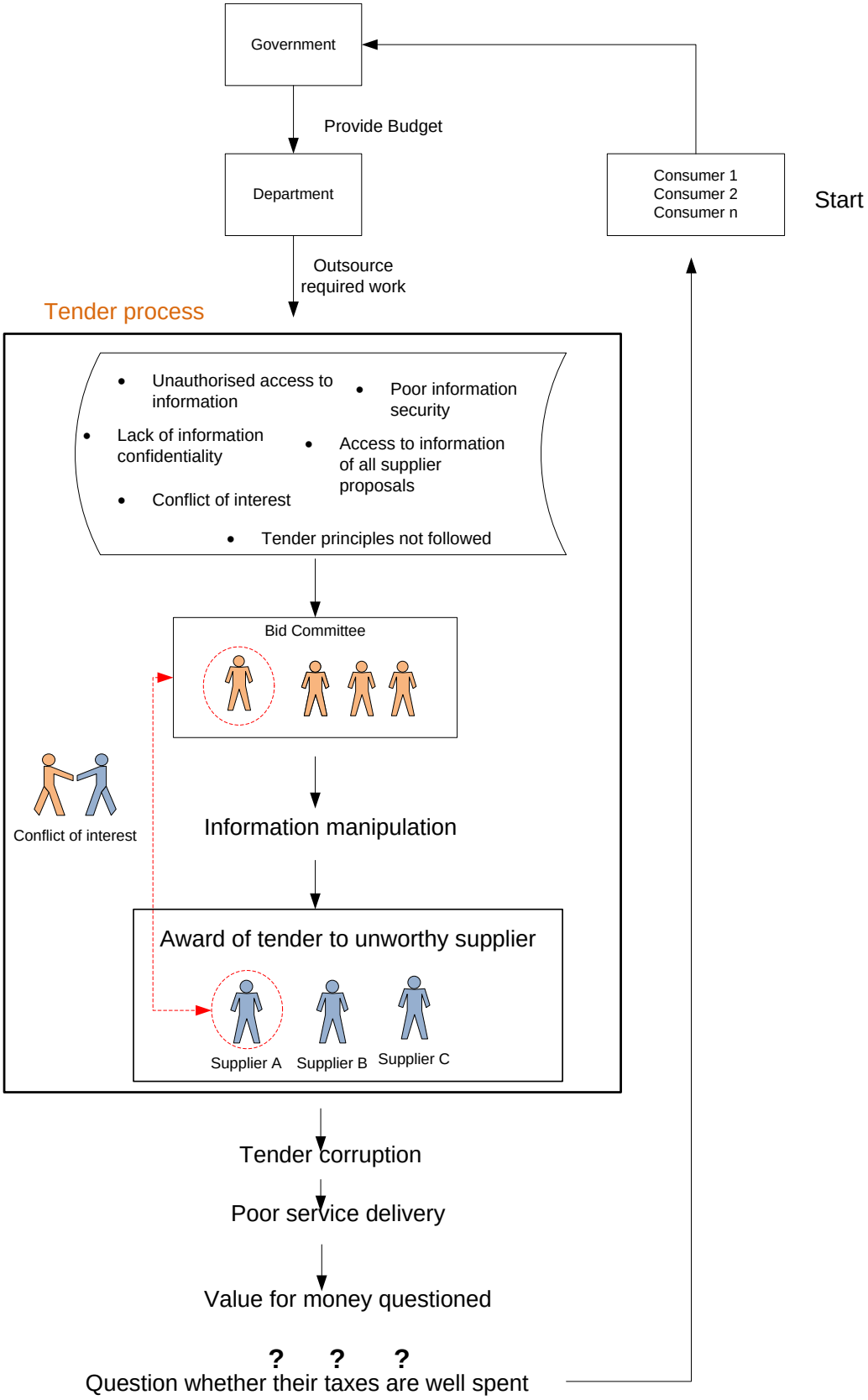


Figure 2.1 Conflict of interest in tender process

(own compilation)

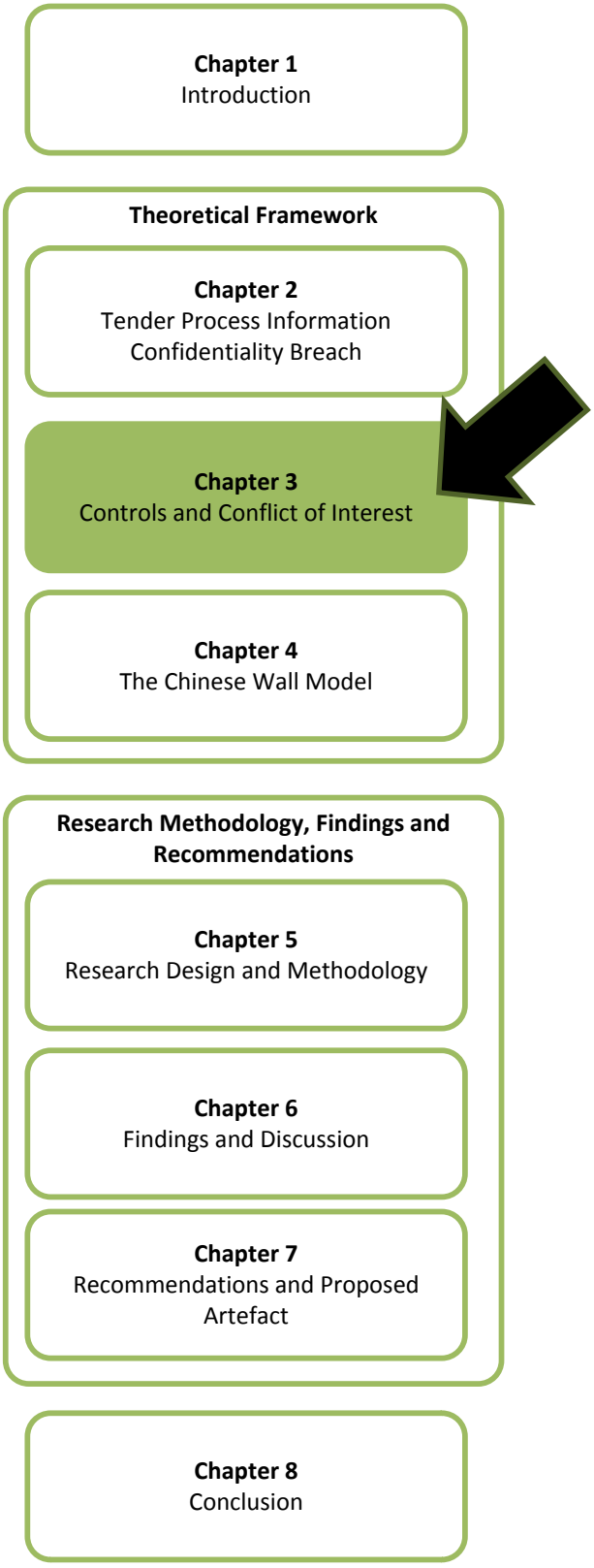
2.9 Conclusion

This chapter explains the high level steps in the government tender process in South African departments. The essential requirements and tender principles which should be in place are reflected. This is followed by an overview of the information systems used and challenges associated with the information system in the tender process. These challenges include how to manage information confidentiality, unauthorised disclosure of information and corruption of some of the tender principles.

An explanation of the concepts, information confidentiality and conflict of interest follows. Thereafter, information security models to manage the lack of information confidentiality and conflict of interest in the tender process are discussed. One such model is the Chinese Wall Model. Presented thereafter are real world cases of fraudulent activities in the tender process. These cases point to the conflict of interest which exists between government officials and suppliers. While corruption can take place at any step in the tender process, most of the corruption is concluded by officials in senior positions (Special Investigating Unit, 2011; Bhattacharya & Marshall, 2012; Gordhan, 2012). These senior officials are members of the bid committees.

This chapter is important to understand the problem being addressed by this research project. The next section will examine the current controls in place to manage the problem in South Africa's tender process. The controls recommended in foreign countries will also be studied.

CHAPTER 3 : CONTROLS AND CONFLICT OF INTEREST



Chapter 3

"Fraud and corruption will be combated through changes to procurement policies and practices and tough enforcement of the law".

Pravin Govin: 2012 Minister of Finance, South Africa

3.1 Introduction

In this section of the study, the researcher investigates the current controls in place to manage information confidentiality in the tender process. This includes an analysis of South Africa's legislation, policies and procedures. This chapter also seeks to highlight the different interventions which government has undertaken to reduce conflict of interest and reduce the breach of information confidentiality in the tender process. Thereafter, an analysis will be conducted on how tender fraud and conflict of interest are managed in other countries in an effort to learn from their processes.

The core focus of this chapter is a system of internal controls. The global technology audit guide known as GTAG1 can be used to understand the different classifications of controls (GTAG1, 2012). Thereafter, a risk assessment model developed, within the Information Technology (IT) security community, known as the Common Criteria Security Model (2009), helps to decide if internal controls have the desired impact and are adequate in controlling the information confidentiality in the tender process. These controls will then be compared against a best practice standard for developing information security controls, namely, ISO/IEC 27002 (2005). The comparison of the existing controls to ISO/IEC 27002 (2005) will be very useful in helping to understand how information security should be addressed in the context of tenders. Furthermore, a substantive review and analysis of international literature published on various tender regulations and controls in developing, as well as in developed countries, will be examined.

The security of information confidentiality does not only refer to the information stored in the system. It also comprises the IT systems that produce, process and store the information (GTAG1, 2012). This includes technological and managerial procedures as well as, software and hardware tools (Pardo, Pino, Garcia, Piattini & Baldassarre, 2011) .

This chapter will therefore focus on:

- South Africa 's regulations applicable to internal controls in the tender process.
- Internal controls compared against the Common Criteria Security Model.
- Internal controls compared against the ISO/IEC 27002 (2005).

- Tender fraud and control of information confidentiality in international countries.

3.2 Internal controls

Internal and information security controls are important for improving accountability of resources and preventing tender fraud. In addition, they provide for consistent reporting of expenditures and ultimately, improving service delivery to citizens.

Countermeasures put in place to ensure that government internal information is accurate, reliable and kept confidential are referred to as internal controls. Government departments usually have, as part of their risk management, a system of internal controls intended to counteract inherent risks. Slay and Koronios (2006) point out that internal controls take the form of operational, financial or administrative controls.

Internal controls, are important from a legislative point of view, are firstly, data protection and privacy of personal information, secondly, safeguarding of organizational records, and thirdly, intellectual property rights (ISO/IEC 27002, 2005).

Internal controls, which are important from an information confidentiality point of view, include information security policy documents, allocation of information confidentiality responsibilities, information confidentiality awareness, education and training, correct processing in applications, vulnerability management, business continuity management, management of information confidentiality incidents and improvements (ISO/IEC 27002, 2005). The system of internal controls can only apply to the system or to the internal environment. These refer to the resources or systems used in the tender process in government. The external environment is not addressed or controlled by the system of internal controls.

Figure 3.1 System of internal controls illustrates how the various controls work together and interact as *a system of internal controls*. This figure helps to classify and understand the control's purpose. IT controls support governance and business management as well as providing general and technical controls over policies, processes, systems and people that comprise IT infrastructures (GTAG1, 2012).

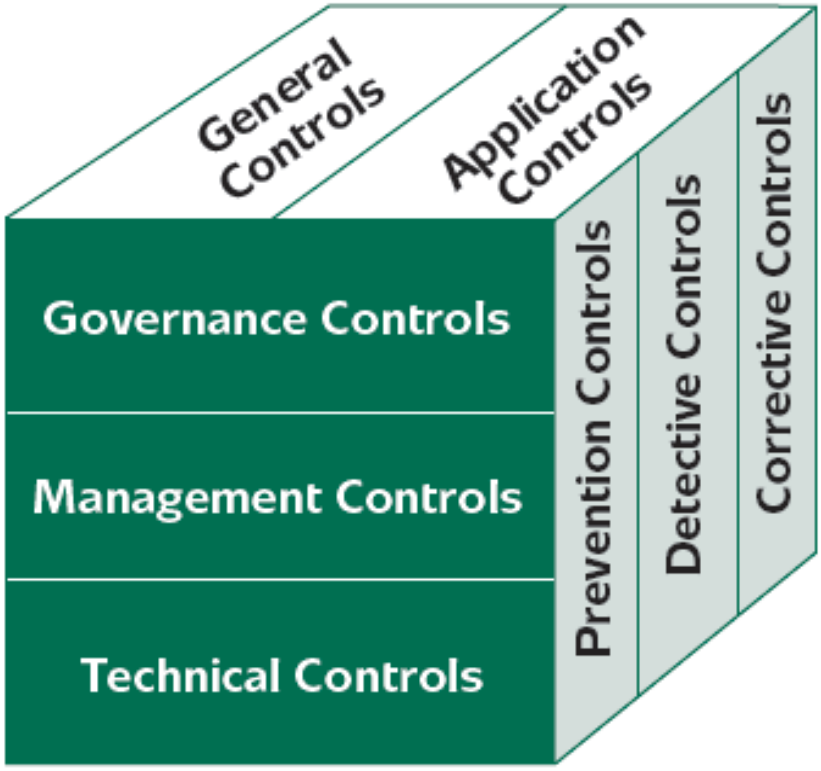


Figure 3.1 System of internal controls

These include the processes that provide assurances for information and assist in reducing associated risks. These risks are fraud and confidentiality breach of tender information. It is necessary to understand the different classification of controls to pinpoint where the Chinese Wall Model can be applied to reduce the conflict of interest. IT controls are either General or Application controls (The Institute of Internal Auditors, 2012). GTAG 1 (2012) assists to clarify general and application controls which are elaborated below.

- **General controls:** These are general computer controls, information technology controls and infrastructure controls. These controls include IT governance, risk management, resource management, IT operations, application development and maintenance, user management, logical security, physical security, change management backup and recovery and business continuity. They support the functioning of programmed application controls and the policies and procedures that ensure the continued operation of computer information systems, e.g. backup, recovery, and business continuity. General controls also include segregation of duty and access control. Segregation of duties is a type of control which can be enhanced with the use of the Chinese Wall Model. The Chinese Wall Model takes the security measure one step further. Although a user has

access to information as per their security level, that user should still be limited to the information they can access within the defined security level.

- **Application controls:** These pertain to the individual business processes, application systems or programmed procedures in application software. In addition, manual procedures, designed to ensure the completeness and accuracy of information processing, are incorporated. For example they include: data edits, balancing of process totals, transaction logging, and error reporting and manual procedures to follow up on items listed in exception reports.

The next group of control classifications, specifically, governance, management and technical controls, will be explained.

- **Governance or operational controls** are intended to administer the operations of the tender process. They are based on process-level measures that the government has to enforce. These are usually derived from a department's business strategy to achieve the objectives of the tender process. Senior government officials should therefore ensure that governance controls are in place and adopted across functional areas. Liu and Lin (2012) add that operational controls will reduce inconsistencies in the tender process and its outcomes. This implies that a well-documented description of the tender controls must be in place to manage information confidentiality. Furthermore, a methodology for implementing these controls is necessary. Operational controls must ensure that technical and management controls work effectively and efficiently (GTAG1, 2012).

- **Management controls** are controls which are implemented throughout government. These controls are deployed by management to manage risks to government, its processes and assets. It is in the form of policies and guidelines to implement information security or in this case, information confidentiality (van Niekerk & Von Solms, 2010). Senior officials implement management controls to streamline the procedures towards attaining the tender objectives.

- **Technical controls** usually refer to checks at the machine level or network level (GTAG1, 2012). They include software and hardware controls which are aimed at preventing a breach in information confidentiality. They also include detecting a breach that has already occurred. These controls include system controls, database control, encryption and logging.

It is the responsibility of government officials to be accountable for decisions made in government (Gordhan, 2011). These decisions must be made on accurate information.

Hence, information must be kept secure and free from manipulation. An effective system of internal controls can achieve this.

It can therefore be concluded that a system of internal controls assists government officials to fulfil their responsibility by protecting government assets (tender information assets) from internal or external threats as well as from direct or indirect threats. A system of internal controls is core to the government's risk management practice. These controls will assist government officials to make accurate decisions concerning the tenders and thus steer the award to a worthy supplier.

The function of a control is relevant to the assessment of its design and effectiveness (Australian Government, 2011). Therefore, controls are often categorised into three groups: *preventative*, *detective* and *corrective* controls. The following are examples of these three control categories (GTAG1, 2012):

- **Preventative controls** prevent risks from occurring in the tender information system. The control must limit or prevent unauthorised access to the tender information. The focus here is to avoid a breach of information confidentiality. This breach is usually in the form of intentional human interference with information.
- **Detective controls** warn the government of security violations or attempts to breach the security of the information. These controls detect when a breach of confidential information has occurred. The detection of the security breach will require corrective action(s).
- **Corrective controls** aim to minimise the consequences of a risk which has occurred. Controls include correction of errors, omissions and incidents once they have been detected.

Understanding the different control categories enables the control analyst and auditor to establish the control position in the control framework. Therefore the classification of these controls assists the responsible IT government official to determine whether detective controls are adequate to identify a possible breach of information confidentiality.

Assessing IT controls involves selecting key controls for testing, evaluating, testing of results and determining whether evidence indicates any significant control weaknesses (Lopez & Gary, 2010). Appendix A provides a checklist for examining the IT control framework to ensure that the government has addressed all elements of control. This checklist will help to ensure that all control elements have been considered when performing an internal audit assessment of IT controls. These key regulations will be addressed in the next section.

3.3 Government Regulation and the tender process

The management of information in records or information systems is a prerequisite of democratic government (Kaisara & Pather, 2011). South Africa's law and regulation on procurement direct the government to act in an equitable, transparent and accountable manner in the administration of its responsibilities (Pereira, 2009). In contrast, a lack of information confidentiality and persistent corruption are the perceptions commonly associated with the tender process. The corruption problem with government tenders is viewed by members of communities as being manageable and special efforts are placed on solving this problem (Gordhan, 2012). On the other hand, corruption of the tender process has become worse despite all conceited efforts to solve the problem (Gordhan, 2011).

When the internal controls of government were audited, it was determined that there was insufficient compliance with law and regulation in certain departments (Special Investigating Unit, 2011). The Preferential Procurement Policy Framework (PPPFA) Act (5 of 2000) (Republic of South Africa, 2011), the Broad-Based Black Economic Empowerment (B-BBEE) Act (2003) and the Prevention and Combating of Corrupt Activities Act, 12 of 2004 are examples of South African legislation aimed to guide the control of operations in the tender process. These will now be clarified in more detail.

3.3.1 The Preferential Procurement Policy Framework (PPPFA) Act

The PPPFA Act (2000) and its regulations also provide rules concerning the access of confidential information to individuals who should not necessarily have access. If access to a record is deferred in terms of subsection (1) of the PPPFA Act (2000), an information officer must notify the person making the request:

(a) that the requester petitioner may, within 30 days after notice is given, make representations to the information officer why the record is required before such publication or submission,

(b) the likely period for which access is to be deferred,

(c) if a requester petitioner makes representations in terms of subsection (a) the information officer must, after due consideration of those representations, grant access only if there are reasonable grounds for believing that the requester will suffer substantial prejudice if access to the record is deferred for the likely period referred in subsection (b) of the PPPFA Act (2000).

This point to the need for effective access control mechanisms for tender information. This is where the Chinese Wall Model becomes useful. The model has a property referred to as

sanitisation. This means that the identity of the record (supplier) must remain unidentifiable. In other words, if a supplier's proposal in the tender process needs to be accessed by a government official who should not have access, but needs access for certain decision-making, then that record can be made available to the official or requester of the information. However, the identity of the supplier must remain unknown to the official. This will reduce the chances of a biased decision which could arise if an official has a vested interest in a certain supplier.

With regard to tendering, the most important law passed is the PPPFA and the accompanying regulations (Republic of South Africa, 2000a). This law introduces a system of evaluating tenders in terms of a package of adjudication criteria with a maximum total of 100 points. Each bid or proposal submitted by a supplier, is evaluated in terms of the agreed criterion. Thereafter, the highest scoring bid in terms of all the criteria combined wins the tender.

The preference point system introduced by the PPPFA is based on the definition of a "Historically Disadvantaged Individual" (HDI). A HDI citizen is any South African citizen who has no franchise in national elections prior to 1994, who is female, or who has a disability. What makes the system fairly complicated is not all kinds of disadvantage receive the same number of points (Republic of South Africa, 2000a).

In order to explain how the preference point system works, it is necessary to explain two examples. Commonly, price is simply one factor amongst many other factors - such as experience in the work being considered, capital backing and number of staff located locally. For the two worked examples below, only two factors will be considered: price and HDI status:

$$Ps = 80(1 - \frac{Pt - P\min}{P\min})$$

Ps = Points scored for price of bid under consideration

Pt = Rand value of bid under consideration

Pmin = Rand value of lowest acceptable bid submitted

Tenders of less than R1 million in value are adjudicated according to the 80/20 preference point system (Republic of South Africa, 2011). According to 80/20 formula, a bid of R120

000 from a bidder with maximum HDI points will beat a bid of R100 000 with no HDI points (Republic of South Africa, 2000a).

Tenders of over R1 million in value are adjudicated according to the 90/10 preference point system (Republic of South Africa, 2011). According to this formula, a bid of R1,1 million with maximum HDI points will beat a bid of R1 million with no HDI points.

3.3.2 The Broad-Based Black Economic Empowerment (B-BBEE) Act

The second law of importance is the B-BBEE. The Minister of Trade and Industry has issued codes of good practice on BEE (Republic of South Africa, 2003c), and is responsible for issuing a strategy and a plan for the financing of broad-based black economic empowerment. With the publication of a number of codes of good practice by the Department of Trade and Industry in December 2006, a measure of certainty has been achieved as to how tenders should be adjudicated in those sectors. However, with the 100 point scorecard system, there are six areas of BEE opportunity: management control (15 points), employment equity (15 points), skills development (20 points), preferential procurement (20 points), enterprise development (15 points), and socio-economic development (15 points) (Republic of South Africa, 2003c). It must be noted that there are weaknesses in these controls.

According to the B-BBEE Act, 'black people' is a generic term that includes Africans, Coloureds (including Chinese) and Indians (Republic of South Africa, 2003c). However, legal practitioners have pointed out two conflicts between the B-BBEE Act and the PPPFA (Tenderscan, 2012). Firstly, the B-BBEE Act's definition of black people differs from the HDI definition in the PPPFA. Secondly, the PPPFA only lists one way of obtaining preferential points (i.e. ownership equity), while the B-BBEE Act provides for six areas of BEE opportunity. In terms of Regulation 5 (2) and 6(2) of the PPPFA, preference points must be awarded to a bidder for attaining the B-BBEE status level of contribution (Republic of South Africa, 2011).

It must be noted that the weaknesses identified are necessary and important as they point to key law and regulation which are intended to guide the tender process. Subsequently, weaknesses in these regulations allows for easy manipulation of tender information where a conflict of interest exists. Corrective action should be taken by the necessary authorities to correct these weaknesses. This raises concern and provokes the need for government to critically analyse all laws governing information security applicable to the tenders. This is however, not within the scope of this study. The next Act, Prevention and Combating of Corrupt Activities Act, 2004, (Republic of South Africa, 2004) will be examined.

3.3.3 The Prevention and Combating of Corrupt Activities Act

The third piece of legislation of importance for tendering is the Prevention and Combating of Corrupt Activities Act, 12 of 2004. According to this law, both the person who offers a bribe and the official who accepts the bribe are guilty of corruption. The bribing of public officials is a crime as well as the offering of inducements for the awarding of a tender. Furthermore, a conflict of interest can become a legal matter when an individual tries and/or succeeds in influencing the outcome of a decision, for personal gain (Republic of South Africa, 2004).

As a corrective measure, the maximum sentence that can be imposed by a High Court for the offence of corruption is life imprisonment or a fine (Republic of South Africa, 2004). Once a person is found guilty of such an offence, his or her details are entered in the register for tender defaulters. This register is established by the Minister of Finance within the National Treasury (Department of Human Settlements, 2009). This registry is open to the public, municipalities and government departments to prevent those listed in the register from tendering in the future. This forms part of a preventative control.

Suspicion of conflict of interest over the awarding of tenders often ends up in court because one bidder appeals against the award (step ten in the tender process, Chapter two). This is not the only way that corruption can be exposed.

An alternative method of uncovering conflict of interest and fraud in the awarding of tenders is by reporting the matter to the National Director of Public Prosecutions (of the National Prosecuting Authority of SA), who then appoints an investigator to investigate the matter of the security of tender information. This forms part of a Detective Control.

Apart from the laws governing tendering, the government has published guidelines to assist members of the public service to conduct the tender process in a fair manner. A few of these laws and regulations are listed below where the relevant section of the document for this study is extrapolated and summarised.

Table 3.1: Legislation pertaining to government tenders and information confidentiality

Document	Relevance to Tender Process
Public Finance Management Act (1999) (PFMA)	: Maintain an appropriate procurement and provisioning system, which is fair, equitable, competitive and cost effective – Section 38(a)(iii) : Discovery of an unauthorised, irregular or fruitless and wasteful expenditure must immediately be reported in writing with particulars of expenditure to the relevant treasury department. In the case of irregular expenditure involving the procurement of goods/ services, the report must go to the relevant tender board – Section 38(g)
Regulations of the Public Finance Management Act, 1999 (2003)	: All role players to comply to ethical standards as stipulated in Section 8 : the accounting officer/authority of an institution must avoid the abuse of the supply chain management system as detailed in Section 9
The Preferential Procurement Policy Framework Act (2000) (PPPFA)	: Together with IT regulations, provides for the implementation of the preference point system in the allocation of contracts for the different categories of service providers
The Constitution of the Republic of South Africa (1996)	: When an organ of state in the national, provincial or local sphere of government, or any other institution, identified in the national legislation, contracts for goods or services, it must do so in accordance with a system which is fair, equitable, transparent, competitive and cost-effective – Section 217 (1)
Supply Chain Management Policy Framework and Procedure Manual (2009)	: A manual which should be used to guide and provide procedure and control to achieve the desired output of the tender process
The Promotion of Access to Information Act (2000)	*:* An objective is to promote transparency, accountability and effective governance of all public and private bodies by empowering and educating everyone
The Prevention and Combating of Corrupt Activities Act (2004)	: Provide for the strengthening of measures to prevent and combat corruption and corrupt activities : To provide for the offence of corruption and offences relating to corrupt activities : To provide for investigative measures in respect of corruption and related corrupt activities : To provide for the establishment and endorsement of a register to place certain restrictions on persons/enterprises convicted of tender corruption :To place a duty on certain persons holding a position of authority to report certain corrupt transactions : To provide for extraterritorial jurisdiction in respect of the offence of corruption and offences relating to corrupt activities
The Promotion of Access to Information Act (2000)	: An objective to promote transparency, accountability and effective governance of all public and private bodies by empowering and educating everyone
Public Service Anti-corruption strategy (2002)	: The strategy considers preventative and combative controls for eradicating corruption in Government

Regarding procedures and administrative actions, the public sector official is bound to comply with the directives and limitations contained in Table 3.1. The implementation of tender process management plays a significant role in every government department

(Department of Human Settlements, 2009). Adequate controls should be in place for an effective tender process and the prevention of over- and- under expenditure. These controls must also ensure that mechanisms are in place to manage the corruption of tender information.

A system of internal controls must encompass political legitimacy and accountability, administrative accountability, financial and budgetary accountability, transparency, openness, rule of law and, of course, information security (GTAG1, 2012). The officials, who are responsible for government resources, should be able to account for the decisions made in the tender process. This signifies the superiority of public interest over private interest. It is therefore of utmost importance that conflict of interest is managed and the flow of information among officials is controlled. A means of doing this is to ensure transparency of the evaluation of tenders and decisions made on the bids.

Transparency, being a major component of internal controls, means that decisions taken and their enforcement are executed, based on clearly stipulated rules and regulations, known to all in government. A component of good governance includes transparency in the awarding of tenders, the executive responsible for formulation of sound policies and ensuring effective functioning of the public service.

Over and above the regulations, policies and procedures, which should be in place to manage tender information and its confidentiality, there are government interventions which support the control of tender fraud. These interventions will be looked at briefly below.

3.4 Government interventions

Besides the law and regulations which control the tender process, government interventions consist of groups of people who are also responsible for combating fraud in the tender process on behalf of the government. These interventions seek to curb fraud at the Preventative, Detective and Corrective levels. It should be noted that these interventions are implemented by external parties of the government departments. However, mentioning as they seek to tighten internal control within government.

3.4.1 Multi-Agency Working Group (MAWG)

The Minister of Finance set up the Multi-Agency Working Group on procurement to make procurement systems more efficient and eliminate abuse (Special Investigating Unit, 2011). The following measures were suggested for implemention:

- Monitor capabilities to detect fraud at an early stage.
- More transparent public disclosure of tender processes.

- Centralisation of some procurement processes to enable better control.
- Heavy penalties of up to double the contract value for suppliers involved in tender fraud.
- To recover losses from corrupt officials.

3.4.2 CorruptionWatch

CorruptionWatch is a non-profit organisation launched in January 2012. This organisation relies on the public to report corruption. Those involved use the reports as an important source of information to fight corruption and to hold leaders accountable for their actions (CorruptionWatch, 2012).

CorruptionWatch provides a platform for reporting corruption. Anyone can safely share what they experience and observe and can speak out against corruption. Their communication platform includes their website, an SMS line, social media, email or post. They investigate selected reports of alleged acts of corruption.

CorruptionWatch will gather and analyse information to identify patterns and hot spots of corruption (CorruptionWatch, 2012). They build campaigns that mobilise people to take a stand against corruption and encourage good governance, especially in tenders. Adherence to good governance creates an environment where corruption struggles to flourish. Failure to adhere to the practices of good governance means that stakeholders increasingly demand accountability. This prompts a need for an information system to centrally store all cases of fraudulent acts. The information system plus adeqauate internal controls will positively affect the security of confidential information.

3.4.3 Case Management System

The government of South Africa has established a web-based corruption system to manage and provide a central mechanism to record the fraudulent acts associated with government officials. It also keeps a record of cases which have been reported to the National Anti-Corruption Hotline.

In addition, the purpose of the system is to assist the leadership of the South African government to access these reported cases and intervene to work towards eradicating fraud (van Rijswijck, 2011). This sytem is fairly new and was completed in 2011. This shows that government is continuously taking steps to improve the reporting of fraudulent incidents in government.

It also demonstrates that government is moving towards a more effective and central method of recording cases of corruption. This is a reactive measure. The approach of the Chinese Wall Model on the other hand is proactive. Its approach is focused on reducing conflict of interest by managing the confidentiality of tender information.

3.4.4 Special Investigating Unit (SIU)

Effective management of information in information systems can reduce corruption in government tenders (Pereira, 2009). In addition, individuals who corrupt the tender process must be reported and the public must be made aware of their identity. This is corruption awareness which will assist in reducing future corruption.

To assist in this regard, the SIU has been tasked to provide assistance in combating fraud in the government. The SIU was established to investigate corruption and maladministration in government and to report on the findings of these investigations. The SIU is funded through the Department of Justice and Constitutional Development (Special Investigating Unit, 2011). Reported in the Special Investigating Unit Annual Report 2010/2011, government contracts to the value of about R15 billion were identified as having irregularities. Of these, about R10 billion related to possible procurement irregularities and R5 billion to possible conflicts of interest (Special Investigating Unit, 2011).

This raises concern as to whether government regulations and interventions, highlighted above, actually exist and if they are used to reduce conflict of interest to manage information security. This points towards the need for regular assessment of the current controls in place. This is explained in the next section.

3.5 Assessment of controls: Common Criteria Security Model

Information technology provides opportunities for growth and a competitive advantage for government. It also provides the means and tools to meet threats they exploit. These threats can be from outside attackers or from trusted insiders. Information Technology (IT) can also provide protection from threats. IT controls do not exist in isolation, but form part of the overall system of internal controls (GTAG1, 2012), which in turn, are an integral part of enterprise risk management. These IT controls promote reliability and efficiency. IT supports the government to adapt to change in an environment which has many tender risks.

Risk is understood to be an event or condition that may occur. The occurrence, if it does take place, has a harmful or negative effect that can adversely affect the prospects of achieving a desired goal. Therefore, risk management relates to decisions about such potentially harmful or negative effects (Artiua, Smith & Bower, 2011). One of the sub-processes of risk management is identification (Artiua *et al*., 2011).

Ma and Ma (2011) observe that the identification phase is critical since it has an enormous effect on the decisions that emanate from the risk management process. Despite these observations, the bulk of risk management research is focused on the analysis and response

phases; and yet it stands to reason that if risks are not identified they cannot be analysed and managed (Common Criteria Security Model, 2009).

Good risk management is considered a critical ingredient for the success of organisations (GTAG1, 2012). Several professional institutions such as the Project Management Institute (PMI), Association for Project Management (APM) and Institute for Risk Management (IRM) have undertaken to provide best practice guidance and risk management bodies of knowledge to enable organisations to effectively manage risk and to make decisions. Both public and private sector organisations have tapped into this body of knowledge to provide guidance on managing risk in project environments. One such model used to evaluate security of information is the Common Criteria Security Model (Common Criteria Security Model, 2009).

The Common Criteria Security Model (2009), which is illustrated in Figure 3.2, is an effective, diagrammatic representation of the critical areas of security and the relationships between them (Common Criteria Security Model, 2009). System evalutors use the criteria to determine whether controls conform to the security requirements of information security, particularly, the management of confidential information. Hence, the model can serve as a means of evaluating the controls in the tender process. In other words, the model serves to evaluate whether a system meets or fails to meet the security of information in the tender process.

It provides a list of criteria to be checked in the system. It provides management control to keep track of the threats. It describes general actions to be carried out and security functions on which to perform the actions. The CCSM is orientated towards evaluating devices such as firewalls and encryption boxes (Common Criteria Security Model, 2009). The principles introduced by the CCSM are applicable to this study because it is necessary to identify the threats, risks and countermeasures needed for securing the confidentiality of tender information.

Thus the Chinese Wall Model, which is similar to the concept of the firewall (Slay & Koronios, 2006), provides an excellent countermeasure for managing conflict of interest in the context of government tenders. The CCSM can be used to evaluate the effectiveness of the Chinese Wall Model in the tender process.

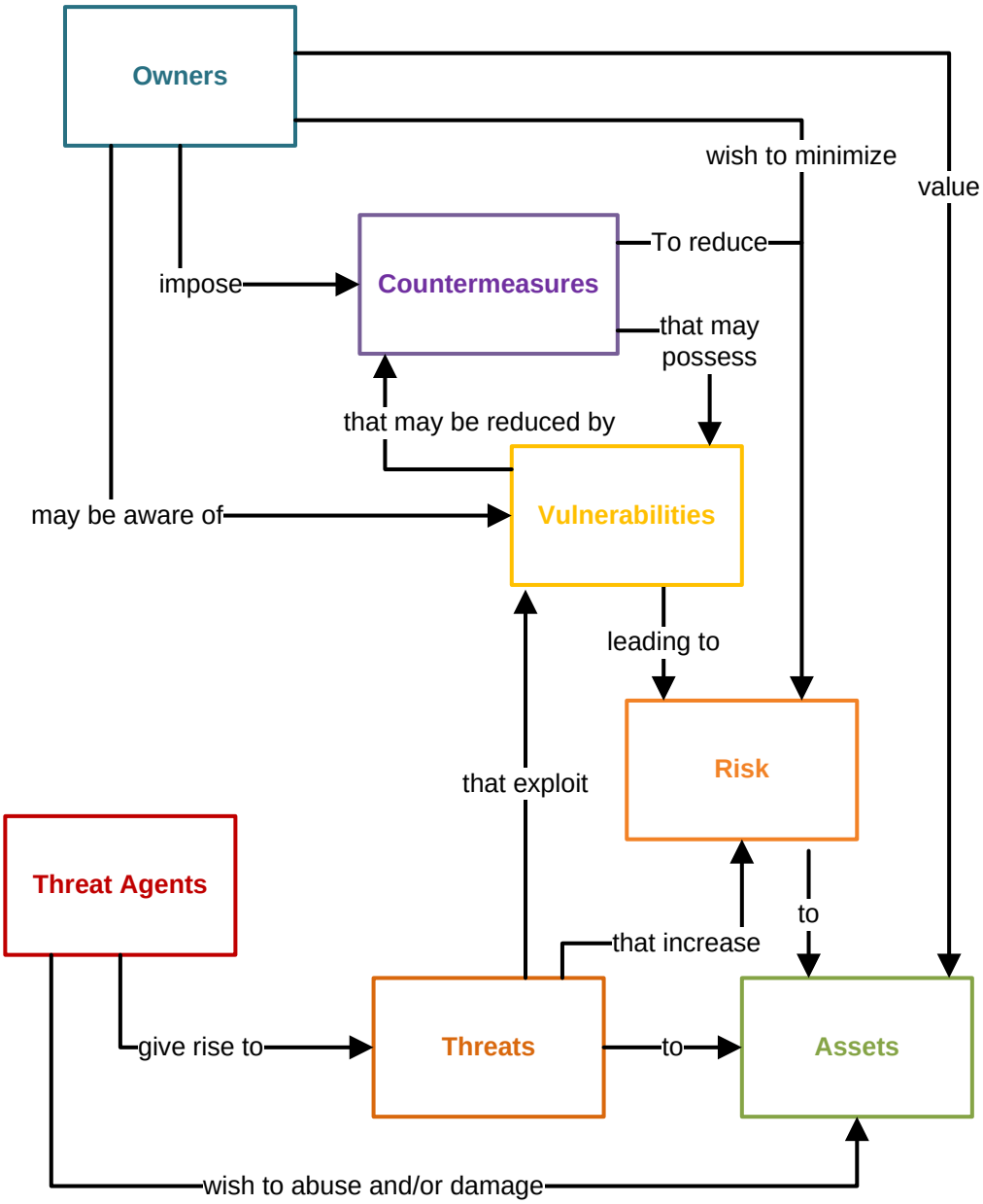


Figure 3.2 The Common Criteria Security Model (Common Criteria Security Model, 2009)

When applying the CCSM model to the tender process, one notes that **threat agents** are fraudulent government officials and suppliers. They give rise to **threats**, or the presence of the ability to commit tender fraud. These threat agents will essentially have a conflict of interest which will lead to a desire to manipulate information and make biased decisions on the award of a tender. It is important to properly identify threats and vulnerabilities because there may be several vulnerabilities associated with one threat. If the more specific vulnerabilities are not identified, necessary controls may be omitted with the result that the conflict of interest is not reduced to an acceptable level and therefore the system of internal controls is inadequate.

Vulnerability is more specific than a threat (Slay & Koronios, 2006). Vulnerability is a weakness that can be used to violate the security requirements in the tender process. A threat is a warning that something is about to occur.

Conflict of interest is the reason why these agents pose such a threat within the tender process environment. In addition, the conflict of interest threat regarding information seeks to exploit weaknesses and vulnerabilities of the tender systems (Common Criteria Security Model, 2009).

For example, the high dependency on information in the tender process for decision-making can be exploited if officials have firstly unauthorised access to information, or secondly, have access to all proposals submitted for a particular tender which can lead to biased evaluation of the proposals. The conflict of interest threat will always exist, but it is the conflict of interest risk that can be managed and reduced to a more acceptable level.

As a result, the objective is to reduce the conflict of interest and manage information confidentiality. Hence, the focus of the study is not the threat itself. Table 3.2 summarises the common criteria identified in the tender process.

Table 3.2 The Common Criteria Security and tender process

Common criteria	Identified in the tender process
Owner	• Government departmental officials
Countermeasures	• Legislations and regulation • Internal controls with the tender information system • Chinese Wall Model application
Vulnerabilities	• Poor system of internal control
Threat agents	• Dishonest government officials • Fraudulent suppliers
Threats	• Conflict of interest • Unauthorised disclosure • Lack of information confidentiality
Risk	• Fraud • Information manipulation • Information confidentiality breach • Biased award of tender
Assets	• Tender related information

The **owner** side of the model must be considered. The owners are the responsible government officials in the tender process. The owners, whether they are aware of their

vulnerabilities or not, require countermeasures to be imposed to effectively reduce their vulnerability to breach of information confidentiality. This can reduce the conflict of interest risk, thus protecting the information they value. An effective countermeasure, a set of security controls such as the ISO/IEC 27002 (2005) will be discussed below.

3.6 Application of the ISO/IEC 27002 (2005)

The UK government understands the importance of Information Technology (IT) best practice, and has developed IT best practices standards to assist private and public sector organisations around the world. One such international security management standard is the ISO/IEC 27002 (2005). The ISO/IEC 27002 (2005) is a code of practice to address information confidentiality, integrity and availability risks (Placeholder4).

If the South African government were to adopt the ISO/IEC 27002 (2005), they should assess the information security risks as identified in the Common Criteria Security Model and apply suitable controls. Thereafter, controls can be selected from ISO/IEC 27002 (2005) or from other control sets, or new controls can be designed to meet specific needs when appropriate. The controls in the ISO/IEC 27002 (2005) international standard can be considered as guiding principles for information security management in a government department.

However, not all of the controls and guidance in this code of practice may be applicable to government. Furthermore, regulations and policies which guide the government tender process, such as those mentioned earlier, should be cross-referenced to clauses in this standard, where applicable, to facilitate compliance checking by information security officers in the government.

Refer to ISO/IEC 27002 (2005) which explains the controls in detail and gives guidance on how to implement the control. Presented below in Figure 3.3 is a high-level overview of the controls. These controls are described below. Note that only the sections of the controls which are most relevant to conflict of interest, information confidentiality and the tender systems are described.

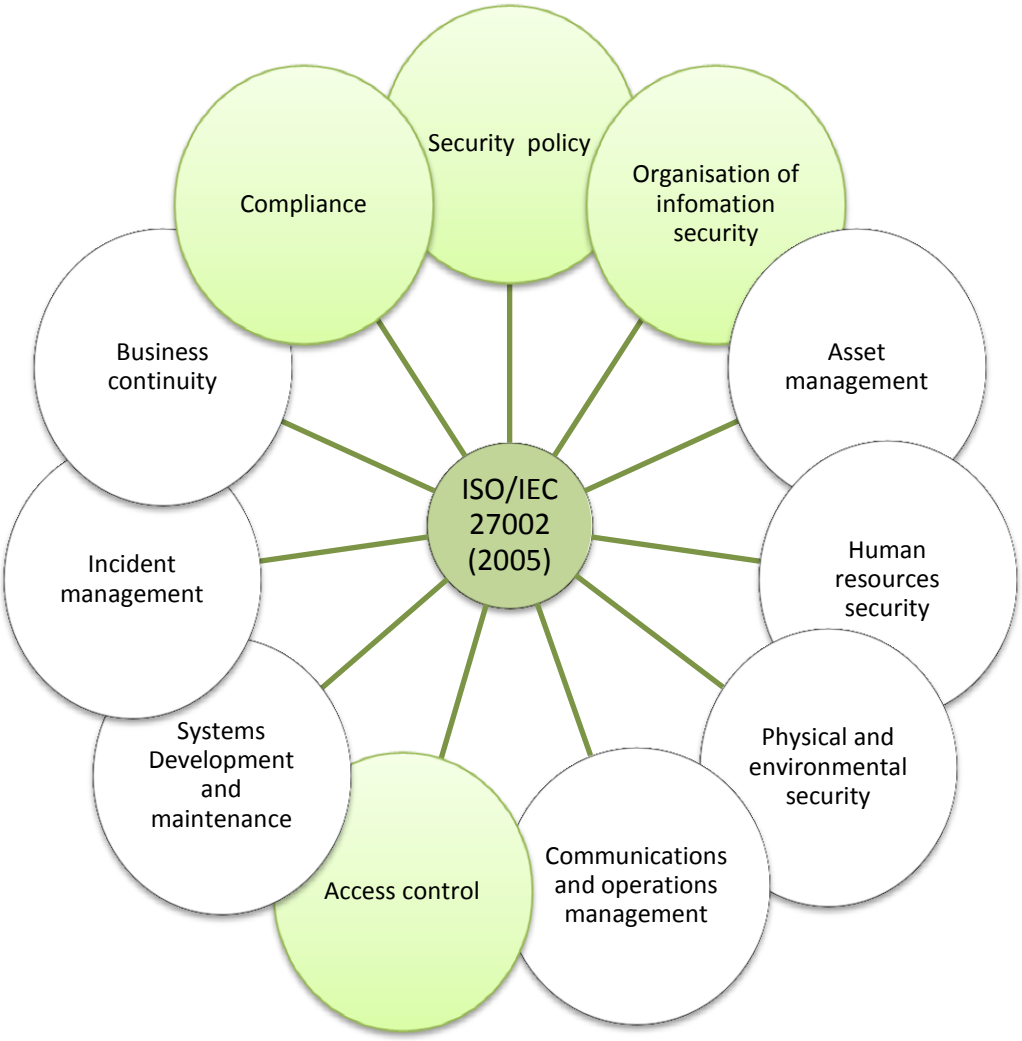


Figure 3.3 ISO/IEC 27002 (2005)

The first control to consider is the ***information security policy.*** An information security policy document should be formulated and implemented by senior officials in the government. It must be published and communicated to all employees as well as to relevant external parties. The information security policy should be reviewed at planned intervals to ensure its continuing suitability, adequacy, and effectiveness (ISO/IEC 27002, 2005).

The second control is ***organisation of information security***. This control stipulates that management should support security within the organisation through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities. Information security activities should be co-ordinated by representatives from different parts of the government with relevant roles and job functions. Security responsibilities concerning information should be clearly defined (ISO/IEC 27002, 2005).

Requirements for confidentiality or non-disclosure agreements reflecting the government's need for the protection of information should be identified and regularly reviewed. For

example, bid committee members need to sign an oath of secrecy document which stipulates that information should not be disclosed to suppliers or any other person not officially connected to the tender process. Information such as the evaluation and the award of a contract should not be disclosed to unauthorised persons before the award of the contract to a successful bidder (Department of Human Settlements, 2009). Appropriate contacts with relevant authorities should be maintained. Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained (ISO/IEC 27002, 2005).

The government approach to managing information security and its implementation (i.e. control objectives controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals or when significant changes to the security implementation occur (ISO/IEC 27002, 2005).

The risks to the government's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. All identified security requirements should be addressed before giving customers access to the government's information or assets. Agreements with third parties involving accessing, processing, communicating or managing the organisation's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements (ISO/IEC 27002, 2005).

The third control is ***human resources security***. Government should manage tender system access rights. Access rights include new employees appointed to the tender process, removal of access rights to employees who move to other sections within the government department and employees who leave the government. Management of access to the system will reduce the risk of theft, fraud or misuse of information where there is a conflict of interest.

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, proportional to the tender information to be accessed, and the perceived risks (ISO/IEC 27002, 2005). These checks can be carrid out with the assistance of the SIU, case management system or the tender register for defaulters.

The necessary government registers should be checked to see if the employee to be recruited has been involved in any fraudulent activities. As part of their contractual obligation, employees should agree and sign the terms and conditions of their employment contract. This contract should state their and the government's responsibilities for information security.

There should be a formal disciplinary process for employees who have committed a security breach. This is stipulated in documents such as the PPPFA, 2000 (Republic of South Africa, 2000a), PFMA (Republic of South Africa, 1999) and The Prevention and Combating of Corrupt Activities Act, 2004 (Republic of South Africa, 2004)

Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized access or misuse of government information. No single person should access, modify or use assets without authorization or detection.

Tender information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Audit logs should be produced and kept for an agreed period to assist in future investigations and access control monitoring. In addition, logging facilities should be protected against tampering (ISO/IEC 27002, 2005).

The fourth control is ***access control***. An access control policy should be established, documented and reviewed, based on government and security requirements for access. There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. The allocation and use of privileges should be restricted and controlled (ISO/IEC 27002, 2005).

The allocation of passwords should be controlled through a formal management process and regular access rights reviews. ISO/IEC 27002 (2005) notes that users to systems which contain tender information should be made aware of their effective access controls. Systems must be left secure when left unattended. Access to network services must be controlled both within the organisation and between organisations. Policy should be defined and remote users should be suitably authenticated.

Access control facilities for operating system access control must be in place. These include user logon credentials, and inactive sessions should shut down after a defined period of inactivity. Access to information and application system functions by users and support personnel should be restricted. Outputs from application systems, handling sensitive information, should contain only the information relevant to the use of the output and are sent only to authorised terminals and locations (ISO/IEC 27002, 2005).

The fifth and last control considered here is ***compliance***. All relevant statutory, regulatory, and contractual requirements and the government's approach to meet these requirements should be explicitly defined and documented. This practice should be kept up to date for the systems storing the tender information (Placeholder4). Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements.

Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

Officials in management positions should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Information systems should be regularly checked for compliance with security implementation standards.

ISO/IEC 27002 (2005) controls are very much aligned to the security models such as the Bell-La Padula model, Clark and Wilson model and the Biba integrity model. The ISO/IEC 27002 (2005) describes controls to prevent the unauthorised access to information. Therefore, the ISO/IEC 27002 (2005) controls should be used together with the Chinese Wall Model to strengthen the controls limitig the access of information by individuals who already have access to the tender information. The next section reviews corruption and controls implemented in the government departments in countries around the world.

3.7 Corruption and controls in other countries

This section looks at the body of knowledge which researchers and practitioners have published on controls for the tender process in other countries. Countries range from developing to developed countries, but the focus is on developing countries because South Africa is a developing country and therefore it is necessary to compare controls across such countries. To show the contrast, developed countries including America, Portugal, Italy and Britain will be investigated. The developing countries explored include Russia, China and South Africa which has already been inspected.

3.7.1 Developing countries

The focus here is on certain developing countries, including BRICS. The economies of BRICS countries are developing at a fast and growing pace (BRICS, 2013).

- **Corruption laws - Russia**

The most prominent example of anti-corruption enforcement on a global level is The Organisation for Economic Co-operation and Development (OECD) anti-bribery convention. This convention focuses on fraud in international business transactions. It aims to reduce corruption in developing countries by encouraging sanctions against bribery in international

business transactions carried out by companies based in the convention's member countries. However, the OECD anti-bribery convention does not include an effective system to punish businessmen for corrupt actions of their local joint venture partners.

However, Karhunen and Ledyaeva (2012) suggest that the anti-bribery OECD convention as suchmay not have strong enough tools to punish the fraudulent activities of local joint venture partners. Additional legislation at national level is needed to address this problem. This is more of a corrective control.

- **Auditing control- China**

Corruption is a difficult problem that hampers economic development, political democracy and social harmony in China (Gong, 2010). Many studies on the determinants of and factors affecting corruption find that corruption is always related to discretional power, incomplete or weak legal institutions and inadequate supervision (Gong, 2010). Among others, the public finance sector is particularly open to corruption because it has been granted many financial powers in terms of government procurement in China (Liu & Lin, 2012).

Research conducted by Lo and Wong (2011); Liu and Lin (2012) and Bhattacharya and Marshall (2012) showcase that governance practices in many countries indicate that government auditing can play a unique role in curbing corruption.

Liu and Lin (2012) note that auditors are experts in detecting fraudulent financial reporting. They are effective in investigating the underlying corruption. Moreover, the deterrent effect of government auditing can be intensified by making auditing results known to the public. This ensures that the public is aware of the corrupt individual and ensures that individuals are held accountable for their actions.

Government tender fraud is like a “virus” that harms economic security and social harmony (Falagario, Sciancalepore, Costantino & Pietroforte, 2012). The government auditing system is supposed to be the “immune system” that detects and clears out the virus. According to Liu and Lin (2012), studies on how to curtail corruption seldom pay specific attention to the role of auditing. Studies by Liu and Lin (2012) examine the role of government auditing in the system of internal controls.

Unlike developed countries in Europe and North America, government auditing in China is part of the local governance institution and is characterized by strong administrative properties. Nevertheless, there is little evidence that China’s audit system plays a different role from its counterparts in western countries (Liu & Lin, 2012).

According to statistics, the US federal government owns the control rights on about two-thirds of the nation’s government funds, whereas in China, public expenditure at local level

accounts for more than two-thirds of all public spending. We demonstrate empirically that China's government auditing has worked actively and effectively in discovering irregularities and preventing corruption. Therefore, it can help to improve government accountability and transparency. Research by Liu and Lin (2012) stress that not only can government auditing prevent or reduce corruption, but it also provides empirical evidence that the rectification effort following an audit is critical to guaranteeing the power of auditing. This is a reactive measure.

Government auditing can only act as a strong deterrent to corrupt activities if adequate effort is made to rectify malpractice (Karhunen & Ledyaeva, 2012). It is important that all audit decisions and suggestions are carried out completely. If not, government auditing will be of little worth.

The root of tender fraud lies in the incompleteness and imperfection of law and internal control policies. Hence, market development that contains institutional reform and legalisation, should lead to less government intervention in the economy which is fundamental to eradicating corruption (Liu & Lin, 2012). Government intervention in South Africa would include CorruptionWatch, MAWG and so forth as mentioned in the previous sections. The next section investigates various tender regulations in developed countries.

3.7.2 Developed countries

- **Tender evaluation models - Portugal**

Research conducted by Mateus, Ferreira and Carreira (2010) show that the reasons for tender fraud in Portugal and biased awards of tenders is due to inconsistent and unreasonable evaluation methods. The criteria for the award of a tender in Portugal are similar to those in the South African government.

Mateus *et al*. (2010) note that in the Portuguese government, the guarantee of equal treatment is ensured by enabling tenders to be compared and assessed objectively. Furthermore, there is an obligation to ensure the necessary transparency to ensure that all tenderers are reasonably informed of the tender criteria.

These tender criteria will be applied to identify the most economically advantageous tender. It is therefore the responsibility of the government's authority to indicate the criteria for the award of the contract and the relative weighting given to each of those criteria. This information must be made available to the public in sufficient time for tenderers to prepare their tenders (Mateus *et al*., 2010).

Mateus *et al*. (2010) conducted research to understand the weight which a government official specifies in a contract notice or in contract documents and the relative weighting which is given to each of the criteria. The government official (s) had to choose between a tender priced at R500 000 with a completion time of 12 months and another one priced at R510 000 with a completion time of 8 months. The government official will choose the tender with a smaller price, because price is the criterion with the greater ‘‘weight’ ’in this procedure.

Mateus *et al*. (2010) state that this weighting procedure follows a rationale which at first glance seems logical, but when further investigated is not viable. Probably for that reason, this weighting procedure is likely to be the most common one used. Unfortunately, it is also the most common mistake in public tender procedures.

Definition of weights described in this example is arbitrary and inconsistent with the real preferences of the government. The authors point out that the weight criteria and evaluation is open to flexibility. This allows officials to intentionally or unintentionally manipulate the scoring for the supplier tenders.

Allowing for the officials’ choice for this exercise clearly shows that the provision, imposed by Directive 2004/18/EC, to publish the weights of all criteria in the contract documents, does not in fact prevent, by itself, government officials from having unrestricted freedom of choice, nor does it provide potential tenderers with objective or relevant information on how they may best tailor their tenders to the tender principles. If, on the other hand, the government does publish the exact way in which it will evaluate each tender according to each criterion, as well as the evaluation criteria and associated weights required by Directive 2004/18/EC, this information would be considerably more meaningful for tenderers when preparing their tenders, and also to evaluation committees when evaluating submitted tenders. But having clear evaluation criteria does not prevent conflict of interest in a given circumstance; this calls for government not to depend solely on officials being objective and ethical. This calls for the managing of confidential information to be more than segregation of duties and access control security.

- **DEA- cross efficiency approach - Italy**

Falagario *et al*. (2012) propose a decision- making tool aimed at helping the awarding committee of the Italian government to evaluate the tenders. This tool assists with the reduction of conflict of interest may arise.

The tool aims to maintain a transparent procedure in accordance with governmental procurement regulations and requirements as well as guaranteeing fair and equal evaluation of all bids. The cross-efficiency evaluation is used for selecting the best supplier among the eligible candidates. The proposed technique allows the evaluation of quantitative data related

to vendor selection and keeps the transparency features requested by public procurement. In addition, all bids are equally assessed according to the same objectively defined weights without any subjective setting from public officers. This reduces the conflict of interest which may exist among government officials in Italy.

Government tender decisions are often not based on a strict and unambiguous ranking of the available bids. Price variation, difficult to compare among different tenders, often results in the selection of the lowest supplier (Falagario *et al*., 2012). Consequently, the awarding method should have the largest possible degree of objectivity. The proposed approach is completely opposite to the approach of Mateus *et al*., (2010).

The proposed approach consists of a novel use of a well-known methodology, i.e., the cross efficiency evaluation based on the Data Envelopment Analysis (DEA), for evaluating bids awarded through the most economically advantageous tender criterion. This is abbreviated to Most Economically Advantageous Tender (MEAT) and refers to the bid price and completion time criteria of the goods/services required by government. This multi-criteria evaluation procedure allows the assessment of bidders without the setting of weights or scoring functions by public officers. Falagario *et al*.'s (2012) research clarifies a number of methods for assessing a bid based on predefined weights and scoring. Falagario *et al*. (2012) add that these methods have a limitation since the assessment is based on some subjective selection criteria, such as the interval between weights or membership functions. These criteria are selected by government officers.

The scores, as defined by the bid evaluation committee, can easily favour a corrupt bidder (Lorentziadis, 2010). Consequently, this type of arrangement can corrupt the transparency of the process. The distinction between the cost and benefit of each bid does not consider that any given project requires other resources such as time and maintenance services. In addition to money to overcome the above illustrated limits, Falagario *et al*. (2012) propose a tender evaluation method based on data envelopment analysis (DEA) and the related concept of cross-efficiency. In this manner, managing conflict of interest does not rely on access control of the information system. This reduces reliance on a government official being ethical and unbiased in the awarding of the tender.

In this way, there is no need to use subjective scoring systems. No scoring functions are required and objective features of the different bids can be used for assessment. In addition, qualitative evaluation of bids is avoided and weights or utility functions are not required (Falagario *et al*., 2012). Moreover, different indicators for the bids can be compared, even if their scales are not homogeneous. Monetary and non-monetary inputs and outputs can be assessed at the same time. Finally, the described procedure meets the transparency requirements of the European Union (EU) Directive with one limitation, that the weights or

priority ranking are not predefined as required by the EU Directive. This technique allows a differentiation between input and output performance measures. Input performance is given by the amount of resources used by the supplier to carry out the supply activity (e.g., the purchasing price). Output parameters express the quality and time of the service provided to the government (Falagario *et al*., 2012).

The DEA method differentiates between inefficient and efficient suppliers only and it does not allow ranking of the efficient ones. In fact, this instrument is often used only for the pre-evaluation phase of supplier selection. Consequently, in order to increase the discriminatory power of DEA, cross-efficiency evaluation was proposed (Mateus *et al*., 2010).

This formula for evaluation has some features that make it particularly suitable for choosing the best offer in a government tender. The choice of weights is not directly made by bidders, because in this case there could be an incentive for conflict of interest. In fact, each set of weights used for a bidder is then used for evaluating the remaining ones. Therefore, the hazard of discretionary evaluation by public officers is reduced significantly.

- **Orange Book and Green Book - Britain**

Although there is no specific 'standard' for risk management in the United Kingdom government (Aritua, Smith & Bower, 2011), principles of risk management are set out in a framework called the Orange Book (Aritua *et al*., 2011). The Orange Book provides a basic introduction to the concepts of risk management as a resource for developing and implementing risk management processes in government organisations. The Orange book can be used to manage the risk of the breach of confidential information in the tender process. These basic principles have been supplemented with more detailed guides such as the Management of Risk (HM Treasury, 2009) and the Green Book — Appraisal and Evaluation in Central Government (HM Treasury, 2008).

The management of risk guide was produced by the Office of Government Commerce (OGC). It was designed to encourage a risk- based approach to investment decisions, including procurement. The principles from these risk management guides have positively influenced tender standards in the process.

For example, in Great Britain, the UK Bribery Act of 2010 makes it clear that British managers will be responsible for their foreign partners if they influence the decision of the awarding of a tender, which for example may be due to a conflict of interest. The consequences of fraud may be a fine or jail. In contrast, Great Britain's ratification of the OECD anti-bribery pact a decade before was less explicit in this regard (Karhunen & Ledyaeva, 2012).

The table below lists the countries mentioned in this section. Key points identified for reducing tender fraud are included.

Table 3.3: Regulation controls in developed versus dveloping countries

Developing country	Tender fraud controls
Russia	OECD anti-bribery convention for reducing fraudulent activities in business transactions with other countries.
China	Audit controls are essential for fraudulent reporting.
Developed country	
Portugal	Tender evaluation models to streamline the weighting criteria.
Italy	DEA-cross efficiency approach for awarding bids.
Britain	The Orange Book and Green Book provide advice on how to manage information security risk.

While controls can assist with information confidentiality, none of the regulation controls in the above countries point to actual access control to the information system in a government department.

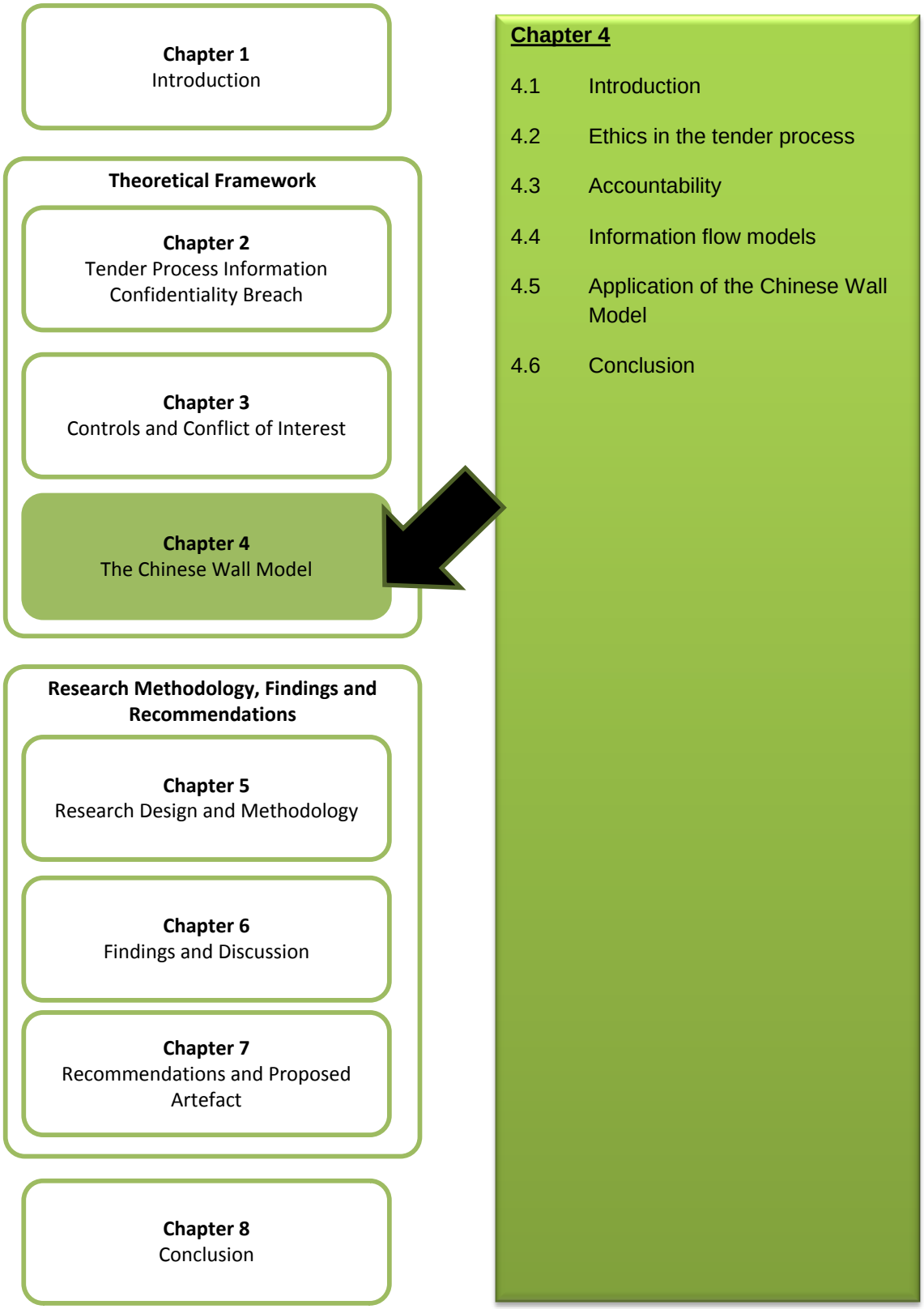
3.8 Conclusion

A system of internal controls has become core to the government's risk management practices. It assists with decision-making in the tender process. Controls should guide and steer the government towards its goals and objectives. It can therefore be concluded that a system of internal controls assists government officials to fulfil their responsibility in protecting government tender information from internal or external threats including direct or indirect threats.

If the definition of operational risk is considered, a thorough system of internal controls can help meet the specified requirements. Additionally, this chapter examines the different classifications of internal control. It analyses the South African government legislation which is applicable to reducing conflict of interest. Thereafter, the South African government intervention in place to manage tender fraud was inspected. The CCSM is used to show how to evaluate the effectiveness of internal controls in the tender process. Following that is an overview of the ISO/IEC 27002 (2005). Finally, the last section reviews the different internal controls applied across the world, with particular focus on the government organisations of the researched countries. These include, OECD anti-bribery convention, UK Bribery Act 2012, government auditing, tender evaluation models, Directive 2004/18/EC, DEA – cross efficiency approach, European Union (EU) Directive, Orange Book and the Green Book.

More needs to be done to build efficiencies to improve the public sector to eliminate opportunities of breach of information confidentiality. The next chapter looks at information security models and compares these to the Chinese Wall Model.

CHAPTER 4 : The CHINESE WALL MODEL



Chinese Wall Model – "a set of rules such that no person (subject) can ever access data (objects) on the wrong side of that wall".

(Brewer & Nash, 1989)

4.1 Introduction

The previous chapter considered how laws and regulations do not directly govern information effectively. It should also be noted that much of legislation and regulation protects information privacy as opposed to information confidentiality (Osborn, 2012). At a presentation held at the ISSA 2012 conference, Osborn (2012) stated that many of the mechanisms used to implement access control are the same ones used to protect information privacy in an organisation. She further adds that in certain cases the mechanisms used to secure information privacy are not always adequate for protecting access control to secure information, and thus information confidentiality. Policies and procedures must often be devised to protect information confidentiality (ISO/IEC 27002, 2005).

It is important to note that information cannot be made completely secure (Marsh, 2012). There is always a risk of information security breach. For that reason, risk of a breach in information confidentiality and tender fraud can only be reduced. Also, government cannot rely on officials being ethical and objective at all times. If this were the case, then the fraud of tenders associated with conflict of interest would not be a problem in the government of South Africa.

Therefore, this calls for government to implement additional measures to manage tender information confidentiality and conflict of interest. Having said that, this measure should be in addition to encouraging officials to be ethical and unbiased in the tender process. The Chinese Wall Model is proposed as an additional measure to manage access control and conflict of interest. The model serves as a preventative control as opposed to detective or corrective control in the system of internal controls.

This chapter addresses ethical behaviour and accountability of a government official in the tender process. These principles were chosen as they have been identified as key tender principles (Republic of South Africa, 2003b) and are also key information security concepts (ISO/IEC 27002, 2005). Thereafter, information flow models and the Chinese Wall Model are discussed as a means of reducing instances where conflict of interest can occur. Finally, an adapted Chinese Wall Model, which includes elements of the tender process, is presented as

a conceptual view of how the Chinese Wall Model can reduce fraud in the government tender process.

4.2 Ethics in the tender process

Promoting and maintaining high standards of professional ethics is one of the principles of the Batho Pele (Department of Public Services and Administration, 2011). Ethical behaviour is important in government tenders as the expenditure of public money is involved. Ethics are the moral principles or values that guide officials in all aspects of their work. *Ethical behaviour encompasses the concepts of honesty, integrity, probity, diligence, fairness, trust, respect and consistency* (Hellriegel et al., 2007). Ethical behaviour includes avoiding conflicts of interest, and avoiding improper use of an individual's position.

Government officials should always behave ethically and fairly. Ethical behaviour can also reduce the cost of managing risks associated with fraud and conflict of interest. Ethical behaviour will enhance confidence in public administration and in the expenditure of government money (Australian Government, 2011).

Value for money is one of the key principles of the Batho Pele and underpins the South African government. The application of the highest ethical standards will help ensure the best achievable tender outcome. The official must be aware of ethical behaviour and behave ethically when having access to confidential information in the tender process.

An important and effective way to maintain ethics awareness in Government is to provide training for employees. Awareness is important for employees to understand unethical behaviour. Ethics training and seminars can be provided, along with training in more specific areas, such as tender procedures, record keeping, records management, accountability and administrative law (Australian Government, 2011). Government officials should therefore seek to develop and maintain levels of knowledge and skill commensurate with their responsibilities.

Hellriegel *et al*. (2007) provide guidance for organisations to minimise unethical behaviour in an organisation. This guide can be applied also to the tender process as well and is summarised in Table 4.1.

.

Table 4.1 Government's practice for minimising unethical behaviour (Hellriegel et al., 2007)

Practice	Practice
Signal the importance of ethical conduct through the Government vision and values statement.	Document the Government's ethical rules through a written Code of Ethics.
Have an ethics officer who is responsible for monitoring the government's adherence to its stated standards.	Appoint an ethics committee to oversee the organisation's ethics initiatives and supervise the ethics officer.
Use an integrity test when screening job applicants.	Emphasise the importance of ethical conduct in training and development programmes to ensure that employees understand unethical behaviour i.e. Ethics Awareness.
Provide ways for government employees to report the questionable actions of peers and superiors, such as through an ethics hotline.	Conduct ethical audits and take steps to address concerns that such audits may uncover.
Develop enforcement procedures that contain strict disciplinary and dismissal procedures for unethical behaviour.	Constantly communicate the government's ethical standards and principles by using all channels of communication if possible. Top managers are especially important in communicating ethical standards.
Treat allegations of wrongdoing seriously.	It is important for senior officials in government to communicate and demonstrate ethical standards.

Government must have measures in place to manage the security and confidentiality of its tender documents. This includes physical security of submissions and related documents, access to secure documents, and confidentiality of commercial information (Australian Government, 2011). Physical security of documents is an important aspect to ensure no information is accessible to unauthorised persons. A lack of confidence in information security could deter bidders or reduce the detail of information bidders include in their bids, which would have poor results for government.

Ethical behaviour demands that necessary officials work to a moral code when securing confidential information. Government should also consider electronic security issues, and have documented processes and strategies for electronic storage and communication. Government must ensure they have control over electronic delivery of submissions, and protection of data stored on networks. This includes segregation of hard-drives, storing confidential information and the allocation of secure passwords to those authorised persons (Australian Government, 2011). Other security measures may include transmitting documents as Portable Document Format (PDF) files to prevent alterations and by double-

checking any emails and attachments before sending to potential suppliers (Australian Government, 2011).

A growing body of research demonstrates that ethical behaviour supports openness and accountability in the tender process and gives suppliers confidence to participate in the government marketplace (Republic of South Africa, 2003b; Pereira, 2009; Department of Human Settlements, 2009; Department of Public Services and Administration, 2011; The World Bank, 2011). The next section looks at government accountability.

4.3 Accountability

Effective records management enables government authorities to enforce a wider government agenda to increase openness, transparency, trust and especially accountability in the government. Effective access management and exploitation of official information are the means by which governments can demonstrate accountability and transparency in the use of public resources, expose corruption and fraud, protect citizens' rights, as well as improve overall service delivery (Mutula & Wamukoya, 2009).

Sound management of information in government is needed for efficiency and productivity in the sharing of information by different units in government. Furthermore it increases pressure on government to demonstrate accountability in the use of resources (Khuarana & Mandke, 2009). Knappa, Morris, Marshallc and Byrdc (2009) note that the information security policy should be regularly audited to enforce accountability of government to follow the policy. Principles of accountability can be established if there is a track record or audit log of decisions made on tenders (Australian Government, 2011).

The Government of South Australia points out that there are several benefits from adequate records management. These include the ability to reduce the considerable risks associated with inadequate records management practice such as accountability, transparency, sound corporate governance and public sector efficiency (Australian Government, 2011).

Records, if well managed, can serve both as instruments of accountability and authoritative sources of information which can be used to support decision-making of tenders and the delivery of government services.

Well managed records can act as an effective deterrent to fraud by leading investigators to the root cause of fraud. Good governance is an essential component of a thriving democratic government and is premised on a system of openness, trust and government accountability.

The World Bank (2011) notes that despite President Zuma's effort to strengthen accountability of government officials and policymakers, fraud is still an issue in government. This is due to incomplete implementation of the Bath Pele principles. The World Bank (2011) stresses the following accountability issues which amongst others, emerge:

- Lack of practical and comprehensive operation manuals for tender implementation;
- Inadequate monitoring, evaluation, feedback, and learning processes. This shows that monitoring and evaluation are ancillary rather than integral to service delivery;
- Financial management and information systems are not integrated with the data on inputs and outputs, resulting in dispersed, inaccessible, poor and untimely basic data on services;
- Underdeveloped feedback mechanisms with no systematic approach for correcting errors quickly;
- Lack of follow-up and sanctioning— both exacerbated by poor data— when manager performance, including the financial management is unsatisfactory;
- Overlapping mandates and responsibilities among the provinces, districts, government departments and service providers.

In addition, effective management of access to information entails compliance with statutory requirements, confidentiality of records and information resources contained within multiple databases and the ability to increased individual accountability (The World Bank, 2011). The Chinese Wall Model can assist in this regard with individual accountability. A particular official will have access to only one dataset in a conflict of interest class as opposed to a number of officials having access to the same dataset. The model will be clarified in feature later in this chapter. Thus, the official can be recognised and held accountable for decisions made on the information contained in the dataset. Furthermore, the application of the model defers the complete reliance on an official acting ethically at all times when decisions are made on tenders. The model is explained in detail in the next section.

4.4 Information flow models

There are a number of information flow models to manage access control and the flow of confidential information in an information system. This section will discuss information flow models with a summarised view of the Clark and Wilson Model, the Biba Integrity Model, the Bell-LaPadula Model and a detailed view of the Chinese Wall Model. The typical use of the Chinese Wall Model in an investment banking perspective will be used to explain concepts, but the model can be applied to the tender process. In the following section, it will be discussed in the context of tenders.

An information flow model explains how subjects (*users*) should interact with objects (*associated with data*) in a system (Coull, Green & Hohenberger, 2011). Information should flow between subjects and objects so that there is no conflict with any existent security policy requirements (Coull *et al*., 2011). For example, information cannot flow vertically between a high security, top-secret level, to a lower security secret level. This is to avoid instances of information misuse occurring, which can lead to fraud associated with the information.

The objective of the Clark and Wilson Model is to primarily prevent information fraud in a commercial environment (Clark & Wilson, 1987). This model requires subjects having access to systems that manipulate objects (*associated with data*) rather than direct access to actual data (Clark & Wilson, 1987).

On the other hand, the Biba Integrity Model prevents possible data corruption by limiting information flow among objects (Biba, 1977). This model groups data into levels of integrity rather than confidentiality (Slay & Koronios, 2006). A subject cannot read data at a lower integrity level or read and modify data at a higher integrity level (Biba, 1977).

The Bell-LaPadula Model focuses on information confidentiality and controlled access to classified information (Bell & La Padula, 1975). This model separates subjects and data according to secret or top secret levels of confidentiality. Subjects need to have authorization to access information corresponding to each level. This prevents information flow from higher security levels to lower security levels and vice versa (Bell & La Padula, 1975).

The Clark and Wilson Model, Biba Integrity Model and Bell–LaPadula Model are based on a set of access control rules for datasets, which already exist in the database. However, there are static limitations with the handling of datasets by the subject. The Chinese Wall Model addresses the limitation of the static nature of the three information models and allows for a dynamic handling of datasets by the subject.

A. An overview of the Chinese Wall Model

The Chinese Wall Model is an access control model used to limit user access to confidential information (Brewer & Nash, 1989). A Chinese Wall is an internal measure adopted by a firm to ensure that information gained while acting for one client does not disclosure to people in another part of the same firm to whom that information may be highly relevant (Slay & Koronios, 2006).

The Chinese Wall Model is structured so that all information is stored in a hierarchy consisting of three layers. The lowest level refers to the ***objects*** pertaining to a particular

company. The intermediate level is where the objects concerning the particular company are grouped. This level is referred to as the **company dataset**. The highest level or **conflict of interest classes**, groups all company datasets together where the companies are in competition (Brewer & Nash, 1989). In summary, each object is associated with a company dataset which is linked to a conflict of interest class.

The Chinese Wall Model explains that information cannot flow between the subjects and objects in a way that would create a conflict of interest. To achieve this requirement the model prescribes that a subject can access a maximum of one dataset within a class. Consequently, the minimum number of subjects needed for this model is dependent on the number of datasets within the largest class (Brewer & Nash, 1989). If all subjects are allowed to access the same dataset in a particular class, then none of the subjects can access the other dataset(s) in the same class(s). Thus, the number of subjects required must not be less than the number of datasets in the largest class (Brewer & Nash, 1989).

B. Comparing the models

When the above models are compared and contrasted, the Chinese Wall Model is more relevant for this research project as it addresses the problem of conflict of interest, rather than the modification of information in the database which can be addressed by the three information flow models, previously discussed.

The Clark and Wilson Model accommodates the Chinese Wall Model by requiring that subjects may only access certain processes and those processes can only access certain objects (Clark & Wilson, 1987). The Bell-LaPadula model does not allow subjects the freedom to choose which company dataset they wish to access, i.e. access to the dataset is dependent on the security level the subject has in the information system (Bell & La Padula, 1975). Whereas with the Chinese Wall Model, subjects may choose the dataset they wish to access (Brewer & Nash, 1989). However, once that choice has been made, the user is restricted from accessing another dataset within the same conflict of interest class. The information system would create a separation of the subject from any further interaction with any datasets within that conflict of interest class.

Table 4.2 Information flow models compared

Model	Key Properties				
	Access dependent on security level	*Access to dataset dependent on user's access to process*	*Limit information flow among datasets*	*Freedom to choose access to dataset*	*Access dataset in same conflict of interest class*
Bell-La Padula Model	✔				✔
Biba Integrity Model	✔				✔
Clark and Wilson Model	✔	✔			✔
Chinese Wall Model	✔	✔	✔	✔	

Table 4.2 provides a matrix comparison of the key properties of the three information flow models and the Chinese Wall Model, which have already been discussed. It can be noted that the shaded area (*Chinese Wall Model*) does not allow a subject who has a conflict of interest to access specific information that could create a conflict of interest. The other models' reliance on access controls means that access and changes therein would require changes to the access control roles of the users.

In a dynamic environment where the dataset being used is constantly in flux, the different datasets for each tender process becomes problematic. Investment banking and government tender processes are two such instances that will be explained as two environments where an information system should allow for fluidity in accessing datasets, based on the current context or associations of the subject to the dataset. The Chinese Wall Model is being used by certain banks, but could be used by the government of South Africa.

4.5 Application of the Chinese Wall Model

A. An investment banking context

Typically, the Chinese Wall Model has been applied within the context of investment banks between the corporate-advisory area and the brokering department. Individuals who give corporate advice about takeovers are not allowed to disclose information to individuals advising clients to buy shares (TechTarget Corporation, 2011). Unauthorised disclosure of this information could influence the advice given to clients who make investments, thus allowing staff (subjects) to take advantage of facts not yet known to the general public. Individuals have been prosecuted for not complying with this rule (Hui, 2009). In the United

Kingdom and Australia, the relevant legislation has explicitly established the legal status of the Chinese Wall Model as a general defense mechanism for breach of fiduciary duties and insider trading (Hui, 2009). The United Kingdom and Australia have very stringent requirements with respect to the set-up of the Chinese Wall Model. The requirements are documented in the Securities Industries Act of 1980 and Financial Service Act 1986, for the United Kingdom and Australia respectively (Hui, 2009). In addition, the courts of the United States of America have accepted the Chinese Wall Model as a strategy to fight insider trading and serve as a defense for the breach of fiduciary duties. This is explicitly specified in the Insider Trading and Securities Fraud Act of 1988 (Hui, 2009).

The information systems in investment banks store information about various business sectors active on one or more stock exchanges. Assume that an investment bank is active in technology (***Class A***) and the financial service sector (***Class B***), as represented in Figure 4.1.

The technology sector has three identified companies called Tech Company A (dataset f), Tech Company B (dataset g) and Tech Company C (dataset h). The financial service, Bank A is class B. It has datasets from f to h. Tech Company B has data object: O1; O2; O3; and, O4. Whereas Tech Company C has its own data object: O1; O2; O3; and, O4.

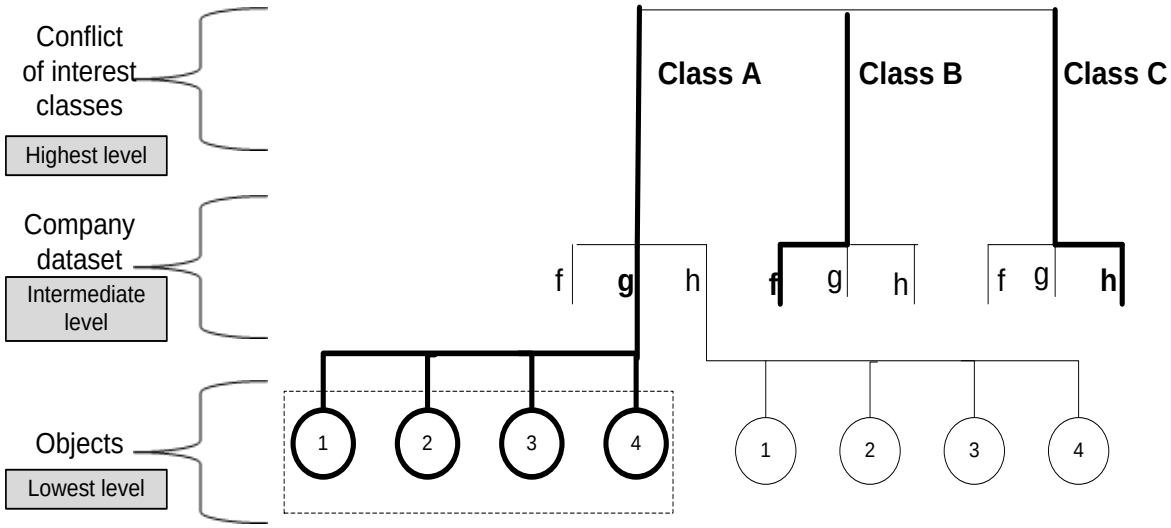


Figure 4.1 The Chinese Wall Model (Brewer & Nash, 1989)

A particular subject in the system has access to class A, dataset g and its data. The same subject can access class B, dataset f and its data. This is permissible according to the Chinese Wall Model. Bank A and Tech Company B belong to different classes. Therefore no conflict of interest exists. The subject may access a dataset from a different class.

However, the subject may not have access to data belonging to dataset h or dataset f of class A as they belong to the same conflict of interest class (Brewer & Nash, 1989).

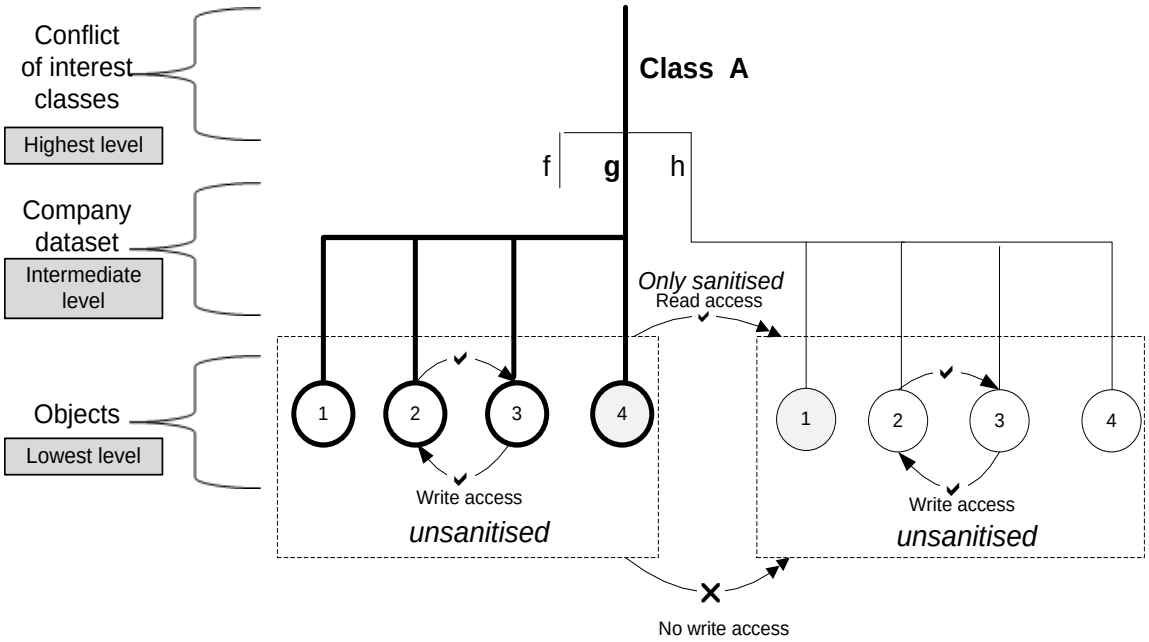


Figure 4.2 Sanitised and unsanitised information (Brewer & Nash, 1989)

The subject may in some instances need to access datasets in the same class to compare information for certain decision-making. The Chinese Wall Model cleverly caters for the restriction to be removed. The identity of companies in a particular class must remain disguised or unidentifiable (Brewer & Nash, 1989). The model refers to this as ***sanitisation***.

Sanitisation can be used as a protection mechanism against the abuse and access of information. Table 4.2, represents a sanitization state by ensuring that write access to Class A, dataset g, and object O4 will only be allowed if the subject has specific write access such that they do not have write access to dataset h (Brewer & Nash, 1989).

Additionally, individuals who do not belong to a corporate advisory or brokering department must not have access to processes which access objects on the information system. This policy must be transparent to ensure its effectiveness.

B. The government tender process context

The Chinese Wall Model can be applied in the government tender process to create an environment which decreases instances of fraud. Class A refers to the professional service needed by the Department. Bid documents are received by service provider f, g and h in figure 4.3. Each bid document contains data for a particular service provider. Service

provider g contains data consisting of, but not limited to, a financial proposal, a technical proposal, statutory documents and application form. This information must be recorded on the information system in the Department.

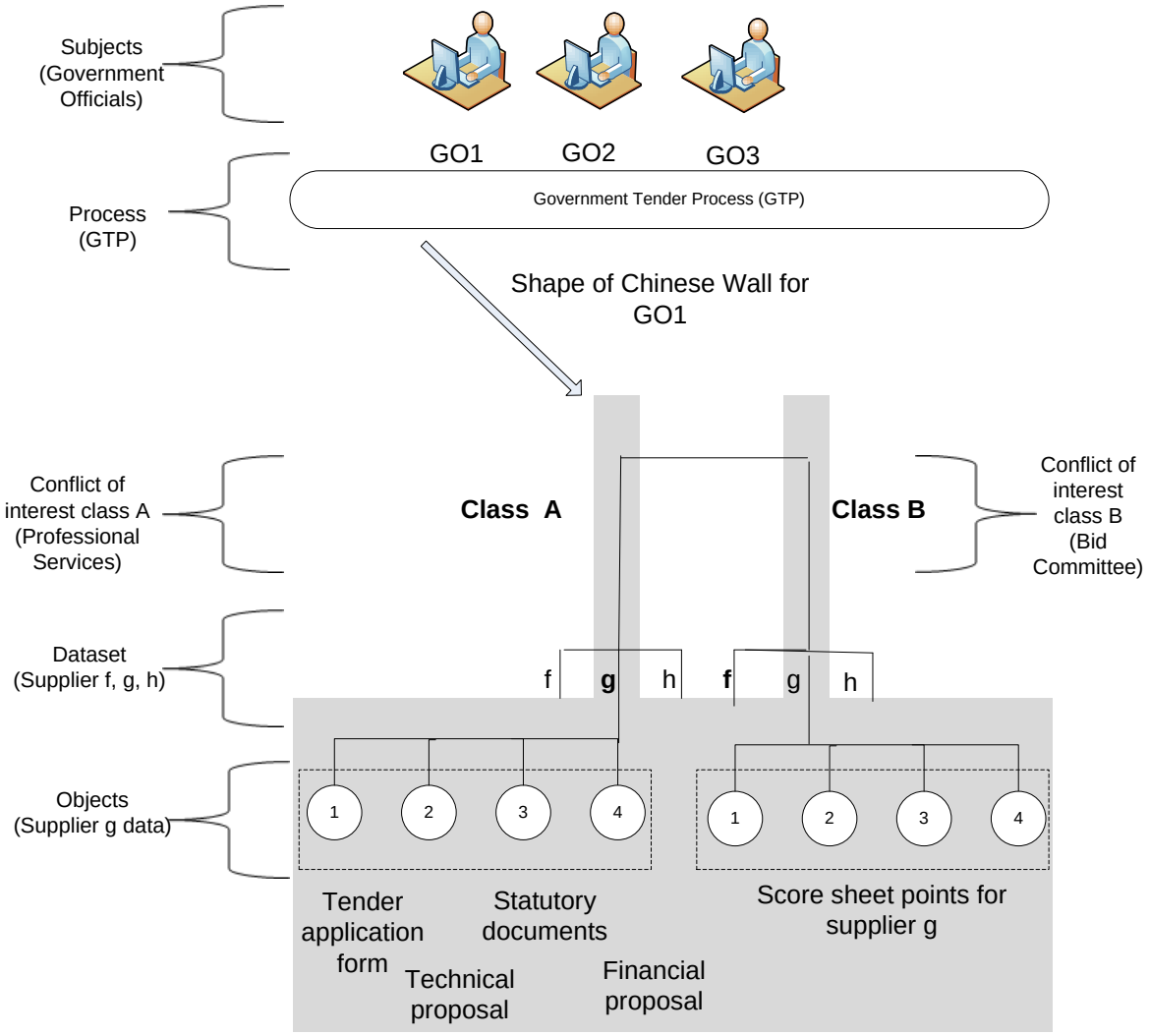


Figure 4.3 Chinese wall applied in tender process (Brewer & Nash, 1989) (adapted)

Service providers' f and h contain data relating to their company. Government officials GO1, GO2 and GO3 are allowed to participate in the tender process. GO1 has access to service provider g dataset and therefore may not have access to datasets for the other two service providers.

The official is therefore held accountable for the decisions made on a particular dataset. By denying GO1 access to the other service providers' datasets, the conflict of interest GO1 may have across the different service providers is reduced.

Service providers are awarded a tender, based on preferred methodology and then on the highest points scored (Republic of South Africa, 2003b). GO1 does not have access to the

other service providers' data, and therefore cannot compare datasets across the other two service providers. Therefore, an "*ethical wall"* is put up. GO1 will potentially resist the urge to manipulate the points scored for the service provider g, as GO1 will be unable to compare datasets across the class.

GO1 may, however, have access to a dataset in another class. In this case, it is dataset g from class B which is the Government's Bid Committee. Since points scored for a service provider play a role in the award of a tender, the points scored for the service providers will need to be made available for comparison. This is where the concept of sanitization by the Chinese Wall Model becomes useful.

The Government official may compare points scored across the different service providers at the bid committee, but the name of the service providers must remain disguised. This also implies that the official must be ethical and not disclose the name of the service provider for whom the points are being revealed. This model therefore could be applied to the tender process.

However, there is a possible limitation of the Chinese Wall Model in this context. The number of government officials needed in the tender process in this example is three as the largest number of datasets is three. It is not always possible for Government to make available the number of officials required by the model.

This could be due to numerous reasons such as lack of budget for the position or a lack of skilled person(s) available to participate in the tender process (Gordhan, 2011). Also the number of datasets varies for every tender process.

The model will be ineffective if this rule is compromised. So there is a possibility that an official may have to access more than one dataset in the same conflict of interest class.

However, with the Chinese Wall Model, an official will have access to only a few datasets as opposed to all datasets which is the current state in the tender process. Thus the conflict of interest is significantly reduced.

For example, it is estimated that R 30 billion per year of governments procurement is lost to corruption (Special Investigating Unit, 2011). If this amount could be reduced to ,for example, R20 billion it would be worth implementing the Chinese Wall Model. Having said that the conclusion is that government is better off with the Chinese Wall Model implemented in the tender process than without the model.

Table 4.3: Tender principle and Chinese Wall Model

Tender Principle	Chinese Wall Model
Information	An official who is unauthorised to view sensitive information in the tender documents received, should not have access to such information. Subjects who have access to a company's proposal must not have access to other company proposals in the same conflict of interest class.
Transparency	If a supply chain official has a business interest in a contract to be awarded, that official must be denied read and write access to objects in the respective conflict of interest class.
Value for money	The Chinese Wall Model has the potential to reduce the award of a tender to an unworthy supplier. The award of a tender to a worthy supplier can be achieved, thus ensuring value for money.
Competitiveness	An accurate evaluation of bid documents, thus a fair decision can be made on the award of the tender.
Efficiency	The model prevents an official write access to data within the same class thus improving the tender process.
Accountability	Officials can be held accountable for decisions made as access to dataset will be restricted to certain individual(s) instead of all members having access to all datasets as is currently the case

Based on the case studies, mentioned in Chapter 2, it is concluded that most of the conflict of interest occurs at the bid committees. The explanation of the Chinese Wall Model as explained in Figure 3 can be applied to these cases where Class A represents the service providers and Class B the bid committees.

Applying the Chinese Wall Model can prevent information from being compromised in the tender steps of two, four, five, six and seven. These steps are respectively, approve tender specifications, bidder submitted completed tender forms, observe bid closure process, evaluate tender documents and award the bid to the highest scoring bidder.

This is achieved by managing the read and write access of datasets across the conflict of interest class. That is, the BEC and BAC members may only necessarily access a dataset which is not in conflict with another dataset. This prevents all the BEC and BAC members from accessing the entire supplier's company datasets.

This improves tender information checks and reduces manipulation of supplier scores as tender proposals across all the companies cannot be compared by any one individual unless sanitisation of company information is in place.

Managing information confidentiality is essential in reducing tender fraud (Mutula & Wamukoya, 2009) and upholding tender principles. These tender principles and recourse for tender anomalies associated with cases can further be explained with respect to the Chinese Wall Model (Table 4.3).

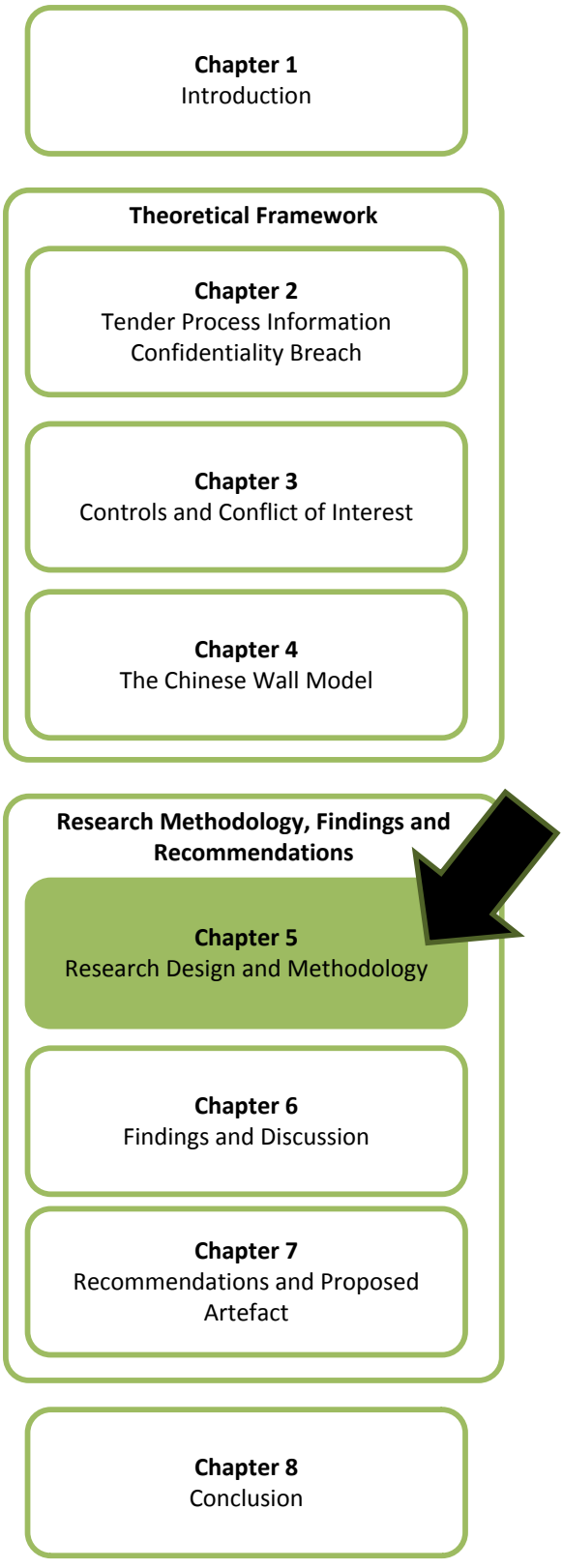
4.6 Conclusion

Confidential information in the government tender process is often not properly secured, exposing it to possible fraud. This chapter highlights the importance of ethical behaviour in the tender process. Focus is placed on government officials being accountable for the decisions they make on tenders. Having said that, it is not wise to solely rely on officials being ethical and accountable for decisions made. There is a need for alternative measures to reduce conflict of interest and manage confidential information of tenders in the system.

Fraud in the sense of a conflict of interest which a government official has with a particular supplier, may result in an award of tender to an unworthy supplier. The problem this chapter addresses is how to reduce instances of conflict of interest which may corrupt the process. The proposed solution is the application of the Chinese Wall Model in the tender process, while adhering to the tender principles.

The application of the Chinese Wall Model is a preventative control as opposed to a detective or corrective measure. While a limitation of the model has been identified, the initial conflict of interest problem has been solved, and the objective of applying the model has been achieved. The Chinese Wall Model for information confidentiality in tenders can be added to the body of knowledge where the various controls across foreign governments have been researched in the previous chapter. The next chapter will explain the research methodology adopted in this research.

CHAPTER 5 : RESEARCH DESIGN AND METHODOLOGY



Chapter 5

> "The selection of a research design is also based on the nature of the research problem, and the audience for the study".
>
> (Creswell, 2009)

5.1 Introduction

The previous three chapters presented the literature review relevant to this study, thereby, setting a solid theoretical foundation. Chapter 2 presented a discussion on the research problem of corruption relating to conflict of interest in government tenders. This problem is mainly due to the lack of information confidentiality in systems storing tender information. Conversely, Chapter 3 focussed on controls to prevent the breach in information confidentiality. Following that, Chapter 4 applied the Chinese Wall Model to manage access control to confidential information and thus reduce the conflict of interest. These chapters helped address the research questions presented in Chapter 1 and provided a theoretical base that supported the conceptual framework of the Chinese Wall Model.

This chapter is principally concerned with the **research methods** (Figure 5.1). The layers of the onion assist with writing the research methodology chapter which will examine the research design and thesis methodology applied in this study. The research method has been influenced largely by the project's objective. The objective was the creation of an artefact to reduce conflict of interest as well as breach of confidential information. As referred to in Coull, Green and Hohenberger (2011) empirical research methods are those methods where empirical information is collected.

Collection can be in data or observation form to obtain answers to research questions. Creswell and Tashakkori (2007) explain that methods are the procedures followed by researchers who seek to obtain and articulate the information gained, resulting in a credible study.

As a result, an analysis of existing quantitative and qualitative research methods is given to determine the best possible method to use in this research project. Essentially, the aim of this chapter is to explain how the study was conducted. This chapter also provides insight into how the results were obtained. Furthermore, the chapter provides a theoretical basis of the chosen method. This refers to the method on which the research and results were founded. In a more detailed sense, a description of the data collection, analysis and validation processes that were followed is given. In addition, Creswell and Tashakkori (2007)

are of the opinion that all research must be conducted within the boundaries of a particular research paradigm. An appropriate paradigm is selected for this study. This paradigm is described and its details are provided below.

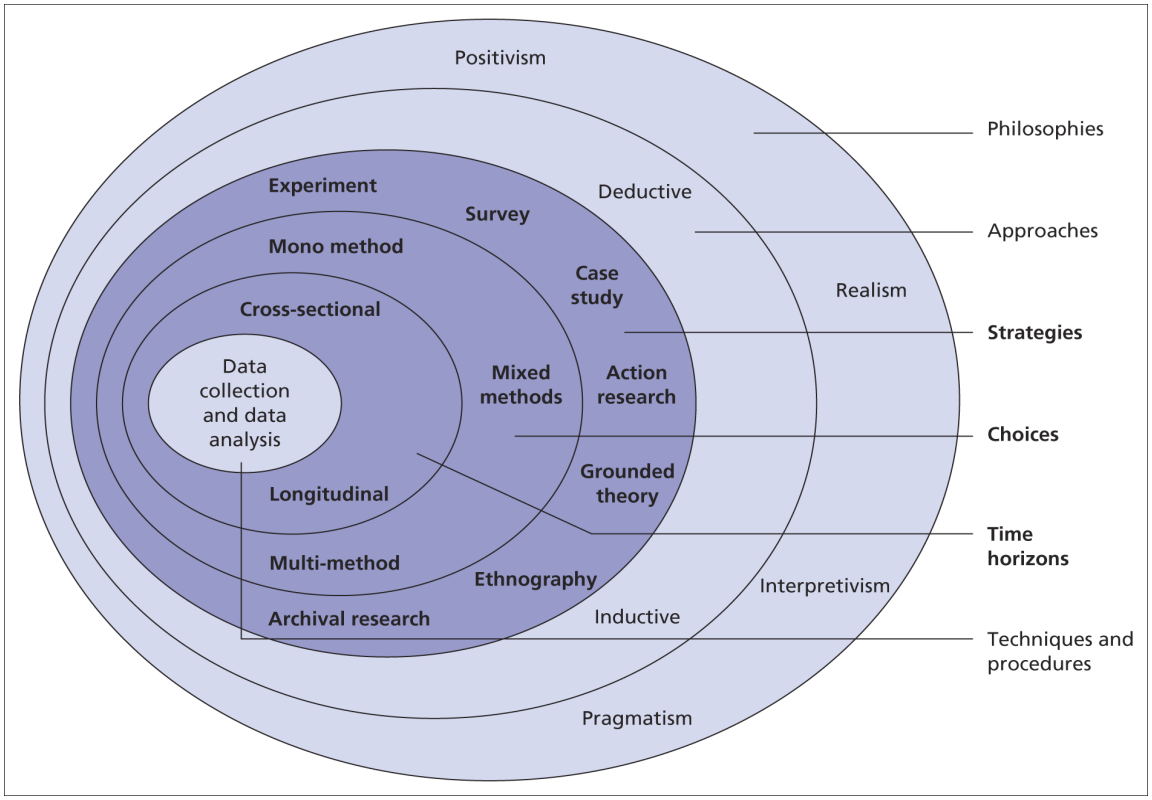


Figure 5.1 The research onion (Saunders, Lewis & Thornhill, 2009)

5.2 Philosophical research paradigms

The research methodology adopted in this study is represented in Figure 5.2. The outer layer of the research onion, the research philosophy is critical as the adopted philosophy will influence the way in which the research is undertaken. The adopted philosophy needs to be clearly stated since it helps to present the perception of the world by the researcher, what the researcher believes constitutes reality (ontology), how that reality is understood (epistemology) and the methods that can be used to obtain further knowledge of that reality (Saunders, Lewis & Thornhill, 2009). The philosophy will make clear what evidence is to be gathered and how it helps in addressing the research questions posed.

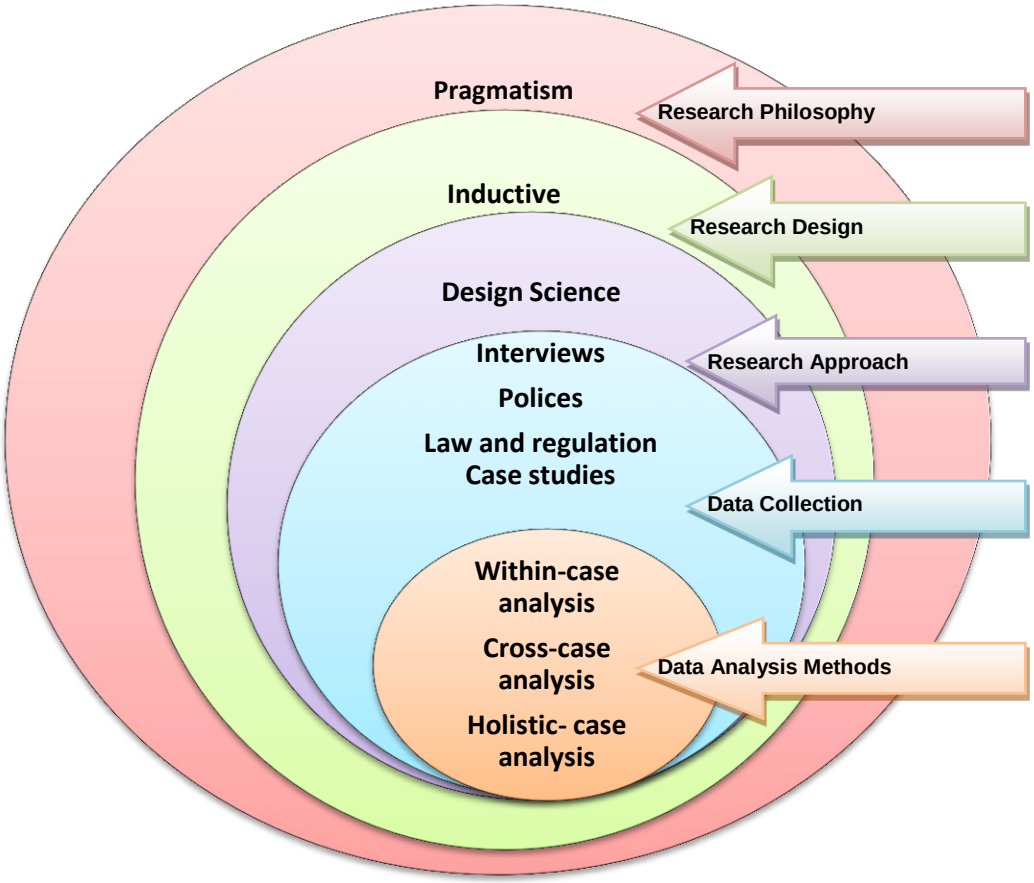


Figure 5.2 Research methodology adopted in this study (Saunders *et al*., 2009) (adapted)

Three classifications of paradigms will be compared here. These include positivism, Interpretivism and pragmatism paradigms. Moreover, these paradigms are philosophically unique, but in practice, they are often not always clear. The paradigms and their differences are described below.

5.2.1 A comparison of research paradigms

Morgan and Smircich (1980), depict the research paradigms in the form of a continuum, which is effective in illustrating the difference between the two opposing extremes of thought, being positivist and phenomenologist. The extreme left depicts the area in which the positivist or objective research paradigm is utilised while on the extreme right, the interpretive research paradigm is applied and followed. Movement along the continuum signifies that the applied assumptions of the one paradigm are reducing, and are slowly being replaced by those of the other paradigm. It must be noted that this continuum does not mention the pragmatic approach.

This research involves firstly, questioning and personal opinions (*interpretivist stance*) in understanding the research problem. Secondly, it involves developing practical critical success factors for managing access to confidential information in the tender system, where

those Critical Success Factors (CSFs) can be applied to other contexts which also implement the Chinese Wall Model. The different classifications of paradigms are compared below and their appropriateness to this study is discussed.

5.2.2 Positivist

Reality is ordered, predictable and is objectively given. Positivism states that reality can be described via measurable properties that are completely independent from the observer (Myers & Klein, 2011). This ensures that there is a distance between the subjective biases of the researcher and the objective reality he or she studies.

In this view, the world is considered as external and objective to the researcher, and people and things are considered to be alike (Saunders *et al*., 2009). Further, the ontological assumption is that the research subjects and the researcher do not have direct contact. The epistemological assumption is that, knowledge can be measured with great accuracy and precision. The researcher should not interfere with the research respondent's opinions, perceptions and ideas (Saunders *et al*., 2009). The use of deductive logic to test causal relationships and theories is adopted in the methodological approach (Teddlie & Tashakkori, 2009).

Overall Aim : It relies heavily on experimental and manipulative methods. It involves studies which test theories to understand the phenomenon and provide objective results.

This study : The positivist approach produces effective results that are easily generalisable, but fails to capture the social nature of humans. Therefore, this positivist philosophical stance is not suited for this study which explores the fraudulent activities of people in government, poor information security culture and the meanings people attach to their situation. Next, the opposing view, interpretivism will be discussed.

5.2.3 Interpretive

Access to reality is through social constructs such as language, culture, consciousness and shared meaning (Myers & Klein, 2011). The paradigm focuses on the full ability of a human's logic and thinking. It is also highly subjective to a specific context. Dependent and independent variables are discovered throughout the process of the study instead of being predefined beforehand. In the interpretivist philosophy reality and knowledge are constructed socially (Myers & Klein, 2011).

In this view, the ontological assumption is that, the researcher's knowledge of the subject is based on the subjective experiences of the research participants, and the epistemology is that the knowledge obtained should be interpreted (Carlsson *et al*., 2011). Research conducted within this philosophical view often takes a qualitative approach and inductive

reasoning is adapted to provide rich data for theory building (Hellriegel *et al*., 2007; Myers & Klein, 2011).

Overall Aim : This philosophical stance involves studies which attempt to understand phenomena through the various meanings that people assign to them.

This study : One cannot assume that mere access control to tender information is the solution to managing information confidentiality. The researcher has to understand the problem, compare various access control models and propose a solution which is practical to the South African government. Also, the CSFs incorporating the Chinese Wall Model to manage access control must be suited to other countries, for example, where the model is implemented. Thus, the interpretivist philosophy is not appropriate to this study. Next pragmatism will be discussed.

5.2.4 Pragmatism

Pragmatism is not new to social sciences. Pragmatism provides a new option for addressing methodological issues in social science. It is seen as a belief system to social science. Pragmatism influences the positivist and interpretivist paradigms (Feilzer, 2010). The movement back and forth between different approaches to theory and data does not have to be limited to combinations of methods within a single research project. These are the kinds of opportunities that a pragmatic approach to research has to offer (Morgan, 2007). Pragmatism acknowledges that any knowledge generated through research is relative and not absolute (Feilzer, 2010). The unpredictable human element forces pragmatic researchers to be flexible and open to the emergence of unexpected data (Carlsson *et al*., 2011).

This philosophy influences the qualitative and quantitative aspects of this research. Feilzer (2010) questions whether quantitative and qualitative methods are really that different or is their dichotomy politically motivated and sociologically constructed.

- **Qualitative Research**

Qualitative research methods were designed to operate within a social science context. This method enables researchers to study human behaviour and the reasons that determine certain human behaviour (Creswell & Tashakkori, 2007). This is referred to as social and cultural phenomena. The focus of this method is on the collection of data which is based on the opinions of others who are influential in the field of study. Commonly included methods are the use of case studies, relevant theories and literature e.g. historical research and action research (Feilzer, 2010). A further contribution is surveys, expert reviews and the use of the Delphi Technique. Observing on-the-job tasks or analysing processes, and structured

or open ended interviews, formal and informal experiments are included here (Collins, Onwuegbuzie & Johnson, 2012). Quantitative Research

Quantitative research methods were created in the natural science domain. Quantitative Research observes and learns from natural occurring phenomena that occurred (Luyt, 2012). The focus of these methods is the systematic collection of highly objective and statistical data which can be numerically measured (Feilzer, 2010). Commonly used methods are questionnaires and surveys. For example, online surveys, paper-based surveys or over-the-phone questionnaires. Included also are more specialised methods such as statistical analysis, graphs, trend and relationship mapping. The next section explains the chosen philosophy, pragmatism, in extensive detail.

5.3 Pragmatism research paradigm

A publication of noteworthy books and articles on pragmatism includes Teddlie and Tashakkori (2009), Morgan (2007), Feilzer (2009), Collins, Onwaegbuzie and Johnson (2012), Creswell (2009) and Luyt (2012). These works have contributed to the choice of paradigm selected in this study. The pragmatist position is particularly appealing and suitable for this study due to the practicality aspect of the study. Table 5.1 represents a comparison of pragmatism with the two other methodological stances namely, qualitative and quantitative. The key issues to these approaches are shown in the table. There is a clear definition between induction and deduction in connecting research and data. Morgan (2007) emphasises that the clear difference is necessary to guide novice research students in the approach they will take. However, he further adds that an experienced researcher is aware that moving between theory and data is never only in one direction. During the actual design, collection and analysis of data it is impossible to operate in an exclusive theory. The next section explains the pragmatic paradigm in detail (Table 5.1). Thereafter, its relevance to this study is demonstrated (Table 5.2).

Table 5.1 A comparison of key issues in social science methodology (Feilzer, 2010)

Issues	Approach		
Method	Qualitative	Quantitative	Qualitative and/or Quantitative
Connection of theory and data	Induction	Deduction	Abduction
Relationship to research process	Subjectivity	Objectivity	Intersubjectivity

According to Feilzer (2010), the pragmatic approach relies on a version of abductive reasoning. It includes induction and deduction. This reasoning converts observations into theories and then assesses those theories through action (Feilzer, 2010). One of the most common uses of abduction in pragmatic reasoning is to advance a process of inquiry that assesses the results of prior inductions. This assessment is done through the ability to envisage the workability of future lines of behaviour. Also, the inductive results from a qualitative approach can serve as inputs to the deductive goals of a quantitative approach, and vice versa (Feilzer, 2010).

Some reseachers see the reasoning for pragmatism as abductive (Morgan, 2007; Feilzer 2009). Other researchers, (Teddlie & Tashakkori, 2009), state that reasoning can be inductive and deductive, or both. This study adopts the latter stance, arguing that in academic work, this study lean towards qualitative analysis by conducting semi-structured in-depth interviews with expert reviewers and the analysis is conducted using inductive reasoning.

Morgan (2007), believes the contrast between subjective and objective is an 'artificial' summary of the relationship between the researcher and the research process. Morgan (2007) states that there are arguments about the impossibility of "complete objectivity" as well as "complete subjectivity". The classic pragmatic emphasis is an intersubjective approach capturing this duality. However, for the purpose of this study, the relationship to this study is subjective.

Inevitably, the researcher has to have an understanding of the people who participate in the research. The processes of communication and shared meaning are key to any pragmatic approach. This is essential for the understanding of people in government.

In a pragmatic approach, there is no problem with asserting both, that there is a single "real world" and that all individuals have their own unique interpretations of that world.

So for example, the application of the Chinese Wall Model in investment banks has been applied in this study in the context of government tenders. These are the reasons for following the pragmatic approach in this study.

A strong point of the pragmatic approach is its emphasis on the connection between epistemology and methods. In other words, it is the nature of the knowledge a researcher produces and the method used to generate that knowledge. The table below shows the pragmatic characteristics in relation to this study.

Table 5.2 Pragmatic characteristics in relation to this study (Creswell & Tashakkori, 2007; Feilzer, 2010; Collins, Onwuegbuzie & Johnson, 2012)

Assumptions	Description	This Study
Research Purpose	Supports the use of different research methods with the use of abductive reasoning.	Understand meanings that government officials and IT experts associate with information confidentiality in the tender process.
Nature of reality (ontology)	The nature of reality is singular or multiple. It may include either or both subjectivity and objectivity. Researchers test hypotheses and provide multiple perspectives.	Application of the Chinese Wall Model in the tender process and the feedback from participants present evidence of different perspectives.
Nature of knowledge (epistemology)	The relationship between the researcher and the research is that the researcher seeks practicality. Researcher collects data from what works to address the research problem.	The researcher collaborates with the participants in an interactive process of listening, talking, reading and writing.
Axiology (values)	The role of values may have multiple stances. The researcher may include biased and unbiased stances.	The researcher's understanding of the research problem (tender fraud) may be biased, but the proposed solution may be unbiased.
Methodology (research process)	The process of research is a combination of deductive and inductive reasoning. The researcher may collect qualitative and quantitative data.	The researcher collects theoretical data on tender fraud. Also expert opinions on the research problem and the proposed solution of the Chinese Wall Model are gathered.

The pragmatic philosophy chosen will guide the research methodology. This is noted in the following section.

5.4 Research Methodology

Research methodology becomes especially important when looking into approaches of research design where the design process becomes the central device for research. In the

opinion of Madnick, Lee and Zhu (2009), the method is at an analytical level and produces credible research in an academic peer reviewed format.

This concept acknowledges that many kinds of investigations can be adequate within design research. Hence several perspectives and approaches as well as theories and methods might co-exist. Luyt (2012) expresses the need for constructive research methods. This will allow the disciplined, rigorous and transparent building of Information Technology (IT) artefacts as outcomes of Design Science research. Madnick *et al*. (2009) proposes that researchers are encouraged to consider employing more than one research method, including one or more quantitative methods with one or more qualitative methods.

While using Design Science as the research method, included here is the review of expert opinions and the implementation of these reviews in a structured process.

A study of Design Science has been called for in the information systems community (Madnick *et al*., 2009). With an artefact-centric view of Design Science, Hevner *et al*. (2004) developed a framework and a set of guidelines for understanding, executing, and evaluating research in this emerging domain. The aim of this study, in more specific terms, is to develop CSFs which incorporate the Chinese Wall Model.

The output is an artefact comprising CSFs for government officials in action in order to decrease the risk of conflict of interest and the breaching of confidential information, the reason for this study. Design science methodology is explained below.

5.5 Design Science research methodology

This section will provide a discussion on the Design Science methodology together with the approach to data collection and analysis. Design Science, as a research methodology, seeks to grow human potential by developing innovative solutions (Hevner *et al*., 2004). It is also a problem-solving process which has a fundamental principle. Understanding of problems and their solutions is obtained through the design and implementation of an Information Technology (IT) artefact. Wang and Wang (2010) support this view by adding that the significance of research in the information systems domain is closely related to its applicability in design which must be implementable. This clearly supports the pragmatic paradigm.

A conceptual research framework proposed by Hevner *et al*. (2004) has been developed to understand, execute and evaluate the research. This framework is illustrated in Figure 5.3.

Figure 5.3 Information systems research framework (summarised) (Hevner et al., 2004, p. 80)

Figure 5.3, at a summarised level, seeks to evaluate the ***environment***, which is the problem space. This space requires certain business needs from ***information systems research***. The ***knowledge base*** is applied to IS research, which becomes new knowledge and adds to the knowledge base. This IS research is then applied to the problem space (Hevner *et al*., 2004).

At a detailed level, Figure 5.4, the leftmost environment block is where the problem resides. It consists of the people, organisation and technology present within the IS discipline. Together these will express certain ***business needs*** therefore forming the 'problems' for which IS research solutions have to be found. Comparing Behavioural Science with Design Science, Behavioural Science aims to develop theories to explain problems (Niehaves, 2007).

Design Science, on the other hand, speculates about the use of an implementable artefact to solve problems (Wang & Wang, 2010). Hevner *et al*. (2004) continue along the lines of comparison, add that the goal of Behavioural Science is the acquisition of truth, while the goal of Design Science is focused on utility. Nonetheless, truth and utility are inseparable (Hevner *et al*., 2004), therefore an artefact may have a certain level of utility based on the possibility of discovered truth.

Furthermore, Behavioural Science develops theories which explain and predict human phenomena surrounding the implementation and use of the information systems. Whereas, Design Science applies knowledge of situations to create artefacts (Niehaves, 2007). In summary, Behavioural Science is *knowledge-producing* and Design Science is *knowledge-using.*

As a result, an ongoing process of ***assessing and refining*** research in Figure 5.4 is instilled, that will continue to occur in research conducted in the future. IS research draws on **knowledge base**, rightmost box, that consists more specifically of IS ***foundations*** and ***methodologies***. The appropriate use of this knowledge base is applied to IS research.

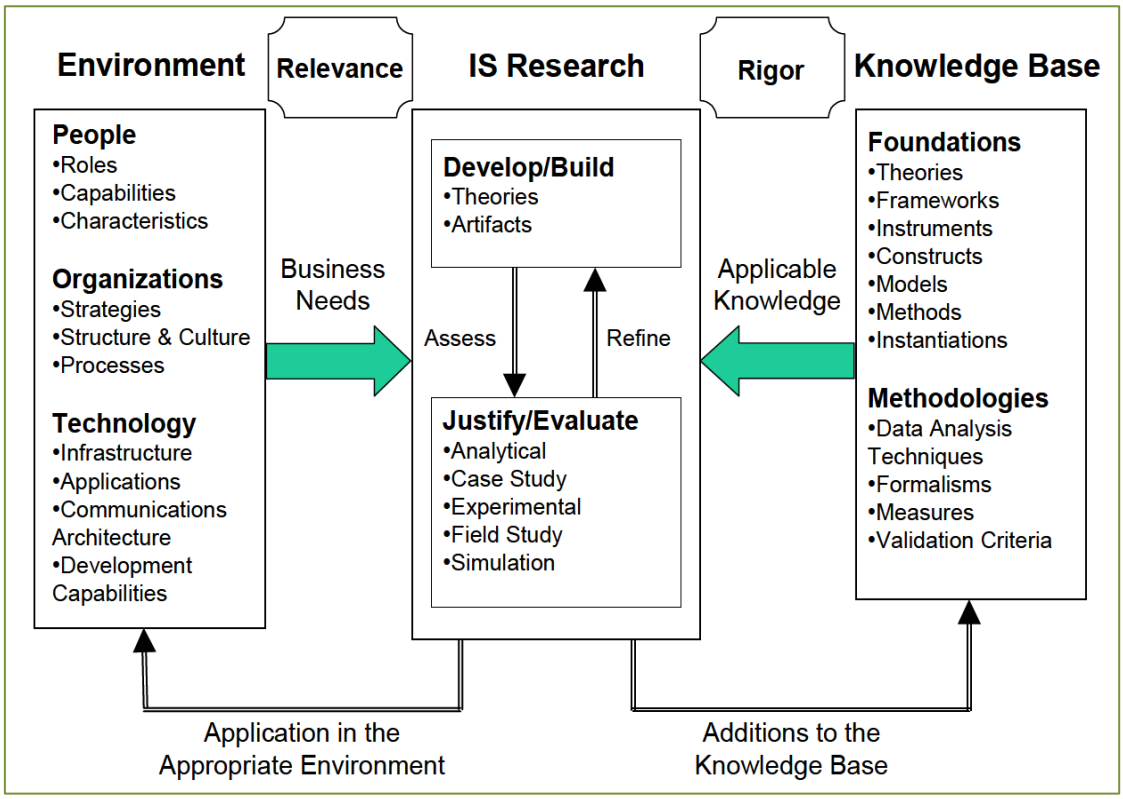


Figure 5.4 The information systems research framework (detailed) (Hevner *et al*., 2004, p. 80)

Hevner *et al*. (2004) explains that IT artefacts can be defined as either:

- *Constructs* - which are the symbols or the vocabulary used to define problems and solutions. These artefacts provide the language in which problems and solutions are articulated to others.
- *Models* - the abstractions and representations of real world situations or problems. The model provides a solution space for the exploration of possible design decisions and solutions.
- *Methods* - comprising complex algorithms and effective development practices. Their purpose is to provide guidance on how to solve problems.
- *Instantiations* – these refer to existing systems that have already been implemented to solve a problem, or prototype systems that are currently being designed.

Whether the artefact is a construct, model, method or instantiation, Design Science is centred on creating and evaluating IT artefacts that have been designed to solve real organisational problems. As behavioural sciences use field studies to understand problems in a particular context (Niehaves, 2007), Design Science will similarly follow a process of building and implementing IT artefacts, so as to understand the problem addressed by the artefact and the viability of the solution (Wang & Wang, 2010).

The design process mentioned, consists of a chain of specialised tasks that firstly, *build* an innovative product (i.e. the IT artefact), then *evaluate* the artefact, after which feedback is

received from this evaluation. This feedback is used to improve the understanding of the problem which leads to improvements in the quality of the solution and the design process itself. This ***assess*** and **refine** cycle continues and iterates until a final and complete artefact is built.

Hevner *et al*. (2004) emphasise that Design Science can either address important unsolved problems or look at alternatively solved problems in a more effective and efficient way. For this reason, Design Science was the best choice to address the problem of conflict of interest in tender fraud and in the breach of confidential information. To do this, the next section will discuss the research instrument which was used to conduct the study.

5.6 Design Science Guidelines

To conduct effective and thorough IS research by using Design Science methodology, Hevner *et al*. (2004) provide seven guidelines to aid researchers in understanding what exactly is required for such research. Hevner *et al*. (2004) point out that researchers should make use of their own individual creativity and sound judgement, to determine when, where, and how the guidelines should be applied. These guidelines also have the ability to overcome the lag between discoveries in academic research and their adoption in industry. Thus, it is advised that each of these guidelines be followed closely to ensure that the research is complete. These guidelines are summarised in Table 5.3.

Table 5.3 Design Science Guidelines (Hevner *et al*., 2004, p. 83)

Guideline	Description
Guideline 1: Design as an Artefact	Design Science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of Design Science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5: Research Rigour	Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
Guideline 6: Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design science research must be presented effectively both to technology-oriented as well as to management-oriented audiences.

These seven guidelines will now be discussed in more detail. Thereafter, the section will conclude with a summary of their application for ease of reference.

5.6.1 Guideline 1 – Design as an Artefact

As discussed earlier in this chapter, the primary objective and end result of Design Science research in the IS domain is a purposeful design artefact. The artefact must specifically and effectively address a known organisational problem: in this study, the breach of confidential information in the tender process in South Africa. In order for an artefact to be implemented in an appropriate domain, it needs to firstly be clearly described. This artefact can be in the form of a construct, model, method, or an instantiation.

After much evaluation, the most suitable artefact chosen for this study is that of a Design Science artefact, which presents various critical success factors to reduce tender fraud and to increase the confidentiality of information in the system. The artefact is designed by analysing data obtained from both primary and secondary data sources.

Primary data sources refer to data which has not already been published and which the researcher has gathered directly from various participants (Teddlie & Tashakkori, 2009). In terms of the primary data analysis, an iterative process of expert reviews was conducted and performed, based on the practices and procedures of the expert review process (Hevner *et al*., 2004). This helped to construct a relevant and plausible model comprising the Chinese Wall Model and CSFs. Thereafter, several cycles of refinement followed, improving the quality of the model. Research obtained from previous literature formed the secondary data analysis which was the main source of data used in this study.

Secondary data sources include any previously published research material, such as books, journals, online articles, theories and frameworks (Carlsson *et al*., 2011). This consists data of a variety of pertinent information flow models and theories that apply to the management of access control to confidential information in a system. The application of the information flow model, the Chinese Wall Model, is the most appropriate proposed solution and therefore is discussed in detail in the literature chapter.

Various government laws and regulations were also discussed. This discussion included analysis of law and regulation in South Africa as well as in foreign countries. Various tender fraud case studies and recent newspaper articles were also included to bring a practical element to the study.

5.6.2 Guideline 2 – Problem Relevance

This guideline concerns itself with the research problem and the way in which the designed artefact relates to the problem. It is reiterated that Design Science research in the IS domain revolves around seeking knowledge and understanding to allow for the development and implementation of technology- orientated solutions to unsolved business problems. These problems can often be found in literature, as emphasised by other researchers who accept that these problems still remain, warranting further study and examination (Hevner *et al*., 2004).

The problem articulated in this study is the breaching of confidential information in government tenders. The fraud is directly related to government officials and results directly from conflict of interest. The conflict of interest is due to selfish gain, which results in the awarding of a tender to an unworthy supplier. This negatively impacts government's service

delivery as the goods and service outsourced by government are not completed as required. This causes major loss of government expenditure and tax payers' money.

5.6.3 Guideline 3 – Design Evaluation

Hevner *et al*. (2004) place great emphasis on the evaluation of the artefact. Ultimately, it forms a fundamental component to the Design Science research process and directly influences the final product that is developed. "The utility, quality, and efficiency of a design artefact must be rigorously demonstrated via well executed evaluation methods" (Hevner *et al*., 2004, p. 83). Artefacts must be evaluated regarding their accuracy, consistency, functionality, reliability, completeness and performance. This ensures credibility of the product.

Furthermore, feedback produced by an evaluation phase is used as an input for the design of the final product. Then, improvements are applied to the quality of the design artefact and the product being developed. A key principle must be noted: The evaluation and construction phases are repeated until the design artefact is complete. An artefact is complete only when it meets all the design requirements and constraints of the problem it was designed to solve. One of the primary data collection methods,that of expert review process is considered here (Hevner *et al*., 2004).

Expert review is a used and accepted method for achieving convergence of opinion concerning real-world knowledge, solicited from experts within certain topic areas. The expert review process is an iterative, structured communication technique that relies on the opinions of experts in a specific field. It is based on the assumption that the judgements and views held by these experts are regarded as more valid or authoritative than those held by individuals. The distinctive structure of this technique is to allow for the input of a number of participants who may be geographically dispersed (Hevner *et al*., 2004).

Rounds of discussions are dependent upon completion of the artefact (Hevner *et al*., 2004). Since this research is pragmatic and aims at a solution which is practical in government, the chosen experts consist of individuals who are proficient in information security as well as industry experts from government. The reviews received from five rounds will assist to refine and provide constructive feedback on the proposed artefact.

Firstly, a broad review was received on the research problem; a summary of previous research conducted on the topic, and the application of the Chinese Wall Model in the context of government tenders. The Chinese Wall Model was initially applied, by other researchers, in a military context and in investment banks to manage conflict of interest.

This model was then applied to government tenders to possibly help curb tender fraud by better managing access to confidential information. This critique was based on the originality, significance, technical quality and relevance of the research project. Experts provided comments, thoughts, opinions, suggestions and judgements on each area. This feedback was used to refine the proposed solution.

Further detailed review was sought from the industry experts from government as well as from IT experts. These expert opinions were obtained using a questionnaire. The questionnaire is available in Appendix A. The feedback was documented, analysed and taken into consideration for the development of the initial artefact. The final review was on the CSF's artefact. As a result, feedback consisting of a number of valuable comments and recommendations was received, which will then be used to refine the research once again.

Participants are allowed to express their opinions and findings privately. This will relieve undesirable pressure from other chosen experts. Ultimately, this will encourage the participants to consider the ideas of the model based purely on the merit of that idea, and not on any other criteria.

Feedback received from the experts may be anonymously shared amongst those experts should they wish to be informed. The feedback from the experts will be presented in the next chapter.

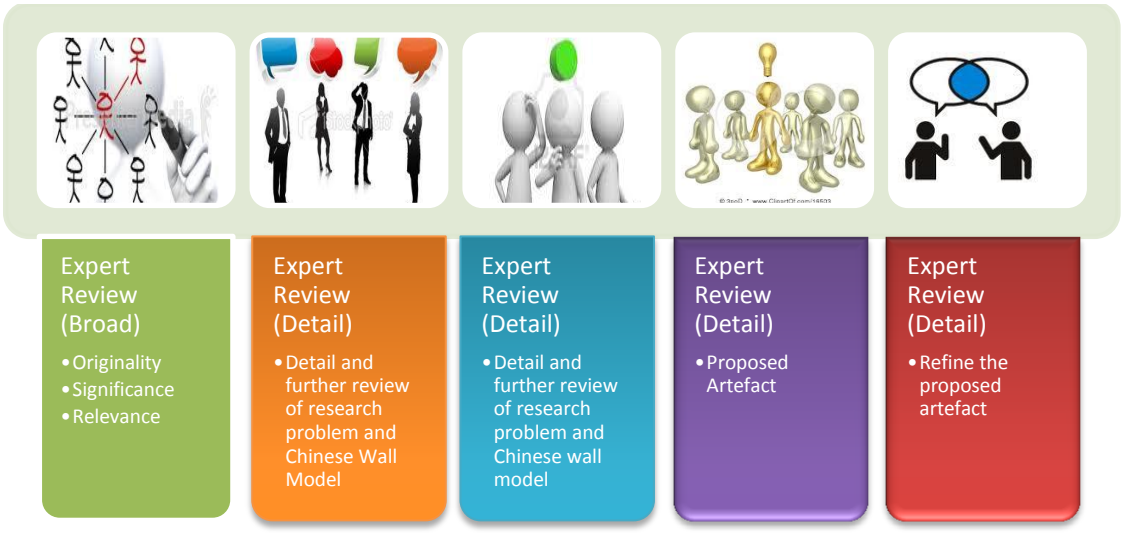


Figure 5.5 Expert review process

5.6.4 Guideline 4 – Research Contributions

It is a requirement in Design Science that the outcomes of the study are a clear contribution made in the area of a design artefact, knowledge base construction or design evaluation knowledge (Hevner *et al*., 2004). Presented in Design Science research are three major

research contributions. Included here are the design artefact, foundations and methodologies. The contribution varies according to the originality, level of detail and importance of the artefact being designed.

In any research project employing Design Science methodology, one or more of these contributions must be evident. The **design artefact** refers to a contribution which is that of a design artefact. This artefact must provide solutions to problems, extend the existing knowledge base, or apply existing knowledge in new and innovative ways.

The **foundations** contribution refers to the development of creative and well- evaluated constructs, models, methods, or instantiations. These should have the capability to extend and improve the existing foundations of the Design Science knowledge base (Hevner *et al*., 2004).

The **methodologies** contribution refers to the creative development and the use of evaluation methods such as experiments, analysis, tests, informed arguments and case studies or scenarios. These can all provide Design Science research contributions (Hevner *et al*., 2004).

The research contribution of this study aligns to the foundations artefact. This artefact will be in the form of a model and aims to address the information confidentiality issues created by the poor security of tender information in the government (as highlighted in earlier chapters of this study). This model comprises critical success factors which incorporate the Chinese Wall Model to improve the confidentiality of tender information. This will aid in reducing conflict of interest and tender fraud associated with easy access to confidential information. These form part of the elements of the artefact. The artefact contributes to the body of knowledge by proposing a thorough research solution which has not been considered by other researchers in the field.

5.6.5 Guideline 5 – Research Rigour

Research rigour essentially describes the manner in which Design Science research is conducted. Design Science research requires that in each stage of the artefact's design process (construction and evaluation) rigorous methods are applied. This ensures that research is conducted thoroughly and with integrity (Hevner *et al*., 2004).

- **Research integrity**

The ability to demonstrate research integrity is critical in research. Research integrity can be considered as a general evaluative judgement of the extent of truth contained in the study

(Saunders *et al*., 2009). This duty to represent data honestly extends to the analysis and reporting stage of the research. Lack of objectivity at this stage will clearly distort the researcher's conclusions and any associated recommendations (Saunders *et al*., 2009). In this study, the following actions were taken to ensure:

- The research design employed conformed to the philosophical stance adopted in the study.
- The use of standard questions in the questionnaires and the interview schedules used helped to ensure that the research participants were subjected to similar questions.
- Views from academic colleagues (who had an interest in the topic and were familiar with issues being researched) were sought to associate the determinants/characteristics with suitable themes.
- The government officials recruited to participate in the study were only those who were knowledgeable and who participated in the tender process.
- The study uses multiple case studies and cross-case analysis.
- The participants were requested not to answer questions posed unless they had directly observed or had knowledge of the questions posed.
- Evidence of the findings is represented in a manner that enables easy applicability by others researchers.

Saunders *et al*., (2009), further add that a great deal of trust is placed in each researcher's integrity and it would be a serious ethical issue were this to be open to question. Any research that involves humans does raise certain ethical concerns (Saunders *et al*., 2009). The sub-section that follows, therefore, presents the ethical considerations put into place to address the ethical concerns for this study.

5.6.6 Guideline 6 – Design as a Search Process

As mentioned previously, Design Science is a methodology characterised by an iterative process that aims to search for the most optimal and suitable design that best addresses the identified problem. Comprehensive search strategies produce effective, viable designs that can be implemented directly into a particular business environment for which they were designed.

5.6.7 Guideline 7 – Communication of Research

In the final stage of Design Science research methodology, effective communication of the results of the research is twofold. The research needs to be communicated to technology-oriented audiences, as well as to those in management domains.

Technology- oriented audiences require that the artefact has a sufficient level of detail for it to be implemented in a particular real- world context. On the other hand, management-oriented audiences require a higher level, value added, and process knowledge that can affect management techniques and methods in a practical way. Although this study has a high level of focus on the management audience of government, information security in general is a highly technical subject. Thus, the artefact will incorporate certain elements of technology.

The findings of this study will be presented to worldwide user groups. Relevant owners, including management of government departments, the chief information officers, head of the tender process as well as the Auditor General will be informed about this study and the proposed solution. Distribution will also be effected over the internet as an effort to encourage people to put these findings into practice. Relevant stakeholders will be educated towards better management of information confidentiality in the context of government. The following section will stress the importance of integrity in research.

5.7 Structuring data using a narrative

The reviews received from the expert reviewers were analysed in the form of a narrative. A narrative is a type of data analysis which can be used to represent the findings from primary data collection (Saunders *et al*., 2009). The primary method used to collect data in narrative approaches is through in-depth interviews. As part of the interview process, the participants provided accounts that took the form of narratives. A narrative is an account of an experience that is told in a sequenced way. This is the approach taken to represent the reviews received from the different rounds of expert reviews.

In other words, it indicates a flow of related events that are significant for the narrator and which convey meaning to the researcher (Saunders *et al*., 2009). The researcher deliberately seeks to encourage and search for meaning by asking participants to provide responses. Coffey and Atkinson (1996) note that understanding and meaning are likely to be promoted through analysing data in its originally related form. This is based on qualitative analysis with broad-based questions (Teddlie & Tashakkori, 2009). This incorporates inductive data analysis where the researcher builds the patterns, categories and themes by organising data into abstract units of information. The key idea behind the chosen qualitative

research is to learn about the problem and allow solutions based on practical experiences from the expert reviewers to emerge. This aligns with the pragmatic belief of this study. The population is clearly communicated as to the number of expert reviewers consulted in this research.

Therefore, narrative analysis allows the nature of the participants' engagement, the actions that they took, the consequences of these actions and the relationship events that followed, to be retained (Saunders *et al*., 2009). This is further supported by Creswell (2009) who states that this should be undertaken within the narrative flow of the account without losing the significance of the social or organisational context within which these events occurred.

5.8 Ethical issues

The introduction of data protection legislation has led to this aspect of research assuming a greater importance and to a need for researchers to comply carefully with the set of legal requirements protecting the privacy and interests of their data subjects (Hofstee, 2009).

"Ethics refers to the appropriateness of your behaviour in relation to those who become the subject of your work, or are affected by it" (Saunders *et al*., 2009, p. 183). Research is team work involving different people and as such, great care should be taken to prevent any one being negatively affected by the research work (Resnik, 2010). Adhering to ethical norms in research is essential in any research work.

Ethical issues are important throughout research. Saunders *et al*. (2009) provide guidance on ethical issues at the various stages of research. A detailed explanation can be viewed in Saunders *et al*. (2009, p. 188).

To ensure that ethical principles were fully observed and to guarantee anonymity of the expert reviewers recruited to participate in the study, the following measures were taken:

- The Faculty Research and Higher Degrees Committee of the University of Fort Hare approved this study and its procedures, consequently giving it ethical approval;
- Formal approval from a government department in South Africa was sought in order to receive relevant tender procedure processes, necessary tender documents and feedback on the research problem and its proposed solution. See Appendix D : Letter Requesting Access to **Department** and Appendix E : Approval Letter Granting Access to Department.
- Consent of all participants was sought before their involvement.
- The participants were fully informed of the purpose of the study, issues, benefits and risks arising out of the study.

- The confidentiality of the information provided their anonymity, position and address, was maintained.
- The interviews were securely stored, and only the researcher of this study and study supervisors had access to the raw data.

Before the interviews were conducted, all the participants were informed about the nature, conduct, benefits and risks associated with the study. The participants were assured of their anonymity and confidentiality. All participants voluntarily participated and were informed that they could withdraw from the process at any time with no adverse consequences.

5.9 Conclusion

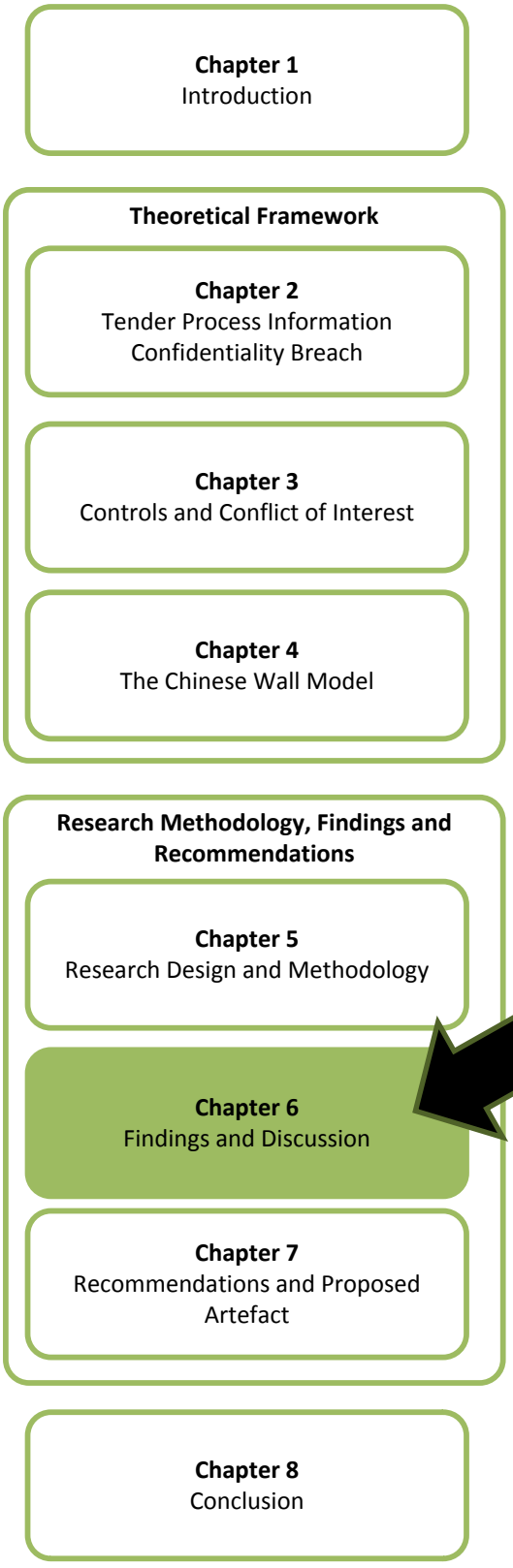
This chapter described the research methodology used in this study. Three popular research paradigms were compared; positivism, interpretivism and pragmatism. This comparison was performed to determine the most appropriate philosophy. The research philosophy chosen is that of pragmatism which focuses on the practicality of the proposed artefact. Fraudulent tender activities and the results can be generalised to a certain degree across governments in other countries which experience tender fraud; thus being inductive in nature. However, this study also explores the fraudulent activities of people in government, poor information confidentiality and conflict of interest. This suggests that the research will be significantly interpretivistic in nature.

The pragmatism position argues that the most important determinant of the research philosophy adopted is the research question. It argues that it is possible to work within both positivist and interpretivist positions. It applies a practical approach, integrating different perspectives to help collect and interpret data. This study is conducted in a way in which the researcher deems appropriate, and the results are used in ways that can bring about positive consequences within the researcher's value system.

The importance of research methodology was explained after which a detailed examination into each of the guidelines to Design Science, as provided by Hevner *et al*. (2004), was performed. The data collection methodologies used in this study were then identified and described; these were twelve expert reviewers and secondary data sources. An explanation was given on the two methods by which research can be performed, i.e., qualitative and quantitative, and it was pointed out that the pragmatism approach uses a mixture of qualitative and quantitative approach. However, this research followed the qualitative approach with inductive reasoning. Following that, was an explanation of the importance of research integrity and the adherence to ethics. Ethical concerns can occur at all stages of a research project. These concerns include seeking access to a government department,

during data collection, analysis of data and reporting on findings. Ethical clearance was received from the University, the government department and all participants. The following chapter will present the empirical findings from the expert reviews and the literature analysis.

CHAPTER 6 : FINDINGS AND DISCUSSION



Chapter 6

> "Data collection, data analysis and the development and verification of propositions are very much an interrelated and interactive set of processes".
>
> (Saunders, Lewis & Thornhill 2009, p. 488)

6.1 Introduction

Chapter five discussed the research methodology used for this study and also provided an introduction into the nature of the primary data collection method; the expert review process. This chapter discusses the research findings obtained from the expert reviewers across the four review rounds as explained in the previous chapter. These findings are analysed and interpreted for this study.

The purpose of analysing data is to create meaning from the collected raw data. This is done by comparing, evaluating and analysing the feedback received from the experts (Creswell, 2009). The various experts provide perspective on the research problem and solutions through different lenses, namely, academia, government and industry experts. Related to this is the lens from an information security point of view; whereas reviews from government officials rely more on the practicality of the Chinese Wall Model and the proposed artefact to the research context. These reviews help to clarify the research problem and strengthen the research solution.

The results obtained and illustrated in this chapter will be used to meet the objective of this study. The objective is the creation of an artefact incorporating the Chinese Wall Model to reduce the breach of confidential information in the tender process.

The discusssion will begin with a review on the originality, significance and relevance of this research project and the proposed information security model. This will be followed by an assessment of the detailed reviews received on the application of the Chinese Wall Model to reduce the breach of confidential information in the government tender process.

The final section of this chapter will present a review on the finer details of the proposed artefact. Incorporated is the analysis of the reviews received on the artefact. The artefact is designed to ensure information confidentiality and the reduction of conflict of interest as a consequence. To satisfy the Design Science requirements, these outcomes will form the basis of the proposed artefact to be discussed in Chapter 7.

In addition, the key points that emerge from the expert reviewers will be summarised in the conclusion. This summary will compress long statements into brief statements in which the main sense of what has been said is rephrased in a few words (Saunders *et al.*, 2009). By

summarising, the principal themes have emerged from the expert reviews. The findings from the expert reviewers are narrated below.

6.2 Examination of expert review opinions

This section describes the process in which the research and its main contribution was critically analysed by a number of experts. The selected sample for the Expert Review Process was a mixture representing a cross-section of information security experts and government officials.

These expert reviewers and officials are knowledgeable about information security and the tender process, respectively. It is also useful to indicate that all experts are at a senior level in their organisation with more than five years' experience in either academia or industry and all have a high level of education (graduate level and above). The in-depth interviews used to collect data from the experts, as described in the previous chapter, is powerful because it uses one-to-one interaction between the researcher and the interviewees (Saunders *et al*., 2009).

These interviews provided the researcher with the opportunity to ask for an explanation of vague answers and this allowed the researcher to provide clarification if a question was unclear. The researcher structured a few questions for each round of expert review, with the final question for each round prompted the experts with open-ended questions in case the research had overlooked something. The responses to the open-ended questions were captured and used to improve the artefact. Open-ended questions allowed the expert reviewers to express their own understanding, in their own terms as opposed to closed-ended questions that limit respondent into a particular category (Teddlie & Tashakkori, 2009).

By following the Expert Review Process, twelve experts were interviewed, and were requested to conduct a critical analysis of the main contribution of this study. This analysis occured over four rounds of review, with feedback from each round serving as the refinement of the research contribution. Table 6.1 shows the expert review rounds, together with the number of experts, experience in academia or industry and their level of education.

Table 6.1 Expert reviewers details

Expert Review Round	Number of experts	Area of expertise	Experience in academia or industry	Level of education
Round 1	3	Information security experts	More than 5 years	Graduate level and above
Round 2	5	Information security experts		
Round 3	2	Government officials		
Round 4	2	Information security and industry experts		

The open-ended questions asked at each round of expert review served to prompt the expert reviewers to reflect more deeply on the topic of interest. The details of the open-ended questions and the responses are follows:

6.2.1 Expert review process: Round 1

The researcher conducted interviews with South African and international academics to gather data on the originality, significance and relevance of the theoretical framework of this study. The secondary data collected and represented in the theoretical framework of this research project formed the basis of the artefact. The researcher identified the main components, themes and issues in this research project and the predicted or presumed relationships between them. This theoretical framework was summarised and presented to the experts.

The theoretical framework represents the research problem which entails the breach of confidential information and conflict of interest in the tender process, which as a consequence, leads to tender fraud. Furthermore, it analysed different access control models to manage the flow of confidential information.

These models included the Bell-La Padula Model (Bell & La Padula, 1975), Biba Integrity Model (Biba, 1977), Clark and Wilson Model (Clark & Wilson, 1987) and the Chinese Wall Model (Brewer & Nash, 1989). Of these, the proposed solution is the application of the Chinese Wall Model, which resulted in the most favourable solution in the present dynamic environment of government. The researcher showcased the alignment of the Chinese Wall Model to uphold and enforce the key tender principles.

The theoretical framework is included in Chapter two, three and four. The researcher's semi structured interview protocol included the following questions. The responses from the three experts are noted after each question.

1. **What do you think of the originality of the application of the Chinese Wall Model to the problem of the breach of confidential information in the government tender process?**

The experts noted that the Chinese Wall Model was definitely an original approach to the research problem. The explanation of how it was applied in investment banks assisted with an understanding of the security concepts of the Chinese Wall Model. Consequently, the problem of insider trading or conflict of interest which exist in investment banks was shown to be similar to that in government tenders. The application of the model to manage the flow of confidential information in the tender process was clearly explained.

The experts further added that the terminology of sanitisation was creative by limiting the access of confidential information to government officials who have authority to access all tender information. It was further stated that the chosen case studies were relevant and significant for the application of the adapted model.

2. **Will this study significantly add to the body of knowledge?**

Firstly, given the extent of the tender fraud, government cannot rely solely on the fraudulent officials to behave in a trustworthy manner. The Chinese Wall Model can increase the reliance of trustworthy information in the tender process, by managing the flow of confidential information. Secondly, the security of the tender related information must become part of the socio-organisational culture. Thus, the introduction of the Chinese Wall Model to the tender problem is significant, which will allow for future research to be conducted in this area.

3. **Do you think this study is relevant?**

The experts agreed that the research had a solid theoretical framework. The research problem was clear and the use of case studies together with recent articles published in the newspaper indicated that conflict of interest was a serious problem in the South African government.

Thus, there is an urgent need to reduce the breach of confidential information in the tender process and reduce the wastage of tax payers' money as indicated by the experts. One expert stated that "This study of information confidentiality in the South African government is indeed interesting and relevant."

4. Do you have any further comments and recommendations?

An expert reviewer explained that it would be worthwhile researching the breach of trust in government tenders. In addition, it was added that "the breach of trust is precipitating fraud in the government tendering process, which seems to be a socio-organisational issue that is extemporaneous to the information system." The researcher agreed with the reviewer that trust and even ethical issues contribute to tender fraud, but managing access control by using the proposed model could possibly induce a fiduciary to be completely trustworthy and ethical in the tender process.

Furthermore, it was recommended that the term conflict of interest be clearly defined and how it impacts the fiduciary duties of a government official. Subsequently, this was elaborated in the study.

The expert reviewers stated that the diagrams explaining the Chinese Wall Model reflected a good graphical representation of the model with well substantiated arguments. However, it was suggested that the sanitisation diagrams should be more clearly illustrated. The relevant diagrams were then redrawn and improved accordingly.

The response from these expert reviewers was used to further develop and refine the study. The next round will outline and discuss the expert reviews attained from both experts in academia and industry. Consequently, it justifies the use of the Chinese Wall Model explained in the literature review chapters.

6.2.2 Expert review process: Round 2

After the first round was completed, the research project was updated, and a second round of review commenced. The expert reviews from five experts in this round, shed light on this study from the lens of an information security point of view.

The interactive nature of data collection and analysis allowed the researcher to recognise important themes, patterns and relationships which further refined this study. As a result the researcher was able to re-categorise the existing data to see whether these themes, patterns and relationships were present in cases where data had already been collected. The researcher's semi structured open-ended questions for this round are included in order to refine the main recommendations.

1. Do you think that the Chinese Wall Model will reduce the breach of confidential information in South African government tenders?

It has been stated that the model can help reduce tender fraud from a high rate of 74% (as mentioned in the literature review chapters) to an estimate of 40% for example. Therefore,

government would be in a better position to have this access control model implemented than without the model. This can be achieved by reducing the breach of tender information as explained to the expert reviewers.

An expert reviewer noted that the various information flow models were analysed in the theoretical section of the research project which showed that the researcher had explored various options of information flow models. However, an expert noted that the Role Based Access Control model (RBAC) was not considered. RBAC is an information security approach to restrict access only authorised users (Slay & Koronios, 2006). The expert reviewer further questioned the researcher by asking if the RBAC model could work in the context of government tenders in South Africa. The researcher explained that RBAC would not be ideally suited as it leans more towards assigning security levels depending on the position of the government official. The Chinese Wall Model looks beyond assigning security levels to officials. It rather considers managing access with a given security level as most government officials who breach tender information actually have authorised access to the tender information as per their security level. The researcher also indicated that this was why the conflict of interest continued to exist as the authorised officials has access to all datasets (supplier tender information). The expert said that "using the Chinese Wall Model is an interesting approach."

2. How practical is the Chinese Wall Model to reduce the conflict of interest and information confidentiality problem?

The experts indicated that the application of the Chinese Wall Model to the tender process was quite original and theoretical. It should achieve the project's research objective. This study should add to the body of knowledge and hence suggest a solution which practically works as seen in other contexts such as investment banks and law firms. However, in terms of the government where tender fraud has been prevalent for so many years, it is not expected to immediately reduce the breach of all confidential information in the tender information systems. This is because tender fraud in South Africa's government has existed for many years; there are many aspects to consider outside of the tender information system. The experts further added "the managing of confidential information in the tender system using the Chinese Wall Model is an electronic solution to breach in information security solution. This proper management of the tender information electronically is partially a solution to the tender fraud. Tender information which is not captured electronically must be managed properly as well to reduce tender fraud".

One of the experts was impressed with the concept of sanitisation and that the supplier's name on the tender document must remain hidden should an official need to access other tender proposals for the same tender. However, a problem exist at present because tender

documents and forms contain the supplier's name, which makes it difficult to maintain anonymity. Thus, government may need to design a new template for the supplier to complete, in such a way that the supplier names are hidden from the respective individuals invovled in the tender process. This needs to be in place before supplier information is captured electronically and the necessary tender scores calculated.

It further follows that the expert reviewers questioned whether all the tender information is electronically saved. The Chinese Wall Model would only work if the tender documents were electronically saved. The experts therefore stipulate, that an electronic document management system was needed if this proposed solution was implemented.

To further add to the practicality of the Chinese Wall Model, the datasets of the model refer to the complete tender proposals as received by a supplier. However, one expert reviewer noted that these datasets can also refer to the different chapters across all tender proposals received. In other words, all of Chapter one from the tender proposal can form part of the dataset. This shows the dynamic nature of the proposed model. Where the different chapters could be in conflict with each other, access to information in the chapters of the proposals can be restricted. This adds additional practicality to the Chinese Wall Model.

3. Do you have any further comments and recommendations?

An expert explained that certain guidelines and tender principles needed to be complied with by the government officials to improve information confidentiality in the tender systems. The expert reviewers stressed that a key principle here was *accountability*. The officials should be held accountable for any wrongdoing conducted. In addition, if the Chinese Wall Model should be implemented in government, and there was a breach of the security model, the individuals involved should be held accountable for their actions.

In addition, the Chinese Wall Model must be consistently implemented for all tender processes within a government department. The experts added that previous information security interventions introduced in the government, were no longer in use due to consistently poor implementation and monitoring. Thus, certain success factors should be identified to ensure compliance and successful implementation of the model so that the same mistakes are not repeated.

After this stage was complete, the proposed Chinese Wall Model was sent to two more experts who managed the tender process. As a result, feedback consisting of a number of valuable comments and recommendations was received and is elaborated below.

6.2.3 Expert review process: Round 3

Research of this nature is based on individual accounts of experiences and the ways in which they explain these through their subjective interpretations and relate them to constructions of the social world in which they live (Saunders *et al*., 2009). This type of analysis from this round of review commences inductively, and needs to remain sensitive to the social constructions and meanings of the government official experts who participate in this study.

While reviews were received from information security experts in the previous rounds, it was necessary for the researcher to obtain views from the experts who participate in the tender process. This provides a different and additional insight. It is for this reason that the same questions as mentioned in the previous round were posed to the expert reviewers in this round. Input received from the government experts takes into account the practical aspect of this research project and ultimately conforms to the philosophical stance of pragmatism.

1. Do you think the Chinese Wall Model will reduce the breach of confidential information in South African government tenders?

The expert reviewers stated that the researcher had captured many of the glaring issues facing the government tender process and the weaknesses in the current systems. There was definitely merit in the researcher's proposed approach.

Also, gratitude was received on the alignment of the Chinese Wall Model to the tender principles.

2. How practical is the Chinese Wall Model to reduce the conflict of interest and information confidentiality problem?

Approval was received on the application of the Chinese Wall Model to manage the flow of confidential information. The experts were pleased with the concept of sanitisation proposed by the Chinese Wall Model. They further noted that a document management system was needed to manage the tender documents.

The experts further added that the Chinese Wall Model could be a start to reducing the breach of confidential information. However, with the considerable number of supplier proposals received by government for certain tenders, it would be impossible to restrict a user to access of only one dataset (supplier's tender information) in a conflict of interest class. The experts added that the government may need to have more government officials on the tender boards and bid committees to accommodate user access to only one dataset in a conflict of interest class. To emphasise this point, the experts were concerned with the practical application of the Chinese Wall Model to the government tender process as it may

not always be possible to increase the number of members in a bid committee or to restrict user's access to only one dataset (supplier tender information) in the conflict of interest class as proposed by the Chinese Wall Model.

However, the experts agreed that the government was in a better position to, for example, view three datasets, instead of all datasets. This would reduce the conflict of interest significantly, even if not eliminate it.

3. Do you have any further comments and recommendations?

The government officials stipulated that it had become a painful reality that lawmakers and regulators tended to add more rules and controls when there is a lack of compliance. The expert reviewers noted that the reason for lack of confidential information in the tender process and the consequence of fraud is due to the lack of compliance by the government officials.

One expert pointed out difficulty for government officials to comply with regulations when guidelines are different at national and provincial level. An expert presented the diagram as seen in Figure 6.1 and mentioned that the government departments across the country do not always comply with the guidelines as they vary across provinces. The experts further added that the essentials of the Chinese Wall Model, should it be implemented, must be made clear and implemented consistently at both national and provincial levels. This adds further motivation for the researcher to identify essentials factors of the Chinese Wall Model to improve tender information confidentiality.

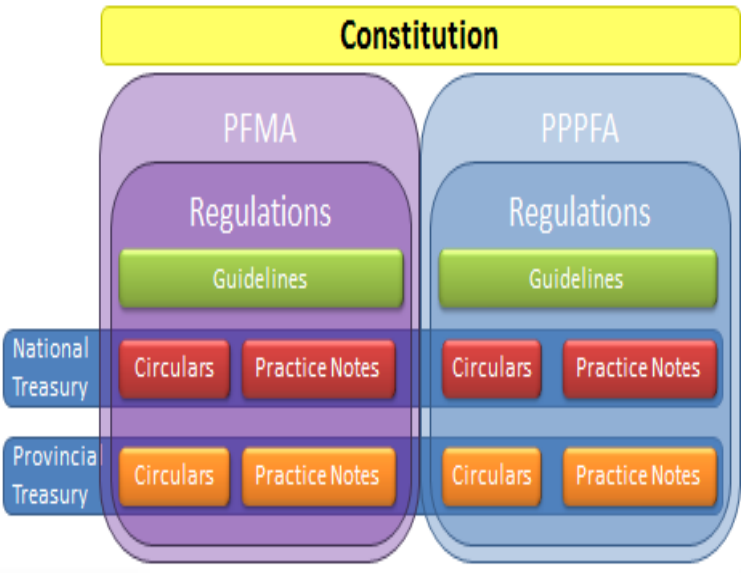


Figure 6.1 Tender regulation (Louw, 2012)

The analysis of the three rounds of review helped to identify important factors which must be complied with for the effective implementation of the Chinese Wall Model. Especially since this study considers the practical aspects of the study and consequently, the critical success factors. The next expert review round considers questions posed and responses received on the proposed Critical Success Factors (CSFs).

6.2.4 Expert review process: Round 4

The theoretical framework of this study was used to develop the proposed artefact. The expert reviewers in this round were industry experts knowledgeable about information security. The two experts were encouraged to explore their own experiences, perceived success factors and measures undertaken to secure information. The reality, as perceived by the experts, had to be described in terms of the meaning the experts attached to the elements of the field of study to which they had to respond. The CSFs needed multiple sources of their knowledge, including insight into their values, experiences, cultures and the way in which they interpret and understand these.

The expert reviewers were presented with the research problem, the objective of this study and the five critical success factors. A diagrammatic representation of the tender process and the vulnerable steps were demonstrated together with an in-depth discussion on how the CSFs addressed those steps. The researcher also showed that CSFs, together would solve the overall problem of this study.

The experts were asked to critique the critical success factors, and the concepts around which they were based, and provide any comments, thoughts, opinions, suggestions or judgements on each area. Questions were posed to the expert reviewers and their expert reviews are included below.

1. Would the five critical success factors help to solve the research problem?

The experts indicated that Critical Success Factors should be tangible, observable and measurable and therefore the proposed success factors met the definition of critical success factors. Additionally, they suggested that if the activities associated with the factors were performed at the highest possible level of excellence, the Chinese Wall Model would indeed, be effective, controlling the conflict of interest in tenders and thus improving the confidentiality of information. The experts added that the critical success factors solved the research problem.

The experts made the following comments on the critical success factors.

CSF01 – Sanitisation Policy Document is a key to understanding how to manage and restrict user access control in the tender process.

CSF02 – Electronic Document Management System, must exist to implement the Chinese Wall Model, as it addresses the electronic flow of access to confidential information.

CSF03 – Tender Evaluation Ethics Document, should already be implemented in government departments to guide the tender process. This factor is therefore important and without doubt influences the way in which tender information is stored electronically.

CSF04 – Audit Log is important as it will keep a track record of users granting access to datasets and users authorised to access the datasets as per the Chinese Wall Model. The experts also noted that government officials should be held accountable for their fraudulent acts.

CSF05 – Tender Register for Defaulters, keeps records on government officials who corrupt the tender process. Thus, individuals who breach the security of the tender information, should be prosecuted. This points to the approval of the fifth critical success factor. These Critical Success Factors wil be discussed in more detail in the next Chapter.

2. Do you think the proposed critical success factors have a serious impact on the effectiveness of the Chinese Wall Model and its role to improve confidentiality of tenders?

The experts noted there were many risks in the tender process; conflict of interest and the breach of confidential information were high risk. At times it is difficult for government officials to collectively focus on the true essentials of this risk as priorities differ among government officials. The experts indicated that by identifying the critical success factors, the government could create a common point of reference to direct those participating in the tender process.

They also added that the critical success factors would definitely impact on the effectiveness of the Chinese Wall Model. This in turn, would assist with compliance to the tender principles and achieve the goals of the tender process.

3. Do you have any further comments and recommendations?

The experts were impressed with the approach followed in creating the artefact. It was stated that the alignment of the success factors to the tender process and research questions were well thought out and the experts commended the researcher. The experts gave positive feedback and recommended the proposed Critical Success Factors to the researcher of this study.

Furthermore, one of the experts emphasised “keep in mind that the Chinese Wall Model together with the artefact is proposed to reduce the research problem rather than completely eliminate the breach of confidential information in the tender process.”

The experts approved the names of four critical success factors. They recommended that the fifth critical success factor, CSF05, be renamed from Tender Register for Defaulters to Chinese Wall Model Prosecution Register as it better describes the register. This recommendation was considered by the researcher.

The researcher took the advice of Creswell (2009) who concluded that data analysis is one of the issues that a researcher should consider at the time when the proposal is formulated. The process of analysing the data in this study began at the time when secondary data was collected and was continued until the final artefact was produced. The expert reviews presented above better justified the proposed critical success factors. These will be discussed in-depth in the next chapter. Following, is the alignment of the Design Science guidelines to this study.

6.3 Design Science Guidelines and this study

This study adopts the Design Science Guidelines as introduced by Hevner *et al*. (2004). Demonstrated in this section, Table 6.2, is the compliance of the seven guidelines to this study.

Table 6.2 Design Science Guidelines and this study

Guideline	Description	This study
Guideline 1: Design as an Artefact	Design Science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	This research produces a viable artefact, the Critical Success Factors incorporating the Chinese Wall Model to reduce the breach of confidential information in the government tender process.
Guideline 2: Problem Relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.	The proposed artefact is an information systems based solution important to the problem of information confidentiality breach in government tenders.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The utility, quality, and efficacy of the design artefact is demonstrated via the expert review process as represented in this chapter.
Guideline 4: Research Contributions	Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	This study adds to the body of knowledge concerning government tenders and the application of the Chinese Wall Model.
Guideline 5: Research Rigor	Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Open-ended questions were posed to the experts and written up using a narrative analysis. Views from individuals in academia and government and industry were sought.
Guideline 6: Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	The means used to reach the desired artefact are those of secondary data collection and the expert review process which provided the primary data to evaluate this study.
Guideline 7: Communication of Research	Design Science research must be presented effectively both to technology-oriented as well as to management-oriented audiences.	Interviews were held with the expert reviewers, where open-ended questions were prepared and posed to the experts who are senior in their positions. These include system-orientated information and government orientated experts. Also, one research paper has been published and the other is under review.

It can be seen that the researcher acknowledged and complied with the Design Science Guidelines. Following, is the chapter conclusion.

6.4 Conclusion

This chapter analysed the data received from the four expert review rounds. In particular, the expert review process was considered for this study in order to obtain an in-depth insight of the research problem and proposed solution. This reflects insight from two different lenses. One being, contribution from an information security point of view and the other from the practical point of view of the government and industry. Insight thorugh different lenses adds richness to the overall contribution of this research and the proposed artefact.

Open-ended questions, following inductive reasoning and the qualitative approach were posed to the experts. The open-ended questions generated considerable information, which lead to reconceptualization of the issues under study.

A narrative approach to analysing data was considered in this chapter. The findings highlight confidence in the thoroughness and credibility of the conclusions drawn from the expert reviewers. This is summarised in Figure 6.2.

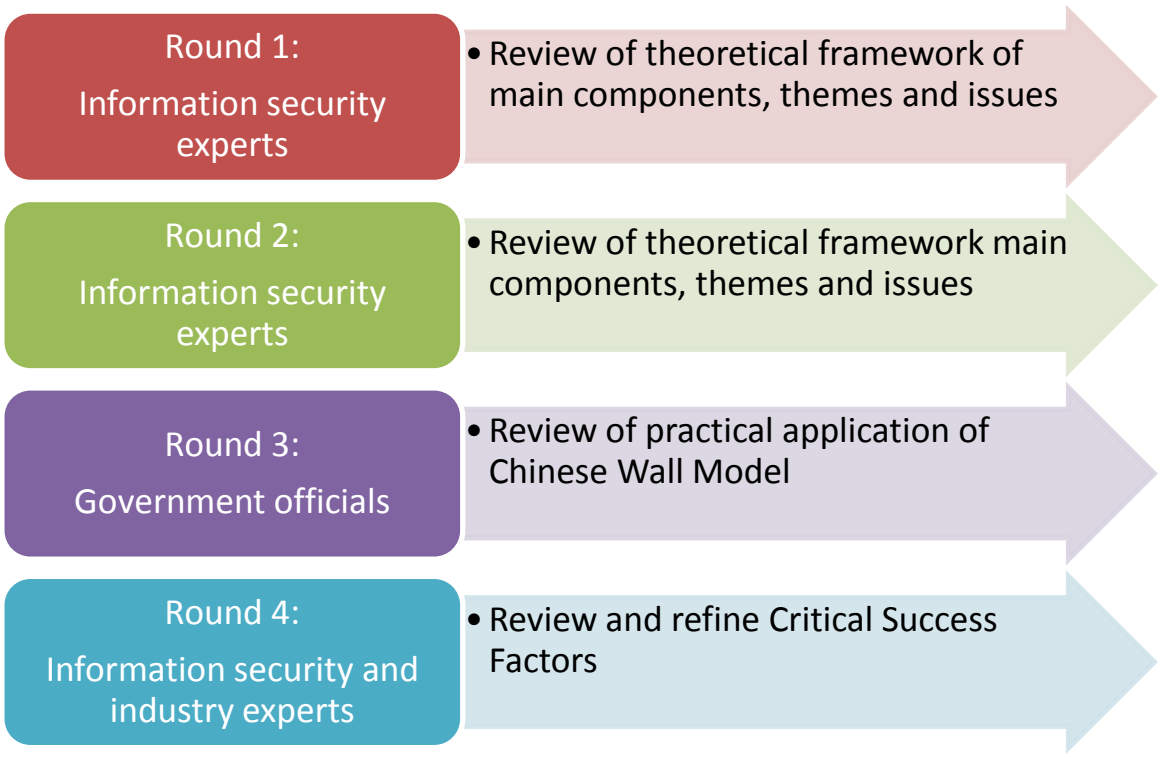


Figure 6.2 Purpose of expert review rounds

The first round reviewed the theoretical framework of this study consisting of the main components, themes and issues in this research project and the predicted or presumed relationships between them. This framework was assessed against the criteria of originality, significance and relevance. The purpose of this round was to link this research project to the

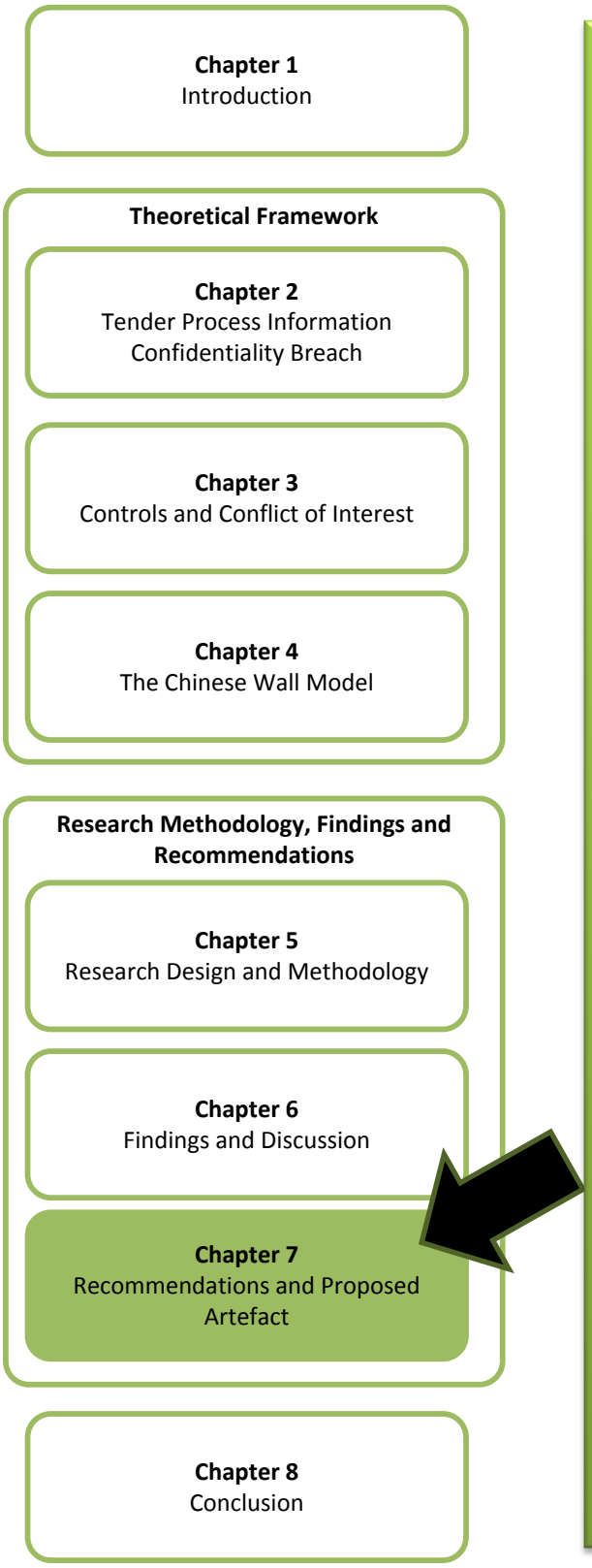
existing body of knowledge in this researchers' subject area. It helped the researcher to initiate the expert review process and to provide a plausible theoretical framework.

The second round of review commenced with information security experts. These experts are knowledgeable on the topic of information security and information flow models. Questions were asked on the practicality and suitability of the Chinese Wall Model with regards to the breach of confidential information in the government tender process. Approval was received on the practicality and suitability of the Chinese Wall Model to reduce the breach of confidential information in the tender process. There were reservations about the the increase in government officials required to implement the restriction of access to a dataset to only one official within a conflict of interest class. This assisted with refinement of the proposed solution. It was presented to experts from the government and industry as explained in the third and fourth round of review.

The third round of review commenced with government experts. This round of review helped to obtain insight into the practical nature of a model based on insight from those individuals who participate in the tender process. Suggestions and recommendations were received from the experts which helped in devising the proposed artefact for this study.

The proposed artefact was presented in the final round of review. The researcher presented the proposed critical success factors, together with the research problem and objective of this study to the industry consultants. Consensus on the proposed critical success factors was received from the experts and the recommendations considered. The concludes by showing that the Design Science Guidelines have been complied with in this study. The next chapter elaborates on the proposed artefact.

CHAPTER 7 : RECOMMENDATIONS AND PROPOSED ARTEFACT



Chapter 7

> "The design artefact is a research contribution which either provides a solution to the problem, extends the existing knowledge base or applies existing knowledge in a new and innovative way".
>
> (Hevner et al., 2004)

7.1 Introduction

The preceding chapter presented the findings from the primary data collected during the expert review process. It described in detail the purpose of each round of review and the outcome.

Together, analysis from the expert review findings, research methodology and literature review presented thus far were analysed to develop the proposed artefact which is the focus of this chapter. The premises derived from the theoretical framework and primary data will be elaborated to demonstrate the sub-conclusions and conclusions obtained. These conclusions are used to develop the proposed artefact. This chapter represents the proposed Critical Success Factors (CSFs) incorporating the Chinese Wall Model to reduce the breach of information confidentiality, specifically in the government tender process.

Directly following this introduction is a section dedicated to the initial research, showing the problem steps in the tender process. The proposed CSFs model will be presented demonstrating that it is influenced by the Chinese Wall Model and that the factors are aligned to the problem steps in the tender process. Thereafter, it will be shown that the CSFs address the research questions of this study. This will be followed by an evaluation of the study. Finally, a summation of this chapter is presented.

7.2 Identified problem areas

At the start of this research project, a problem was identified. This problem is the breach of confidential information in the tender process by those not entitled to access it. This breach of confidential information and unauthorised access is due to the poor system of internal control as well as lack of adherence to law and regulation (Mutula & Wamukoya, 2009; Kaisara & Pather, 2011). The flow of confidential information among the officials in government is not properly managed nor is the information kept secured. In addition, those who have access to all the tender information, are able to easily manipulate tender scores due to the existence of conflict of interest among some of the government officials. This, in turn results in tender fraud (Special Investigating Unit, 2011).

This problem is of great importance due to the enormous amounts of government and tax payers' money being misused. Initially, a high level approach was taken to identify the specific problem areas in the tender process that were especially weak due to a lack of securing confidential information. The problem steps in the tender process are discussed extensively in Chapter 2. It explains how information is used to corrupt the tender process. The problem steps in the tender process is given in Figure 7.1.

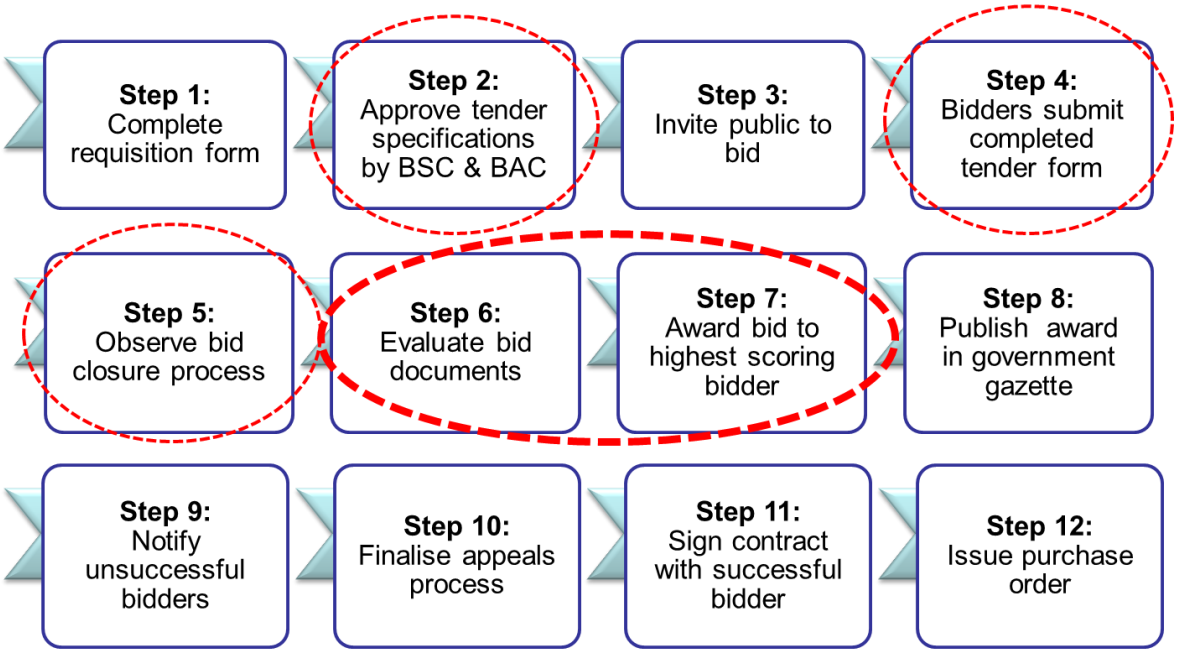


Figure 7.1 Problem steps identified in the tender process

Figure 7.1 shows that conflict of interest and breach of confidential information occurs at steps two, four and five, with steps six and seven being the key problem areas. A reminder of these problem steps with its descriptions are described in Table 7.1.

Table 7.1 Identified problem areas

Identifier	Name	Description
PROB01	**Approve tender specifications document** (Step 2 in tender process)	The specifications should be recommended by the bid committees. The committees must ensure that the functionality criteria and the preference points are approporiate to the needs of the Department. At times there are no specifications draw up or the specifications are not approved. In addition, there is little maintainance for the track record for the approval process (Mutula & Wamukoya, 2009; Special Investigating Unit, 2011).
PROB02	**Bidder submits complete tender form to department** (Step 4 in tender process)	Often there is no log containing a list of suppliers who sumitted tender documents on time. Logs are often stored in a paper trail. At times, certain government officials do not check for compliance of tender documents (Mutula & Wamukoya, 2009; Special Investigating Unit, 2011).
PROB03	**Observe bid closure process** (Step 5 in tender process)	The bid documents received from the suppliers must be placed in a tender box by a certain date and time. The applications received are not always recorded in the tender register. Once all applications are received these are sometimes not stored safely in a lockable storage facility with limited access (Kaisara & Pather, 2011; Cerrillo-i-Martínez, 2011; Gordhan, 2011).
PROB04	**Evaluate bid documents** (Step 6 in tender process)	The scores for preference points and functionality are sometimes manipulated and this results in the recommendation of an unworthy supplier. All members of bid committees have access to documents and scoring. This allows for easy breach of confidential information where there is conflict of interest (Kaisara & Pather, 2011; Special Investigating Unit, 2011; George, 2011).
PROB05	**Award bid to highest scoring bidder** (Step 7 in tender process)	At times there is biased awarding of tenders. Decisions are made on manipulated information. Tenders are awarded without complying with the tender process. It is proven that the entire process has been compromised, yet the tender has been awarded to a supplier (Republic of South Africa, 2003b; Department of Human Settlements, 2009).

The problem areas were identified and defined; the controls currently in place to manage the breach of confidential information were examined in Chapter three. The research concluded that there was a poor system of internal controls, and lack of compliance with existing controls. Thus there was a need to examine the controls used in other countries and where suitable, learn from them. In addition, various information flow models were analysed. The Chinese Wall Model was decided upon as the most appropriate for the problem at hand. This resulted in the need to develop Critical Success Factors that would help with improving the control of access to confidential information by using the Chinese Wall Model to reduce the conflict of interest in tenders. The thought process for the proposed solution is represented in Figure 7.2.

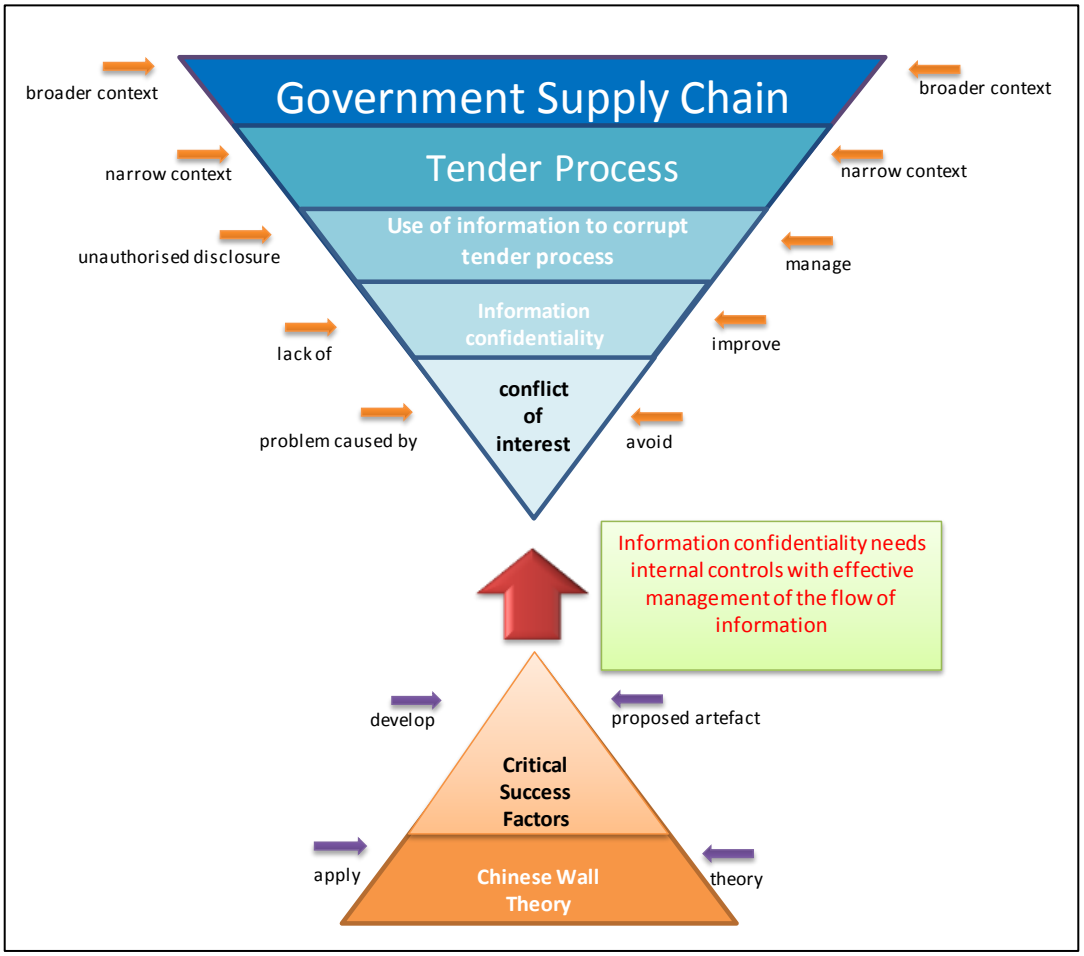


Figure 7.2 Research problem versus proposed solution

7.3 The development of the critical success factors

The section will define the concept of critical success factors. Following, is the definition of critical thinking and how it is applied in this study to develop the proposed artefact. Thereafter, the development of the proposed artefact is explained.

7.3.1 Critical success factors defined

Critical Success Factors (CSFs) are the limited number (usually between 3 to 8) of characteristics, conditions, or variables that have a direct and serious impact on the effectiveness, efficiency, and viability of an organisation, programme, or project (Business Dictionary, 2012). Activities associated with CSFs must be performed at the highest possible level of excellence to achieve the intended overall objectives (Business Dictionary, 2012).

The identification of the success factors will help government to quickly identify the elements which must be achieved to prevent unauthorised access to confidential information and thus reduce the conflict of interest. In order to strengthen the argument line for the CSFs chosen in this study, the researcher followed a particular thought pattern which will demonstrate the construction of an effective argument.

7.3.2 Critical thinking defined

The **argument** line involves critical thinking which is the skill of correctly evaluating arguments made by others. The argument consists of premises and a conclusion. The **conclusion** is the statement that the argument is intended to support. The **premises** are the statements intended to support the conclusions (Rainbolt & Dwyer, 2012). A **statement** is a sentence that makes a claim that can be either true or false (based on the evidence).

Gray (2012) notes that with critical thinking the advantages of proposing the artefact are based on thoughtful understanding of arguments and presenting the overarching, shared aims across arguments. The critical thinking process used here entails a conversational writing style and logical form representing the researcher's thought process.

This innovative semiformal method of standardising arguments will help to illustrate how the researcher decided on the proposed CSFs. This will be done without sacrificing accuracy or detail.

The aim is to put together a series of premises which support the conclusion. In addition, the conclusion can consist of sub-conclusions (Gray, 2012). This will ensure that the argument line is substantiated and clear, and above all convincing. The argument line takes the format represented in Figure 7.3.

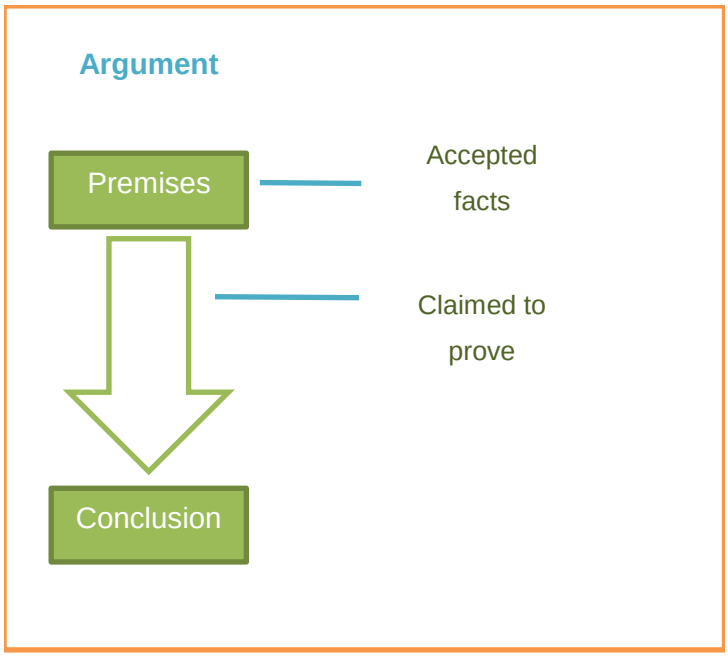


Figure 7.3 Format of argument (Rainbolt & Dwyer, 2012)

In a diagram format, each statement is represented by a number in a circle (See Figure 7.4.). A line with an arrow pointing from the premise to the conclusion is the inference (Rainbolt & Dwyer, 2012). A conclusion is the circle which is touched by the point of the arrow.

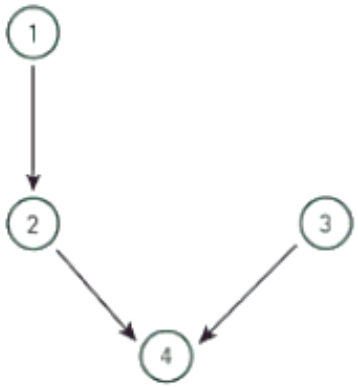


Figure 7.4 A template for the argument diagram (Rainbolt & Dwyer, 2012)

In a set of linked arguments as presented in the next section, a number of sub-conclusions lead to the overall conclusion. The conclusion is the set of critical success factors collected together.

7.3.3 The argument

A graphical representation of the argument for the development of the CSFs is represented in Figure 7.5. Thereafter an explanation follows with a list of premises and conclusions. The argument is constructed with the help of a mind map of all the chapters put together. See Appendix F : My Critical Thought Mind Map.

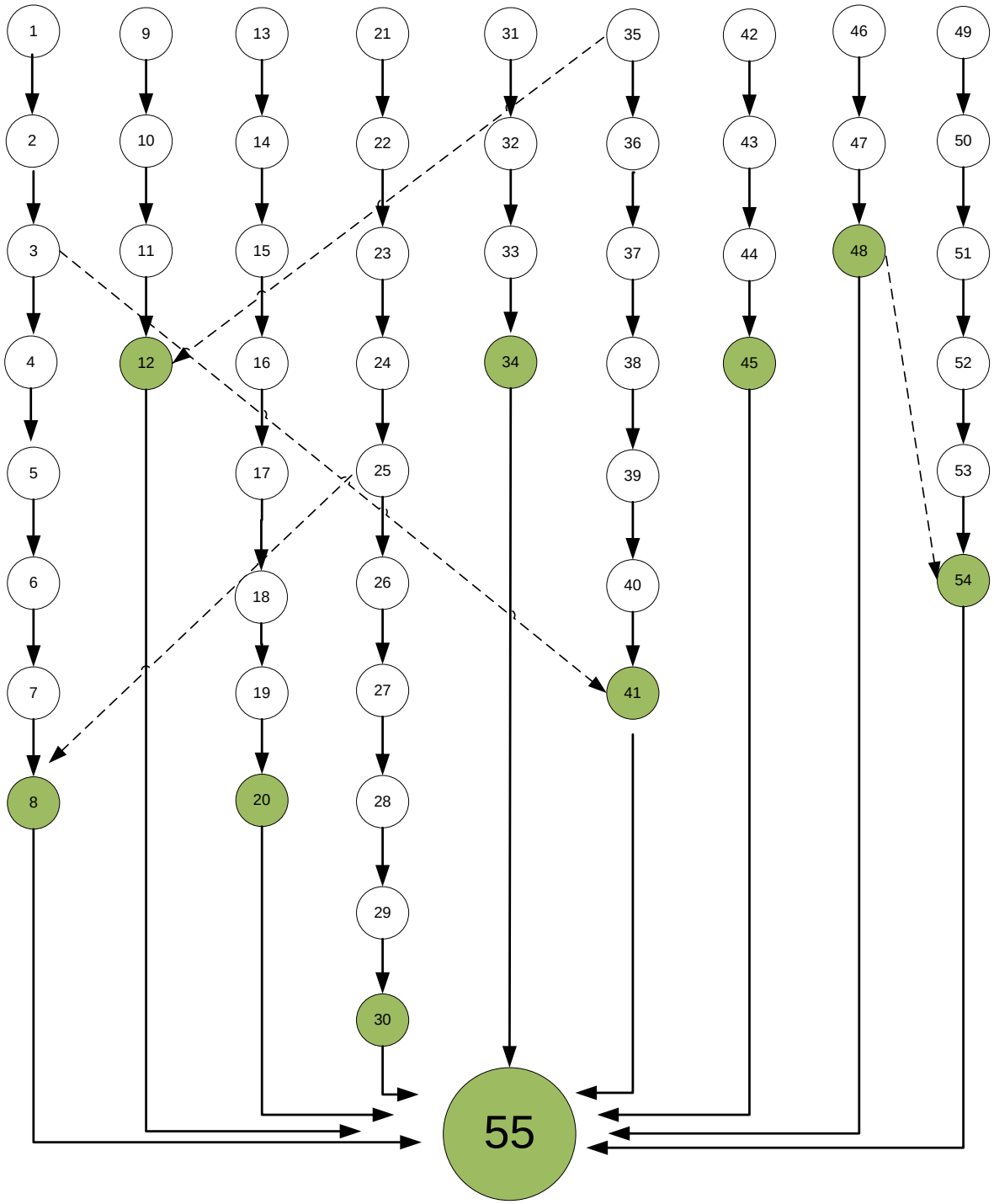


Figure 7.5 My argument diagram

The sub-conclusions are represented by premises [8], [12], [20], [30], [34], [41], [45], [48] and [54]. These sub-conclusions together justify the need for the proposed CSFs. This leads to the conclusion in the argument represented by [55]. It must be noted that certain premises merge to add to the logical thought of a sub-conclusion. For example, premises [3] links to [41], [35] link to [12], [25] links to [8] and [48] links to [54]. The derivation of the conclusion is explained below.

[1] The South African government outsource certain good and services to suppliers by following the tender process.

[2] The tender process is guided by law, regulations and tender principles.

[3] Only some of the tender information is stored electronically and user audit log is not always maintained.

[4] At times there is no audit trail for the decisions made on the approval of tender specifications, evaluation or recommendation of a tender to a supplier.

[5] There is a poor system of internal controls leading to easy access to confidential information in the tender process.

[6] There is poor monitoring of access to confidential information resulting in officials not always held accountable for tender fraud.

[7] Officals cannot be held accountable for their fraudulent behaviour if the audit log does not record the corrupt actions of the officials in the tender process.

Therefore,

[8] An audit log of user access to tender information is needed.

[9] Not all officials understand ethical/unethical behaviour when making decision on tender specifications, tender evaluations or tender award.

[10] Tender scores calculated for suppliers are sometimes manipulated, resulting in biased decisions and awarding of a tender.

[11] Manipulation of tender information corrupts the tender process.

Therefore,

[12] A tender evaluation ethics document is needed.

[13] Various controls (preventative, corrective and detective controls) work together to make up a system of internal controls as represented by GTAG1.

[14] The government of South Africa has laws and regulations which focus on preventative, corrective and detective controls.

[15] These controls are not adequate to address the system of internal controls, nor do they adequately secure confidential information in the tender process.

[16] The Chinese Wall Model is proposed as a preventative control to reduce conflict of interest and manage the flow of confidential information in the tender system.

[17] The current controls in place in the tender process are assessed using the Common Criteria Security Model (CCSM).

[18] The principles introduced by the CCSM are relevant to the tender process as they can be used to identify criteria relevant to information security and the relationship that exists between the criteria.

[19] The CCSM evaluated devices such as firewall and encryption boxes.

Therefore,

[20] The application of the Chinese Wall Model forms part of a countermeasure where the lack of information confidentiality poses threat as identified in the CCSM.

[21] Controls in ISO/IEC 27002 (2005) can be used as guiding principles for the management of confidential information.

[22] Given that not all controls from ISO/IEC 27002 (2005) are applicable to information confidentiality and conflict of interest in the tender process, the important controls highlighted include security policy, organisation of information security, human resource security, access control and compliance.

[23] User access to confidential information can be checked against an audit log as part of the access control measures.

[24] ISO/IEC 27002 (2005) indicates that information systems must be checked for compliance with the security policy.

[25] For this reason compliance with the Chinese Wall Model can be checked against the audit log to determine if users have defined access to dataset(s) as outlined by the model.

[26] The application of the Chinese Wall Model in foreign countries and in other context such as investment banks was researched to understand the model and its purpose.

[27] Also, controls in the tender process across other countries were researched to determine the regulations enforced for breach of confidential information and tender fraud.

[28] These controls were analysed to understand the solutions proposed or enforced in foreign countries and thus to assist with the development of a solution for the problem in South African tenders.

[29] The focus is on certain developing countries as South Africa is a developing country.

Therefore,

[30] Regulation and internal controls across developing countries were contrasted against developed countries to show comparison and presented that there is not much research available on managing acess control as well as information confidentiality in government.

[31] Four information flow models were identified to manage access control and flow of confidential information.

[32] These models were compared and it was concluded that the Chinese Wall Model is best suited to address the conflict of interest in a dynamic environment such as the South African government where datasets (supplier proposals) are constantly in flux.

[33] Individuals have been prosecuted for not complying with the rules of the Chinese Wall Model where the model has been implemented already.

Therefore,

[34] Individuals must be prosecuted for breaching the model and a Chinese Wall Model Prosecution Register must be maintained.

[35] Research shows that ethics in the tender process is a key principle.

[36] With the Chinese Wall Model, an '*ethical wall'* is put up restricting the official to access information which is in conflict with another dataset or on the *'wrong side'* of the wall.

[37] The Chinese Wall Model requires information to be stored electronically in a three layer hierarchy namely: conflict of interest class layer, company dataset layer and object layer.

[38] Expert reviews reveal that not all tender information is stored electronically.

[39] The expert reviewers stated that government needs, consistently, to store tender information electronically throughout the tender process.

[40] Information must be stored in a manner that ensures that the identity of the supplier (dataset) remains hidden during the tender evaluations to comply with the sanitisation concept of the Chinese Wall Model.

Therefore,

[41] An electronic database management system (EDMS) must be implemented and used consistently throughout the tender process.

[42] A government official may need to access datasets (supplier information) which are in conflict with one another in order to compare information (objects) for certain decision-making.

[43] The official may be allowed to access datasets within the same class provided that the identity of the dataset (supplier name) remains hidden in order to avoid conflict of interest.

[44] Sanitisation must be implemented properly, otherwise the Chinese Wall Model becomes useless.

Therefore,

[45] It is essential that a sanitisation policy document be compiled, understood and adhered to.

[46] This research follows the philosophical stance of pragmatism.

[47] An important aspect of pragmatism is the practicality of research and the proposed solution.

Therefore,

[48] The proposed Chinese Wall Model and the CSFs can be aligned and are practical in the current South African government tender process.

[49] The research methodology accepted in this study was Design Science.

[50] Guideline three of Design Science methodology, design evaluation, was achieved with four rounds of expert review.

[51] In order to comply with guideline five of Design Science methodology, rigorous methods were applied to evaluate the design artefact.

[52] This will demonstrate the ability to ensure research integrity which is critical throughout the study.

[53] Chapter five explains that research integrity and ethics are adhered to in this study.

[54] Approval and consensus on the proposed CSFs were achieved by the expert reviewers.

Therefore,

[55] The proposed CSFs are: a Sanitisation Policy Document, Electronic Database Management System (EDMS), Tender Evaluation Ethics Document, an Audit Log and a Chinese Wall Model Prosecution Register.

The next section addresses the five CSFs. Their importance and focus in the tender process are explained.

7.4 The proposed critical success factors explained

This section lists the critical success factors which have been validated during the Expert Review Process. An explanations of each critical success factor follows.

7.4.1 Sanitisation policy document

This document specifies when the identity of a dataset or supplier name must remain disguised or unidentifiable. The document must specify which government official should have access and allow for editing of information in the datasets. It notes who specifically should be allowed only to view the information. This is determined by the number of officials participating in the scoring of suppliers. It explains how the policy must be implemented.

Sanitisation can be used as a protection mechanism against abuse and unauthorised access to information. This policy ensures a condition of sanitisation by ensuring that write access to a particular class, dataset and object will only be allowed if the subject (official) has specific write access to a data set which is not in conflict with the initial dataset. Ineffective

implementation of the policy reduces the Chinese Wall Model useless. Meanwhile, breach of the policy can lead to prosecution.

7.4.2 Electronic document management system

An electronic system dedicated to the management of the tender documents and the necessary compliance checklist is essential for effective implementation of the Chinese Wall Model. Currently, no tender information is stored electronically, and the information which is stored electronically is not securely kept; an electronic management system of the documents is essential.

Although the Chinese Wall Model controls the flow of confidential information in the tender process, tender information needs to be stored electronically and in a certain format. This facilitates the implementation of the read and write access to datasets within particular classes.

7.4.3 Tender evaluation ethics document

This document outlines the do's and don'ts in the tender process. It explicitly specifics how officials should behave and the necessary compliance rules for an effective tender process.

This document specifies the process for scoring tenders. Included herein is the adherence to the declaration of interest forms and oath of secrecy forms. The document stipulates how tender scores must be calculated for each tenders. In addition, to reduce conflict of interest with the application of the Chinese Wall Model, there needs to be ethical behaviour practiced on the part of government officials and strict adherence to the tender evaluation document.

7.4.4 Audit log

Audit logs should be produced and kept for an agreed period to assist in future investigations and for access control monitoring. In addition, logging facilities should be protected against tampering. The audit log, containing information about user access to datasets, as per the Chinese Wall Model, will be used to hold officials accountable for decisions made on the given dataset(s).

The audit logs for the systems storing tender information should include, when relevant:

- User IDs.
- Dates, times, and details of key events, e.g. log-on and log-off, users who upload documents onto the system; users who calculate tender points; users who recommend a tender to a suppliers.
- Tender document compliance checklists.
- Scoring points calculated for suppliers.

- Suppliers recommended.
- Files accessed and the kind of access.
- Alarms raised by the access control system.
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

7.4.5 Chinese Wall Model prosecution register

An audit trail of user interaction with the tender system must be maintained. This factor is essential in the tender process. It will assist in holding officials accountable for their actions and decisions in the tender process. The audit log must be backed up and remain secure from manipulation.

Key user interactions with the system must be determined, and audit trails set up. Furthermore, the audit trail refers not only to the logs in the digital space, but outside as well. Manual logs, registers and tender checklists must be captured or scanned into the tender system, thus linking the manual logs to the electronic logs.

7.5 The critical success factors and the problem areas

CSFs must have an owner who is responsible for meeting that particular goal. Creating and holding an owner accountable instils a culture of accountability inside the government. Once the owners are in place a process to manage the success factors and a standard reporting structure must be implemented. Once the standard report is created, the establishment of a regular reporting time frame such as monthly, should be implemented (Business Dictionary, 2012).

The identification of these CSFs will assist those involved in the tender process to have a consolidated vision of the important factors which must be in place in order to ensure information confidentiality is improved. The factors must be explicit so that members of the tender process are of the same understanding and jointly focus on the true essentials for achieving confidentiality of information. Thus, it is essential that the CSFs address the problem steps of the tender process as identified in Table 7.1.

Table 7.2, shows exactly which CSFs will address the problem steps of the tender process. This adds further justification for the proposed CSFs.

Table 7.2 The proposed critical success factors addressing the problem areas

Critical Success Factor		Problem Steps in the tender process	
Code	**Factor Name**	**Identifier**	**Problem Area Name**
CSF01	**Sanitisation Policy Document** A document that specifies the rule to implementing the sanitisation policy effectively.	PROB01	Approve tender specifications document
		PROB04	Evaluate bid documents
		PROB05	Award bid to highest scoring bidder
CSF02	**Electronic Document Management System** An information system which is integrated with the tender information system to store the necessary documents in a particular format.	PROB01	Approve tender specifications document
		PROB03	Observe bid closure process
		PROB04	Evaluate bid documents
		PROB05	Award bid to highest scoring bidder
CSF03	**Tender Evaluation Ethics Document** A document which explains the rules for taking part in the tender process. The ethical behaviour is specified and must be complied with.	PROB01	Approve tender specifications document
		PROB02	Bidder submit complete tender form to department
		PROB03	Observe bid closure process
		PROB04	Evaluate bid documents
		PROB05	Award bid to highest scoring bidder
CSF04	**Audit Log** This refers to the audit trail of key decisions made by users participating in the tender process. This will assist in holding officials accountable for their decisions.	PROB01	Approve tender specifications document
		PROB02	Bidder submit complete tender form to department
		PROB03	Observe bid closure process
		PROB04	Evaluate bid documents
		PROB05	Award bid to highest scoring bidder
CSF05	**CWM Prosecution Register** A breach of the Chinese Wall Model will lead to prosecution of the individual. The names of these individuals must be added to a register. Individulas on this list must be prevented from taking part in the tender process.	PROB04	Evaluate bid documents
		PROB05	Award bid to highest scoring bidder

Linking the CSFs to the problem steps, they are also graphically represented in Figure 7.6. This figure consists of six swimlanes namely: tender steps, role players, enabler documents, controls, key challengers and the identified CSFs to address the problem steps.

The tender steps swimlane highlights the problem steps in the tender process. The necessary criteria for each step are shown directly below in the succeeding swimlanes. The individuals responsible for the steps are represented in the second swimlane. The next swimlane shows the documents used in the tender step. The fourth swimlane shows the controls in place for the steps. This is followed by the key challengers identified in the fifth step. The sixth step shows what CSFs must be in place for effective delivery of the tender step.

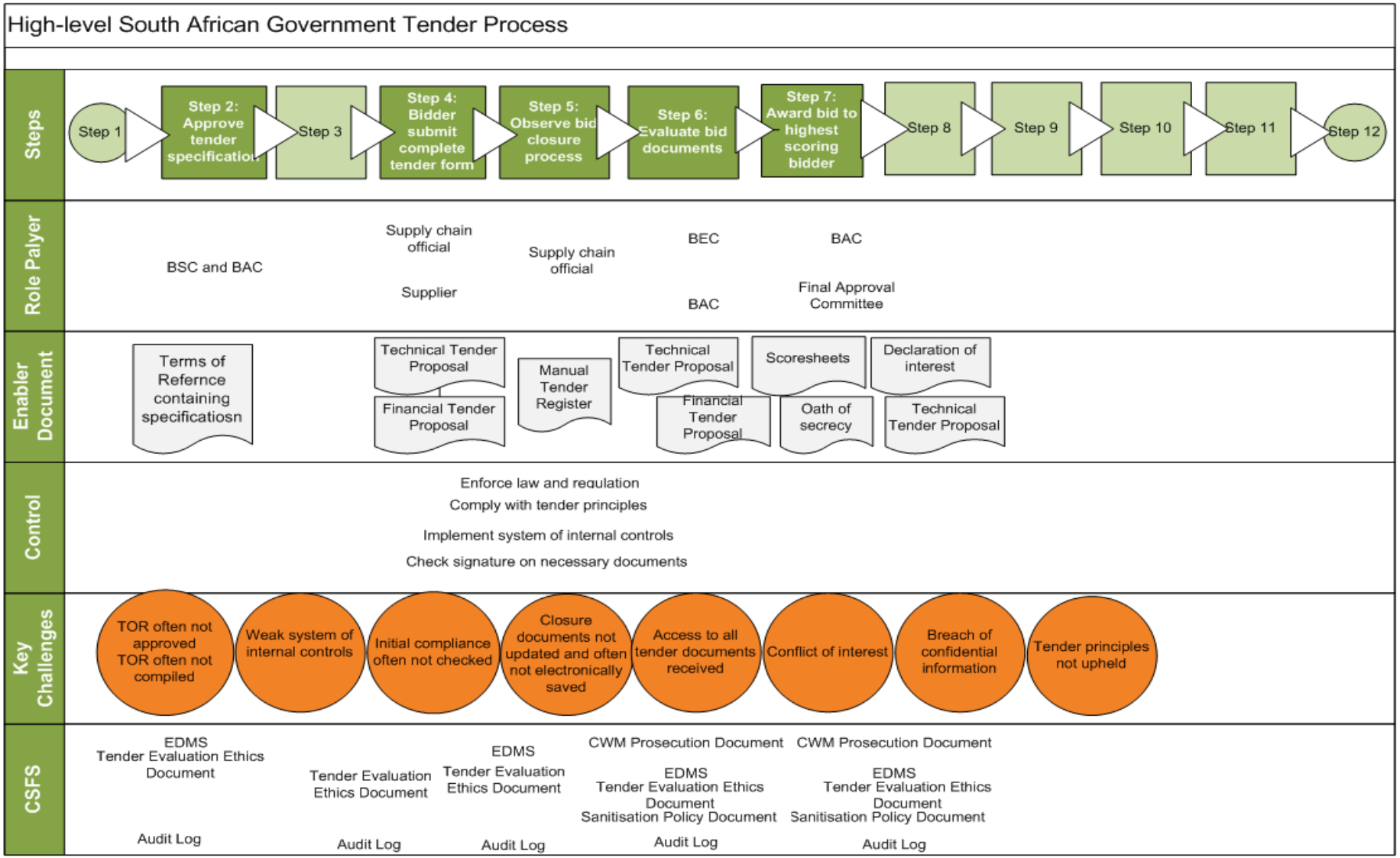


Figure 7.6 Critical success factors aligned to current tender process

Finally the CSFs also address the sub research questions identified in this study and together answer the main research question. See Table 7.3 for the link between the CSFs and the research questions.

Table 7.3 Critical success factors linked to research questions

Critical Success Factor		Research Questions		
Code	Factor Name	**How is information used to corrupt the tender process?**	**What controls are in place to reduce the breach of confidential information?**	**How can the Chinese Wall Model be used to improve information confidentiality?**
CSF01	Sanitisation Policy Document A document that specifies the rule to implement the sanitisation policy effectively.		✔	✔
CSF02	Electronic Document Management System An information system which is integrated with the tender information system to store the necessary documents in a particular format.	✔	✔	✔
CSF03	Tender Evaluation Ethics Document A document which explains the rules for taking part in the tender process. The ethical behaviour is specified and must be complied with.	✔	✔	
CSF04	Audit Log This refers to the audit trail of key decisions made by the users participating in the tender process. This will assist in holding officials accountable for their decisions.	✔	✔	✔
CSF05	CWM Prosecution Register A breach of the Chinese Wall Model will lead to prosecution of the individual. The names of these individuals must be added to a register. This individuals on this list must be prevented from participating in the tender process.	✔	✔	

In the next section, the researcher will evaluate the research conducted in this study. This is reflected in detail in the research methodology chapter. A summary of this evaluation is represented in the following section.

7.6 Research evaluation

When conducting research, it is vital that the researcher remain critical, as there are many pitfalls that might reduce or affect the credibility of the research. Errors can result in incorrect information being communicated. This section will therefore help in concluding this chapter with an evaluation of this research project.

This research project follows the pragmatism approach with focus on interpretivist research. Interpretivist research differs from positivist research; Lincoln and Guba (1985) in (Oates, 2006) highlight a set of criteria for interpretivist research that is an alternative to, but parallel to, those for the positivist approach.

Table 7.4 Quality in positivist and interpretivist research (Lincoln and Guba, 1985, in Oates, 2006:294)

Positivism	Interpretivism
Validity	Trustworthiness
Objectivity	Conformability
Reliability	Dependability
Internal validity	Credibility
External validity	Transferability

Validation of the critical success factors occurred through the use of expert reviews. Twelve experts in the information security and government tender field were presented with the findings of this research study. They were requested to comment on the correctness and applicability of the research problem. This assisted to further refine the artefact being developed. This approach is associated with the Expert Review Process, and therefore follows an iterative process of evaluation and refinement. The Expert Review Process consisted of four rounds of review, analysis and feedback.

The secondary data collected included literature from frameworks, methodologies, online journal articles and other Internet sources, past research projects, case studies, and books. The initial literature review was performed in order to determine the research problem and objectives.

This was most important, as it identified the body of knowledge on which the study has been based and expanded upon. By combining these two data collection methods, and by using them as inputs into a Design Science approach, an innovative artefact was developed. To consolidate this approach, the Design Science Guidelines were complied with. The search for an effective artefact required the utilisation of credible and available means to reach the desired critical success factors. The Design Science research produced a viable artefact.

The research data presented to the experts were continuously and thoroughly refined after each round of review, thereby refining the study of an increasingly credible standard. The way in which the review process was conducted was deemed credible, leading to a perception of trustworthiness. The responses received from the experts can also be said to increase the credibility of this research project they provided comparable data.

The dependability of the responses received from the experts is difficult to measure and heavily dependent on the experts who in the review process, their position and expertise, the situation, expectation and their own perception of the subject. The expert review process was conducted in a non-leading manner using defined research data presented for analysis, with the aim of keeping the process as open as possible.

To ensure and increase the dependability of the literature used in this study, only well-known researchers, authors and institutions have been used in the construction of the theoretical framework.

This study explains the Critical Success Factors (CSFs) pertaining to the tender process and the securing of information in a general sense. They can also be applied to all other government departments where information confidentiality is a problem. Alternatively, these CSFs can be adapted for other organisations such as investment banks who use the Chinese Wall Model to manage conflict of interest. Therefore, transferability can be achieved to some extent.

Since all five constructs of interpretivist research shown in Table 7.4, have been achieved to varying degrees, the soundness of this study is demonstrated. In general, credibility and dependability of this study have been achieved.

7.7 Conclusion

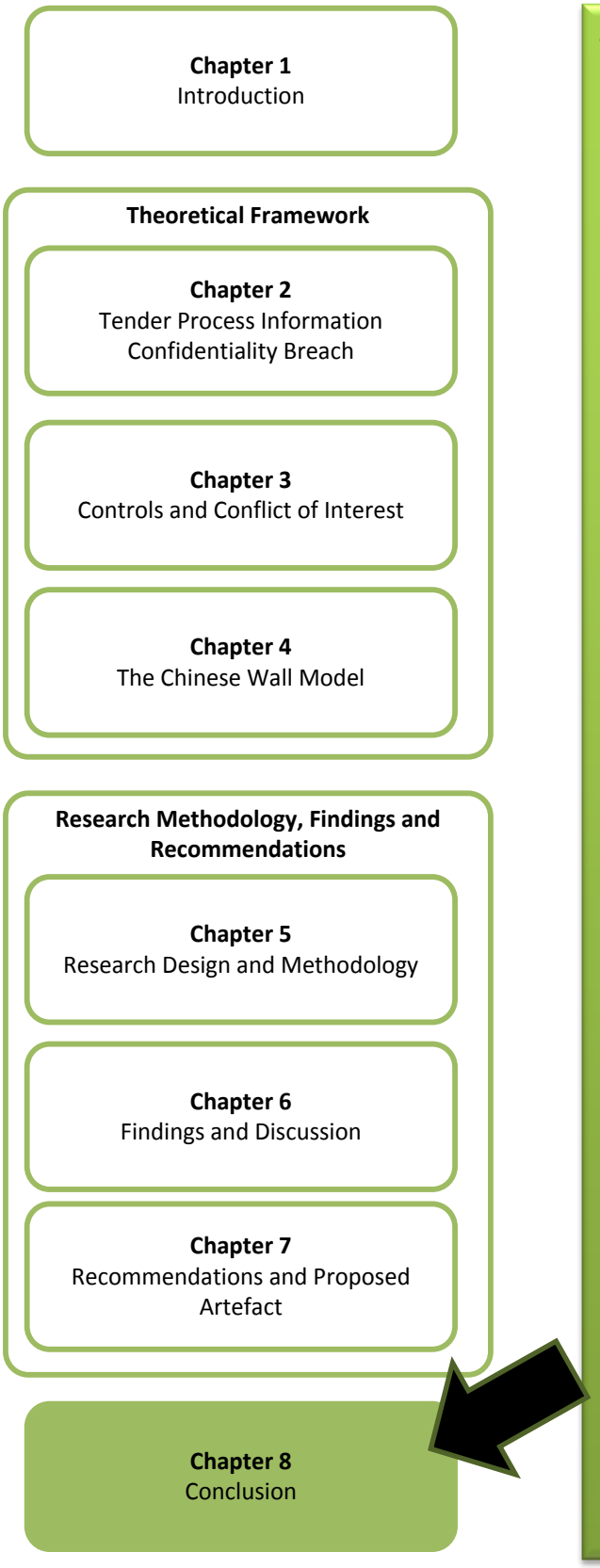
In this chapter, the proposed artefact composition was discussed, highlighting the influences from the primary and secondary data analysis during the research. These influences formed the critical success factors which are the artefact. The recommendations evident from the findings discussed in Chapter six were then presented. The analysis of the literature study and the expert reviews that were collected, and the changes that were made as a result of it, supplied the necessary data to develop critical factors of success model based on the discussed problem areas. The recommendations are in the form of CSFs aimed at reducing the breach of confidential information in the tender process in an effort to reduce conflict of interest.

The chapter began with a reminder and brief explanation of the problem steps in the tender process. The term CSFs is defined. This is followed by the argument for deriving the proposed CSFs. The argument is represented by the premises and conclusion. A number of statements (premises) result in sub-conclusions or success factors. This demonstrates critical thought by the researcher of this study. Together, these success factors constitute the proposed artefact.

The proposed five CSFs are namely: the Sanitisation Policy Document, an Electronic Document Management System, the Tender Evaluation Ethics Document, the Audit Trail Log and the Chinese Wall Model Prosecution Register. These factors form part of the main contribution of this study as represented in the proposed artefact (Table 7.2 The proposed critical success factors addressing the problem area).

These CSFs are then aligned to the problem steps in the tender process. They are then discussed in great detail, justifying their importance for an effective Chinese Wall Model in the dynamic environment of government tenders. The next chapter will provide the conclusion to this research project, summarising all the items discussed and presented throughout the chapters.

CHAPTER 8 : CONCLUSION



Chapter 8

8.1 Introduction

5.7 Background

8.3 The contribution made by this study

8.4 Research questions

8.5 Future research

8.6 Concluding note

"The conclusion chapter rounds off what was started in the introduction chapter".

(Hofstee, 2009)

8.1 Introduction

The purpose and outcome of this research project is summarised in this chapter. The previous chapter discussed the findings and recommendations of the study and provided five critical success factors necessary for the Chinese Wall Model to reduce the breach of confidential information in the government tender process.

This chapter provides a summative conclusion to the study. It will begin by providing a brief background of the study; thereafter, the contribution made by this research will be presented. An evaluation of the research outcomes follows. Then, directions for future research are made and finally some concluding remarks are offered. The next section presents a summary of the preceding chapters in this study.

8.2 Background

In the past few years, research into government tender fraud has gained considerable attention (Kaynak & Hartley, 2008). This fraud is often due to a conflict of interest between departmental officials, potentially leading to significant losses. An important aspect of this research project is the underlying theory. The theory adopted in this study is the Chinese Wall Model. This study emphasises that the Chinese Wall Model is proposed as a solution to reduce the risks associated with information confidentiality breach, by seeking to halt the flow of information to unauthorised persons (Slay & Koronios, 2006).

In Chapter 2, the importance of information in the government tender process is discussed. This chapter explains the most important steps in the tender process in the South African government departments. The essential requirements and tender principles that should be in place are reflected. This is followed by an overview of the information systems used and the challenges associated with the information system in the tender process. Additionally, the chapter explains how information is used to corrupt the tender process.

Chapter 3, examines the different classifications of internal controls. It identifies the current controls used to manage confidential information in the tender process. Then it analysed the South African government legislation which is applicable to reducing conflict of interest. Thereafter, it examines the South African government interventions which are in place to

manage tender fraud. The Common Criteria Security Model (CCSM) is used to evaluate the effectiveness of internal controls in the tender process. Following that is an overview of the ISO/IEC 27002 (2005) standard. Finally, the last section reviewed the different internal controls applied in the tender process in foreign countries across the world, with particular focus on developing countries.

In Chapter 4, the Chinese Wall Model was examined in detail. The basis of the model is that it provides an information barrier designed to reduce the conflict of interest problem in an organisation (Brewer & Nash, 1989). This model has been applied to different scenarios where a conflict of interest may exist (Brewer & Nash, 1989; Slay & Koronios, 2006). The chapter also outlines various information flow models and proposes that the Chinese Wall Model is the most appropriate to the research problem.

In Chapter 5, the research methodology was explained which favours the practical approach of this study and therefore, the pragmatic philosophy was adopted. This study gathered a collection of primary data and inductive reasoning was applied to analyse the data. The research approach is Design Science Guidelines. The Expert Review Process forms the evaluation of this study.

The explanation of the Expert Review Process and the primary data collection followed Chapter 5. The four rounds of expert reviews were presented in Chapter 6. Open-ended questions were posed to the experts to obtain validation and consensus on the main contributions of this study, including the critical success factors. The findings were analysed by using narrative methods.

The resulting critical success factors are explained in Chapter 7. The development of the critical success factors is based on critical thought by following an argumentative approach. The argument is represented by the premises and conclusion. A number of statements (premises) resulted in sub-conclusions or success factors. Together, these success factors constitute the proposed artefact. These critical success factors were then aligned to the problem steps in the tender process. The success factors solve the research problem and achieve the objective of this study. In addition, the critical success factors have an influence on the Chinese Wall Model in the dynamic environment of government tenders. The following section will highlight the contributions made by the research project.

8.3 The contribution made by this study

This section will highlight the research project's contribution to the existing body of knowledge. It was established that tender fraud in South Africa is a serious issue. Unofficially, R30 billion per year is lost to tender fraud (Paton, 2010). This is mainly due to

the existence of conflict of interest within government departments, according to the South Africa's 2011 Budget Speech (Gordhan, 2011). Conflict of interest together with poor management of confidential information in the tender process results in information manipulation (Tomlinson, 2010; Special Investigating Unit, 2011). The Minister of Finance in South Africa emphasises that even though there are government laws and regulations, interventions and procedures to govern the tender process, tender fraud is still a growing issue in the government (Gordhan, 2012 Budget Speech, 2012). Gordan (2012) further adds that it is the responsibility of every citizen to combat tender fraud.

A significant problem that requires attention is that there is no effective information security model to manage the access to confidential information in the government tender process. From this research project, the Chinese Wall Model has been presented to fulfil this requirement. The application of the Chinese Wall Model to manage information confidentiality in the tender process is new. It is known, however, that the Chinese Wall Model is used in investment banks and law firms to reduce the breach of confidential information within an organisation.

The government can utilise the Chinese Wall Model to manage access to confidential information where a conflict of interest may occur thus make contribution to the study. This is done by managing the flow of confidential information. Certain information flow models: Bell and La Padula (1975), Biba (1977) and Clark and Wilson (1987) were investigated to manage the access to information based on a user's security level or role. The Chinese Wall Model, however, goes beyond this control by managing access to confidential information based on who already has authority to access the information according to their authorised security level or role.

The development of the critical success factors can be adapted and applied in other contexts which deploy the Chinese Wall Model. This also forms a contribution to this study. The theoretical and practical implications of this study are that the Critical Success Factors can be applied to the existing tender process without re-inventing the steps in the tender process. However, an identified concern is that a small government tender board or bid committee will have to invite additional government officials to participate in the tender process to accommodate user access to only one dataset in a conflict of interest as proposed by the Chinese Wall Model.

This research project highlighted areas of information confidentiality, which were important to the following respondents:

- Individuals responsible for security in the government.
- Individuals who make decisions based on valid information in the tender system.

- Individuals who conduct research in information security.

The highlighted areas of information confidentiality are derived from the Common Criteria Security Model (CCSM) and the ISO/IEC 27002 (2005) standard which maps the problem steps in the tender process. This provides a detailed starting point from which security users are able to begin implementing security requirements. The results obtained in this study were analysed in the context of the research question which follow.

8.4 Research questions

At the outset, three research questions were provided as stated in Chapter 1. These questions have remained the guiding focus for every step of this project. Topics found not to add value to one of these questions were either removed or refocused. In order to evaluate the success of this research project, an assessment of each of these questions was undertaken. If each of these questions are answered, then the research project has fulfilled its original intentions as these three questions address the problem statement of this study.

The primary research question for this research project was established in Section 1. 4 and is as follows:

How can the application of the Chinese Wall Model reduce the use of information in corrupting the tender process in the South African government?

This question is asked as the primary question for this study. The answer to this question forms the primary output for the research project. In response, critical success factors incorporating the Chinese Wall Model were developed seeking to provide the answer to this question. The artefact allows the government to create a common point of reference to direct the management of confidential information in tenders. It encompasses components from the Chinese Wall Model, the tender controls and ISO/IEC 27002 (2005) standard. By means of the artefact, a solution has been provided which satisfies this question.

To address the main research problem, three secondary questions were established, as noted in Chapter 1. By answering these three secondary questions, their outcomes together address the main research question. These secondary questions are as follows:

The first secondary research question is:

How is information being used to corrupt the government tender process in South Africa?

The secondary data collection revealed how information is used to corrupt the tender process. This section reviewed real world cases to understand where and when a conflict of

interest occurs in the tender process. These cases are specific to South Africa and relate to 2010 and 2011, thus are current cases. It reveals that information is used to corrupt the tender process at specific steps where the role players are members of the bid committees in government.

The findings of the literature reviewed provide ample evidence on how information is used to corrupt the government tender process. As identified in Chapter 2, this is done namely by, and not limited to, inconsistent compliance in the tender process: law and regulation, poor system of internal controls, conflict of interest, easy access to confidential information, unauthorised disclosure of information and poor monitoring of access to tender information (Slay & Koronios, 2006; Special Investigating Unit, 2011; Gordhan, 2012 Budget Speech, 2012). The link between information confidentiality and conflict of interest is explained. Conflict of interest exists among the government officials in the department. If confidential information is not adequately secured, it can be manipulated for personal gain. A reminder is provided in Figure 8.1.

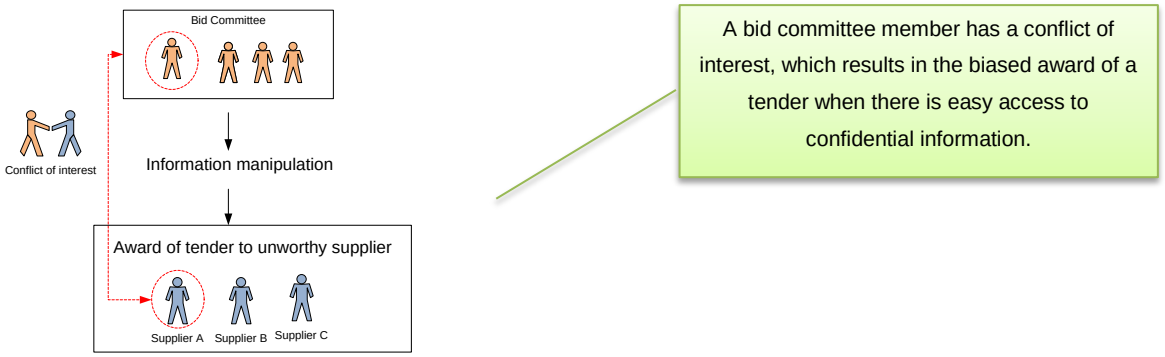


Figure 8.1 Conflict of interest identified

This secondary question has been successfully answered in Chapter 2. Next, the second secondary question is evaluated.

The second secondary research question is:

What controls are in place to reduce the information breach and improve confidentiality in the government tender process?

This question seeks to identify the controls in place to manage information security in the tender process, with particular focus on information confidentiality and conflict of interest. To identify the controls, it was necessary to understand the different categories of controls using GTAG1. Firstly it examines the law and regulation in the South African tender process was examined. Following that is the application of the CCSM model to identify the security criteria in the tender process. The ISO/IEC 27002 (2005) is examined as an information security standard which can be applied and which guides the management of information confidentiality in tenders. Then, is a substantive review and analysis of international

literature published on various tender regulation and controls in developing and developed countries was conducted. Thus, the Chinese Wall Model was presumed to be a preventative control which could be applied to manage confidential information where a conflict of interest existed.

This secondary question has been answered in Chapter 3. The third secondary question will now be evaluated.

The third secondary research question is:

How can the Chinese Wall Model be used to improve information confidentiality in the government tender process?

The Chinese Wall Model has been identified as an information flow model to manage the flow of confidential information within an organisation. It is known that the Chinese Wall Model is applied in organisations where conflict of interest exists. The '*Chinese wall*' is a conceptual wall constructed to prevent the breach of insider information. The idea behind this model is similar to that of a personal firewall in a computerized environment (Slay & Koronios, 2006). The firewall is a security system designed to permit or deny communications based on a given security policy. An individual who fails to adhere to the security policies in an organization, which has implemented the Chinese Wall Model, will be deemed as potentially criminally fraudulent (Mutula & Wamukoya, 2009). Different information flow models were compared and it was established that the Chinese Wall Model was the most appropriate to the tender process. Hence, it was applied to the tender process as demonstrated in Figure 8.2.

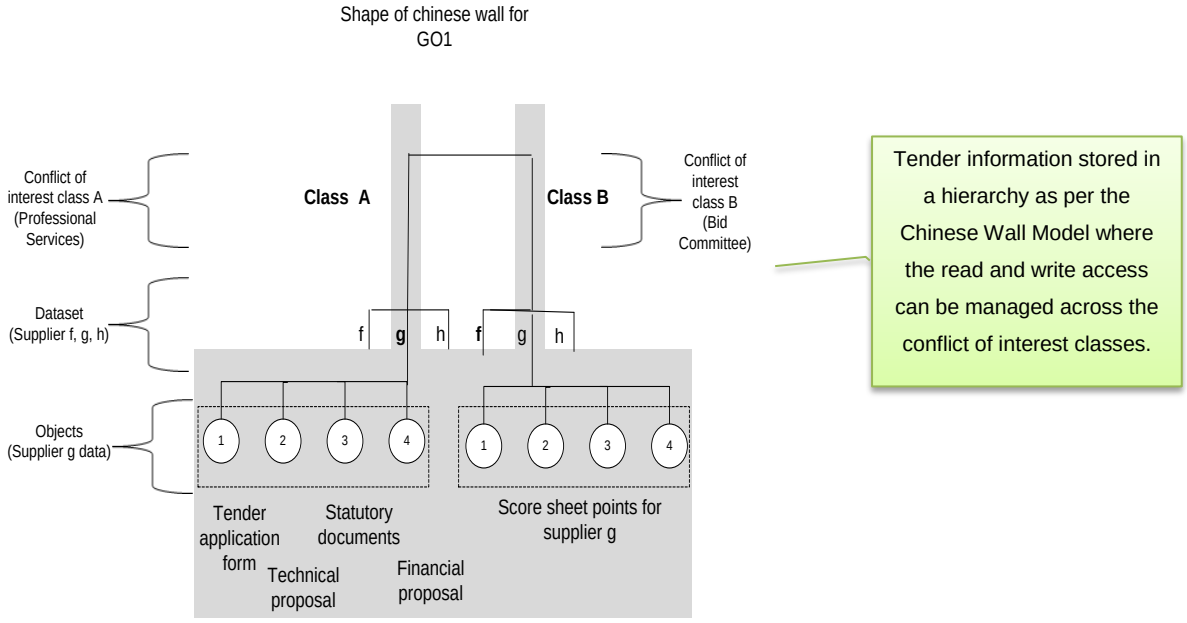


Figure 8.2 Chinese Wall Model applied in tender process

Managing information confidentiality is essential to reduce tender fraud (Mutula & Wamukoya, 2009) and upholding tender principles. These tender principles and the recourse for the tender anomalies associated with the cases can further be explained with respect to the Chinese Wall Model.

This secondary question has been fruitfully answered in Chapter 4. Each of the questions set out at the onset of this research have therefore been adequately addressed by the research project.

Based on the information provided in the preceding chapters, which will be synthesised in this chapter, the main research question has successfully been addressed by investigating the sub-research questions (Chapter 1, section 1.4).

Table 8.1 provides information on the chapters in which the different research questions were addressed and the sections in which the different outputs were provided.

Table 8.1 Chapter in which the relevant research questions were addressed

Question number	Research question	Addressed in:	Output in section:	
Main research question	*How can the application of the Chinese Wall Model reduce the use of information in corrupting the tender process in the South African government?*	Chapter 2,3,4,7	Sections 2.5, 2.7, 2.8,3.3, 3.4, 3.7, 4.4, 4.5, 7.3, 7.4, 7.5	
Sub-research question 1	*How is information used to corrupt the government tender process in South Africa?*	Chapter 2	Section 2.5: Section 2.7: Section 2.8:	Information systems and its challenges in the tender process. Real world government tender cases. Conflict of interest in tender process summarised.
Sub-research question 2	*What controls are in place to reduce the information breach and improve confidentiality in the government tender process?*	Chapter 3	Section 3.3: Section 3.4: Section 3.7:	Government Regulation and the tender process. Government interventions. Corruption and controls in other countries.
Sub-research question 3	*How can the Chinese Wall Model be used to improve information confidentiality in the government tender process?*	Chapter 4	Section 4.4: Section 4.5: Section 7.3: Section 7.4: Section 7.5:	Information flow models. Application of the Chinese Wall Model. The development of the critical success factors. The proposed critical success factors explained. The critical success factors and the problem areas.

Having concluded this section, a few recommendations are made for further research. This is explained in the next section.

8.5 Future research

The purpose of this section is to encourage future research within this field of study. The proposed future research is related to the problem statement and is as follows:

- This study provided a conceptual view of the application of the Chinese Wall Model to the tender process together with the five Critical Success Factors. It would be

worthwhile physically testing this model in the government tender process to determine its true strength or weakness.

- These CSFs incorporating the Chinese Wall Model can be applied to the tender process in private organisations in order to learn from the private context. This future research can then be applied again to the government organisation thus learning from the government and vice versa.

The future research proposed here, would make a useful contribution to the existing body of knowledge if it is undertaken. The next section offers concluding remarks.

8.6 Concluding note

The point of undertaking this study is to gain increased knowledge about information confidentiality and government tender process and also to develop the proposed artefact.

This research project identified a problem in the South African government tender process; the breach of confidential information in tenders and as a consequence tender fraud which is often headline news in the press. The researcher of this research project has published a paper concerning the application of the Chinese Wall Model to the South African government tender process. (See Appendix G).

The Chinese Wall Model together with the five Critical Success Factors can be applied to reduce the breach of confidential information and further adds a solution to managing the conflict of interest. The researcher has written another paper concerning the five proposed Critical Success Factors for effective implementation of the Chinese Wall Model in the South African government tender process. (This paper is currently under review).

This research project concludes by proposing a solution to the growing problem of information confidentiality breach in the tender process, a problem that has existed for many years.

Finally, through the work of this research project, the body of knowledge, interested government officials and information security researchers will definitely benefit from this study. This study's solution can be embraced as an exciting approach to improving access control to confidential information in government tenders.

Reference

Andrade, A. D. (2009). Interpretive research aiming at theory building: adopting and adapting the case study design. *The Qualitative Report, 14*(1), 42-60.

Aritua, B., Smith, N., & Bower, D. (2011). What risks are common to or amplified in programmes: Evidence from UK public sector infrastructure schemes. *International Journal of Project Management, 29*(1), 303 - 312.

Australian Government. (2011, September 06). *Guidance on Ethics and Probity in Government Procurement - FMG 14*. Retrieved September 22, 2012, from The Department of Finance and Deregulation Archive: http://www.ag.gov.au/cca

Barham, C. (2010). Confidentiality and security of information. *Informatics*, pp.502-504.

Bell, D., & La Padula, L. (1975). *Secure computer system: Unified exposition and multics interpretation.* Retrieved 03 30, 2012, from Mitre Corporaion, Bedford, MA: URL: http://csrc.nist.gov/publications/history/bell76.pdf

Bertino, E. (2010, February 02). *Purdue University.* Retrieved June 16, 2011, from Access Control Models Part II: http://www.slidefinder.net/a/access_control/models_part/132197

Bhattacharya, U., & Marshall, C. (2012). Do they do it for the money? *Journal of Corporate Finance, 18*(1), 92 - 104.

Biba, K. J. (1977). Integrity consideration for secure computer system. USA: Election System Division, Bedford, MA.

Brewer, F., & Nash, M. (1989). The chinese wall security policy. *IEEE sysmposium on Security and Privacy* (pp. 206–214). Los Alamitos, CA: IEEE.

Britain Russia India China South Africa. (2013). *Summit to finalise BRICS bank structure*. Retrieved 07 07, 2013, from Fifth BRICS Summit: http://www.brics5.co.za/

Business Dictionary. (2012). *Critical Success Factors*. Retrieved 12 18, 2012, from BusinessDictionary: http://www.businessdictionary.com/definition/critical-success-factors-CSF.html#ixzz2Dh3KFHOu

Byun, J., Sohn, Y., & Bertino, E. (2006). Systematic Control and Management of Data Integrity. *ACM*, pp.101-110.

Carlsson, S., Keller, C., Henningsson, S., & Hrastinski, S. (2011). Socio-technical IS design research: developing design theory for IS integration management. *Information Systems and e-business Management, 9*(1), 109 - 131.

Cerrillo-i-Martínez, A. (2011). The regulation of diffusion of public sector information via electronic means: Lessons from the Spanish regulation. *Government Information Quarterly, 28*, pp. 188–199.

Chen, K., Shing, M., Lee, H., & Shing, C. (2007). Modeling in confidentiality and integrity for supply chains. *Communications of the IIMA, 7*(1), 41 - 49.

Clark, D., & Wilson, P. R. (1987). A comparison of commercial and military computer secuiry policies. *IEEE Symposium on Research and Privacy* (pp. 184 – 194). Oakland, CA: IEEE.

Collins, K. M., Onwuegbuzie, A. J., & Johnson, R. B. (2012). Securing a Place at the Table: A Review and Extension of Legitimation Criteria for the Conduct of Mixed Research. *American Behavioral Scientist, 56*(6), 849 - 865.

Common Criteria Security Model. (2009, July). *Common Criteria Part1: Introduction and general model.* Retrieved July 08, 2011, from The Common Criteria Security Model: http://www.commoncriteriaportal.org/products/

CorruptionWatch. (2012). *Who-we-are-and-what-we-do*. Retrieved 09 01, 2012, from CorruptionWatch: http://www.corruptionwatch.org.za/content/who-we-are-and-what-we-do

Coull, S., Green, M., & Hohenberger, S. (2011). Access Controls for Oblivious and Anonymous Systems. *ACM Transactions on Information and System Security, 14*(1), 10 - 28.

Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed method approaches* (2nd ed.). London: SAGE Publications.

Creswell, J. W., & Tashakkori, A. (2007). Developing Publishable Mixed Methods Manuscripts. *Journal of Mixed Methods Research, 1*(2), 107-111.

Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers and Security, 29*(1), 196 - 207.

Department of Communications. (2010). *Minister of communications of budget vote speech.* Department of communications.

Department of Human Settlements. (2009). *Supply Chain Management Policy Framework and Procedure Manual.* Department of Human Settlements, South Africa.

Department of Public Service and Administration. (2002). *Public service anti-corruption strategy.* 2002: Department of Public Service and Administration.

Department of Public Services and Administration. (2011). Batho Pele Principles. Pretoria, Gauteng, South Africa.

Eastern Cape Provincial Treasury. (2008). *Provincial Suppliers Database Utilisation Policy.* Bhisho: Provincial Treasury.

Falagario, M., Sciancalepore , F., Costantino, N., & Pietroforte, R. (2012). Using a DEA-cross efficiency approach in public procurement tenders. *European Journal of Operational Research, 218*(1), 523 - 529.

Feilzer, M. Y. (2010). Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm. *Journal of Mixed Methods Research, 4*(1), 6 - 16.

Flowerday, S.; von Solms, R. (2007). What constitiutes Information Integrity? *South African Journal of Information Management, Vol. 9*(4), pp. 1 - 4.

George, Z. (2011, 12 09). Officials grab contracts. East London: Daily Dispatch.

Gong, T. (2010). Auditing, accountability, and corruption in China: prospects and problems. *Journal of Public Administration, 2*(1), 69 - 84.

Gordhan, P. (2011). 2011 Budget Speech. *2011 Budget Speech* (pp. 1 - 25). Johannesburg, South Africa: National Treasury.

Gordhan, P. (2012). 2012 Budget Speech. *2012 Budget Speech* (pp. 1 - 34). Pretoria, South Africa: National Treasury.

Gray, J. W. (2012, 02 12). *How To Distinguish Premises from Conclusions Using Argument Maps*. Retrieved 12 12, 2012, from Ethical Realism: http://ethicalrealism.wordpress.com/2012/02/24/distinguishing-between-premises-and-conclusions-using-argument-maps/

GTAG1. (2012). *Global Technology Audit Guide, Information Technology Risk and Controls.* Altamonte Springs, Fla., USA: The Institute of Internal Auditors.

Hellriegel et al. (2007). *Management Second South African edition.* Cape Town: Oxford University Press Southern Africa (Pty) Ltd.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems research. *MIS Quarterly, 28*(1), 75-105.

HM Treasury. (2008). *The green book: appraisal and evaluation in central government.* Office of Government Commerce. TSO.

HM Treasury. (2009). *Management of risk.* Office of Government Commerce: TSO.

Hofstee, E. (2009). *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule.* Johannesburg, South Africa: EPE.

Hookway, C. (2008, August 16). *Pragmatism.* Retrieved August 23, 2011, from Stanford Enclclopedia of Philosophy (Spring 2010 Edition): http://plato.stanford.edu/archives/spr2010/entries/pragmatism/

Hui, H. (2009). Chinese wall system in large finance and market institutions - Experience and lessons of the Anglo-American legal system. *Law China, Vol. 4*(No. 4), pp. 489–506.

Huntley, V. (2010). *Data Security In A Real-Time World Requires 'Defense In Depth' Strategy.* Malvern: National Underwriter Property & Casualty Risk & Benefits Management.

IBM. (2008). *Supply chain risk management: A delicate balancing act.* Retrieved 06 13, 2011, from IBM: http://www.ibm.com/common/ssi/sa/wh/n/gbw03015usen/GBW03015USEN.PDF

ISO/IEC 27002. (2005). *ISO/IEC 27002: 2005 Information technology - Security techniques - Code of practice for information security management.* Retrieved July 19, 2011, from International Organization for Standards: http://www.iso2700isecurity.com/html/27002.html

Kaisara, G., & Pather, S. (2011). The e-Government evaluation challenge: A South African Batho- Pele service quality approach. *Government Information Quarterly, 1*(1), 1-11.

Karhunen, P., & Ledyaeva, S. (2012). Corruption Distance, Anti-corruption Laws and International Ownership Strategies in Russia. *Journal of International Management, 18*(1), 196 -208.

Kaynak, H., & Hartley, J. (2008). A replication and extension of quality management into the supply chain. *Journal of Operations Management, 26*(1), 468-489.

Khuarana, R., & Mandke, V. V. (2009). Business process modeling with information integrity. *Business Process Management, 15*(4), 487-503.

Knappa, K., Morris, R., Marshallc, T., & Byrdc, T. (2009). Information security policy: An organizational-level process model. *Computers and Security, 28*(1), 493 -508.

Ko, R., Lee, S., & Lee, E. (2009). Business process management (BPM) standards: a survey. *Business Process Management Journal, 15*(5), 744-791.

Lambert, D., Knemeyer, A., & Gardner, J. (2011). Supply Chain Partnerships : Model validation and implementation. *Journal of Business Logistics, 25*(2), 21 42.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Newbury Park: SAGE Publications.

Liu, J., & Lin, B. (2012). Government auditing and corruption control: Evidence from China's provincial panel data. *China Journal of Accounting Research, 1*(1), 1 - 24.

Lo, A., & Wong, R. (2011). An empirical study of voluntary transfer pricing disclosures in China. *J. Account. Public Policy, 30*(1), 607 - 628.

Lopez, D., & Gary, F. (2010). Internal control reporting differences among public and governmental auditors: The case of city and county Circular A-133 audits. *J.Account. Public Policy, 29*(1), 481 - 502.

Lorentziadis, P. (2010). Post objective determination of weights of the evaluation factors in public procurement tenders. *European Journal of Operational Research, 200*(1), pp. 261 -267.

Louw, A. (2012). *SCMO Workshop: Procurement Planning (T2) & Bid Processing (T4).* East London: Province of Eastern Cape Provincial Treasury.

Luyt, R. (2012). A Framework for Mixing Methods in Quantitative Measurement Development, Validation, and Revision : A Case Study. *Journal of Mixed Methods Research, 6*(4), pp. 294 - 316.

Ma, J., & Ma, C. (2011). Factor Analysis Based On The COSO Framework And The Goverment Audit Performance Of Control Theory. *Procedia Engineering, 15*(1), 5584 - 5589.

Madnick, S., Lee, Y., & Zhu, H. (2009). Overview and Framework for Data and Information Quality Research. *ACM Journal of Data and Information Quality,, 1*(1), 1 - 21.

Marsh, S. (2012). Trust and Security = Links, relationships and family feuds. *ISSA 2012.* Johannesburg, South Africa: IEEE.

Mateus, R., Ferreira, J., & Carreira, J. (2010). Full disclosure of tender evaluation models : Background and applicationin Portuguese public procurement. *Journal of Purchasing & Supply Management, 16*(1), 206 – 215.

Morgan, D. (2007). Paradigms lost and pragmatism regained : Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research, 1*(1), 48 - 76.

Morgan, G., & Smircich, L. (1980). The case for qualitative research. *Academy of Management Review, 5*(4), 491-500.

Mutula, S., & Wamukoya, J. (2009). Public sector information management in east and southern Africa: Implications for FOI, democracy and integrity in government. *International Journal of Information Management, 29*(1), 333–341.

Myers, M. D., & Klein, H. K. (2011). A Set of Principles for Conducting Critical Research in Information Systems. *MIS Quarterly, 35*(1), 17-36.

Niehaves, B. (2007). On epistemological diversity in design science - new vistas for a design-orientated IS research. *European Research Center for Information Systems* (pp. 1 - 13). Montreal: Twenty Eighth International Conference on Information Systems.

NIST. (2010, 08 03). *New NIST Report Advises: Securing Critical Computer Systems Begins at the Beginning.* USA Government.

Oates, B. J. (2006). *Researching Information Systems and Computing.* London: SAGE Publications.

Osborn, S. (2012). Is it Privacy or is it access control. *ISSA 2012.* Johannesburg, South Africa: IEEE.

Pardo, C., Pino, F., Garcia, F., Piattini, M., & Baldassarre, M. (2011). An ontology for the harmonization of multiple standards and models. *Computer Standards & Interfaces, 1*(1), 1 - 12.

Paton, C. (2010, June 2). *Corruption in government procurement, how are they doing it?* Retrieved April 02, 2011, from SmartProcurement: http://www.smartprocurement.co.za/archives/corruption_in_government_procurement_how_are_they_doing_it.php

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for Information Systems Research. *Journal of Management of Information Systems, 24*(3), 45-78.

Pereira, J. (2009). The new supply chain's frontier: Information management. *International Journal of Information Management, 29*(1), 372 - 379.

Rainbolt, G. W., & Dwyer, S. L. (2012). *Critical Thinking: the art of argument.* Boston, MA, USA: Wadsworth Cengage Learning.

Rama, S., Flowerday, S., & Boucher, D. (2012, Aug 15-17). Information confidentiality and the Chinese Wall Model in Government tender fraud. Presented at Information Security South Africa. Johannesburg, South Africa, doi: 10.1109/ISSA.2012.6320438: Published by IEEE Xplore.

Republic of South Africa. (2000a). *Preferential Procurement Policy Framework Act, No.5 of 2000.* Cape Town: RSA Government Gazette.

Republic of South Africa. (1996). *Special Investigating Units and Special Tribunals Act No. 74 of 1996.* South Africa: Government Gazette.

Republic of South Africa. (1996). *The Constitution of South Africa.* South Africa: Government Gazette.

Republic of South Africa. (1999). *Public Finance Management Act, No.1 of 1999.* Cape Town: RSA Government Gazette.

Republic of South Africa. (2000). *Promotion of Access to Information Act, No. 2 of 2000.* Cape Town: RSA Government Gazette.

Republic of South Africa. (2000b). *The Promotion of Administrative Justice Act (No. 3 of 2000).* Cape Town: Government Gazette.

Republic of South Africa. (2003a). *Municipal Finance Management Act (No. 56 of 2003).* Cape Town: Government Gazette.

Republic of South Africa. (2003b). *National Treasury Supply Chain Management Regulations.* Pretoria: RSA Government Gazette.

Republic of South Africa. (2003c). *Broad-Based Blacak Economic Empowernment (Act No 53 of 2003).* Cape Town: Government Gazette.

Republic of South Africa. (2004). *Prevention and Combating of Corrupt Activities Act, No. 12 of 2004.* Cape Town: RSA Government Gazette.

Republic of South Africa. (2011). *PPPFA : Regulation in terms of GNR 502.* Pretoria: RSA Government Gazette.

Resnik, D. (2010). *What is ethics in research and why is it important?* Retrieved August 24, 2011, from National Institute of Environmental Health Sciences: http://www.niehs.nih.gov/research/resources/bioethics/whatis.cfm

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). England: Prentice Hall.

Slay, J., & Koronios, A. (2006). *Information Technology Security and risk management.* Milton Qld: John Wiley & Sons Australia Ltd.

Special Investigating Unit. (2011). *Annual Report 2010/2011.* Pretoria: SIU.

TechTarget Corporation. (2011). *Chinese Wall*. Retrieved August 02, 2011, from TechTarget Corporation: http://www.whatis.com/chinesewall

Teddlie, C., & Tashakkori, A. (2009). Foundations of mixed methods research. *Thousand Oaks, CA:SAGE Publications*.

Tenderscan. (2012). *Tendering in South Africa*. Retrieved September 11, 2012, from Tender Topics: http://tendertopics.tenderscan.co.za/?page_id=227

The Institute of Internal Auditors. (2012, September 09). *COSO Releases New ERM Framework*. Retrieved September 09, 2012, from The Institute of Internal Auditors: http://www.theiia.org/guidance/additional-resources/coso-related-resources/coso-releases-new-erm-framework/

The World Bank. (2011). *Accountability in Public Services in South Africa.* Washington, DC: The World Bank.

Tomlinson, M. (2010). Managing the risk in housing delivery: Local government in South Africa. *Habitat International, 1*(1).

van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security, 29*(1), 476-486.

van Rijswijck, E. (2011, 11 09). *South Africa's justice system goes hi-tech*. Retrieved 09 15, 2012, from MediaClubSouthAfrica: http://www.mediaclubsouthafrica.com/index.php?option=com_content&view=article&id=2653:justice-091111&catid=44:developmentnews&Itemid=111

Wagner, S. M., & Bode, C. (2007). An empirical investigation into supply chain vulnerability. *Journal of Purchasing & Supply Management, 12*(1), 301–312.

Wang, S., & Wang, H. (2010). Towards innovative design research in information systems. *Journal of Computer Information Systems, 1*(1), 11 - 19.

Acronyms

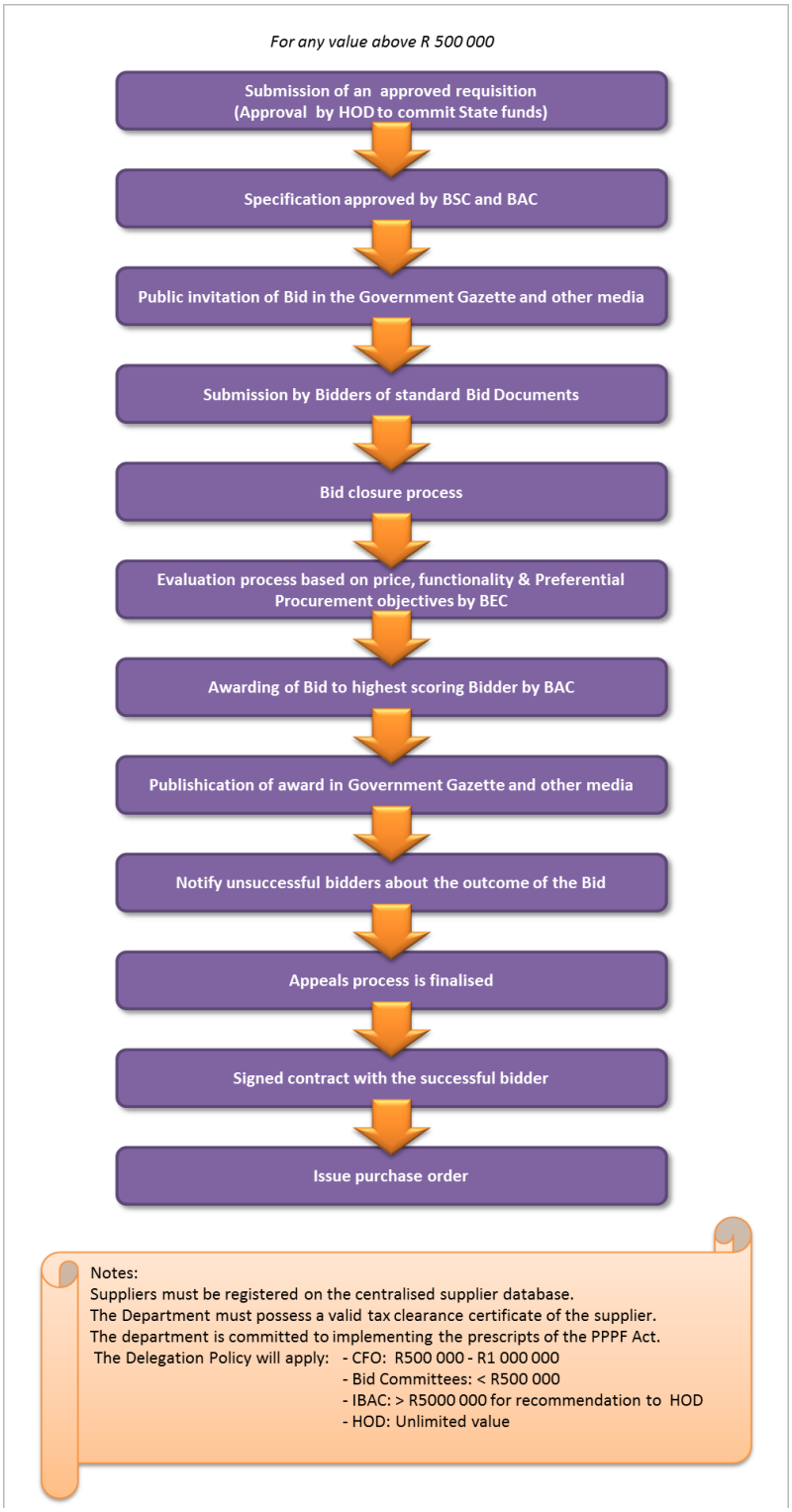
BAC	:	Bid Adjudication Committee
B-BBEE	:	Broad-Based Black Economic Empowerment Act (2003)
BEC	:	Bid Evaluation Committee
BEE	:	Black Economic Empowernment
BRICS	:	Brazil, Russia, India, China, South Africa
BSC	:	Bid Specification Committee
CCSM	:	Common Criteria Security Model
CFO	:	Chief Financial Officer
COSO	:	Committee of Sponsoring Organisations
CSD	:	Centralised Supplier Database
CSFs	:	Critical Success Factors
DPW	:	Department of Public Works
EDMS	:	Electronic Database Management System
EU	:	European Union
HDI	:	Historically Disadvantaged Individual
IBAC	:	Interim Bid Adjudication Committee
MAWG	:	Multi-Agency Working Group
OECD	:	Organisation for Economic Co-operations and Development
PFMA	:	Public Finance Management Act, (Act 1 of 1999)
PPPFA	:	Preferential Procurement Policy Act, (Act 5 of 2000)
SCM	:	Supply Chain Management
SCMPFM	:	Supply Chain Management Procedure Manual Framework
SIU	:	Special Investigating Unit

Glossary

Bid Adjudication Committee	A group of government officials responsible for checking the evaluation of tender/proposal documents and recommending the award of a tender to a supplier.
Bid Evaluation Committee	A group of government officials responsible for evaluating tender/proposal documents received from the suppliers for a tender.
Bid Specification Committee	A group of government officials responsible for compiling the specifications for a tender.
BRICS	It is the title of an association of emerging national economies: Brazil, Russia, India, China and South Africa.
Chinese Wall Model	The Chinese Wall Model is an access control model used to limit user access to confidential information where a conflict of interest exists within an organisation.
Conflict of interest	It is when a government official has personal interest in the award of a tender which negatively impacts the tender information.
Supply Chain	A unit within the government department which manages the acquisition of goods and services required by the government.
Tender Process	It is the process whereby governments invite bids for goods or services required by the government that must be submitted within a finite deadline.

Appendix A : South African Government Tender Process

The following diagram shows the process for procurement of goods or services which is above R500 000.



Appendix B : Supply Chain Categories

The table below summarises the different categories of supply chain risk (IBM, 2008)

Category	Examples
Operational/ Technological	Forecast errors, component/material shortages, capacity constraints, quality problems, machine failure/downtime, software failure, imperfect yields, efficiency, process/product changes, property losses (due to theft, accidents, etc.), transportation risks (delays, damage from handling/transportation, re-routing, etc.), storage risks (incomplete customer order, insufficient holding space, etc.), budget overrun, emergence of a disruptive technology, contract terms (minimum and maximum limit on orders), communication/IT disruptions
Social	Labor shortages, loss of key personnel, strikes, accidents, absenteeism, human errors, organizational errors, union/labor relations, negative media coverage (reputation risk), perceived quality, coincidence of problems with holidays, fraud, sabotage, pillage, acts of terrorism, malfeasance, decreased labor productivity
Natural/Hazard	Fire, wild fire, severe thunderstorm, flood, monsoon, blizzard, ice storm, drought, heat wave, tornado, hurricane, typhoon, earthquake, tsunami, epidemic, famine, avalanche
Economy/ Competition	Interest rate fluctuation, exchange rate fluctuation, commodity price fluctuation, price and incentive wars, bankruptcy of partners, stock market collapse, global economic recession
Legal/Political	Liabilities, law suits, governmental incentives/restrictions, new regulations, lobbying from customer groups, instability overseas, confiscations abroad, war, tax structures, customs risks (inspection delay, missing data on documentation)

Appendix C : GTAG 1 IT Control Framework Checklist

ACTIONS	QUESTIONS
1. Identify the IT control environment of the organisation, including: a. Values. b. Philosophy. c. Management style. d. IT awareness. e. Organization. f. Policies. g. Standards.	• **Do corporate policies and standards that describe the need for IT controls exist?**
2. Identify relevant legislation and regulation impacting IT control, such as: a. Governance. b. Reporting. c. Data protection. d. Compliance.	• **What legislation exists that impacts the need for IT controls?** • **Has management taken steps to ensure compliance with this legislation?**
3 . Identify the roles and responsibilities for IT control in relation to: a. Board of directors. i. Audit committee. ii. Risk committee. iii. Governance committee. iv. Finance committee. b. Management. i. CEO. ii. CFO and controller. iii. CIO iv. Chief Security Officer (CSO). v. CISO. vi. CRO. c. Audit. i. Internal audit. ii. External audit.	• **Have all relevant responsibilities for IT controls been allocated to individual roles?** • **Is the allocation of responsibilities compatible with the need to apply division of duties?** • **Are IT responsibilities documented?** • **Are IT control responsibilities communicated to the whole organization?** • **Do individuals clearly understand their responsibilities in relation to IT controls?** • **What evidence is there of individuals exercising their responsibilities?** • **Doesan internal audit employ sufficient IT audit specialists to address the IT control issues?**
4. Identify the risk assessment process. Does it address: a. Risk appetite?	• **How are the organisation's risk appetite and tolerance determined?** • **Are the organization's risk appetite and tolerance authorized at board level?**

ACTIONS	QUESTIONS
b. Risk tolerance? c. Risk analysis? d. Matching risks to IT controls?	• **Are the terms risk appetite and tolerance clearly understood by all those with a responsibility for IT control?** • **Does the organization use a formal risk analysis process?** • **Is the process understood by everyone responsible for IT control?** • **Is the process used consistently throughout the organization**
5. Identify all monitoring processes, including: a. Regulatory. b. Normal in-house. c. Other than internal auditing.	• **What processes exist to monitor compliance with all relevant legislation and internal policies and standards?** • **Does management carry out monitoring processes outside an internal audit?**
6. Identify information and communication mechanisms, such as: a. Control information. b. Control failures.	• **What metrics are provided to the Board, its committees, and management in relation to IT security?** • **What additional reports are provided regularly to the Board and management?** • **Is management always provided with reports when IT control failures occur?** • **Do the Board and its committees receive similar reports of IT control failures?**

Appendix D : Letter Requesting Access to Department

University of Fort Hare
DEPARTMENT OF INFORMATION SYSTEMS
East London Campus:
P.O. Box 7426, East London, 5200, South Africa
50 Church Street, East London, 5201, South Africa
Tel: +27 (0) 43 704 - 7073 Fax: +27 (0) 43 704 - 7070
Email: Infosys@ufh.ac.za

University of Fort Hare
Together in Excellence

13 July 2011

Chief Financial Officer and Head of Department
Department of Human Settlements (aka Housing)
31-33 Phillip Frame Road
Steve Tshwete House
Chiselhurst
East London

Dear [redacted]

RE: RESEARCH FOR MASTERS DEGREE – ALLOWING ACCESS TO DEPARTMENT DOCUMENTS AND STAFF

I am currently a student at the University of Fort Hare, and studying towards a research-based Masters Degree in Information Systems. The area of research under consideration is the public sector supply chain. For the purpose of research collection and validation access by the Department is required.

The research will specifically reference various legislations, policies and procedures/processes with regard to the tender process in the public sector supply chain. The request is therefore for access to the Department to conduct primary research such as interviews, and secondary research, such as the review of procedure manuals. The outline for the research masters will be detailed in the research proposal that will be presented to the Higher Degrees and Research Committee at the University. Once this proposal is accepted by the committee, it will be forwarded to your attention for review. It will spell out the requirements of the research.

Research at the University requires the adherence to a code of Ethics for conducting research, and respondents will be protected by confidence when/if required. Individuals can opt to remain anonymous when making responses and if so, will be protected by replacing their details with an alphabetic character. The Department could either be named, or recorded in a similar manner, e.g. Department A in the Eastern Cape.

The projected end date for the Masters is at the end of 2012. My contact details are as follows: 079 536 4383 or Sobhana_rama@yahoo.co.in. Please sign the attached access form stating that you have given me access to your Department.

Your assistance with respect to access for research purposes is greatly appreciated.

Your sincerely,

Sobhana Rama

School of Business Enterprise
Faculty of Management and Commerce: Tel: 043 704 7196

together in excellence

www.ufh.ac.za

Appendix E : Approval Letter Granting Access to Department

Province of the
EASTERN CAPE
HUMAN SETTLEMENTS

OFFICE OF THE [redacted]
[redacted] • REPUBLIC OF SOUTH AFRICA
Enquiries [redacted]
Fax: [redacted] www.[redacted].gov.za

Date: 16 August 2011

University of Fort Hare
Department of Information Systems
P.O. Box 7426
East London
5201

Dear Sobhana Rama

RESEARCH FOR MASTERS DEGREE – ALLOWING ACCESS TO DEPARTMENT DOCUMENTS AND STAFF

We are in receipt of your letter dated 13 July 2011 regarding research based on legislation, policies and procurement/processes in the public sector supply chain.

The department does not foresee a problem in the research being done but wishes to inform you that on some occasions there will be confidential documents which cannot be disclosed to you and this will be at the discretion of the Director in Supply Chain Management Unit.

The Department also prefers not to be mentioned.

We wish you good luck with your venture.

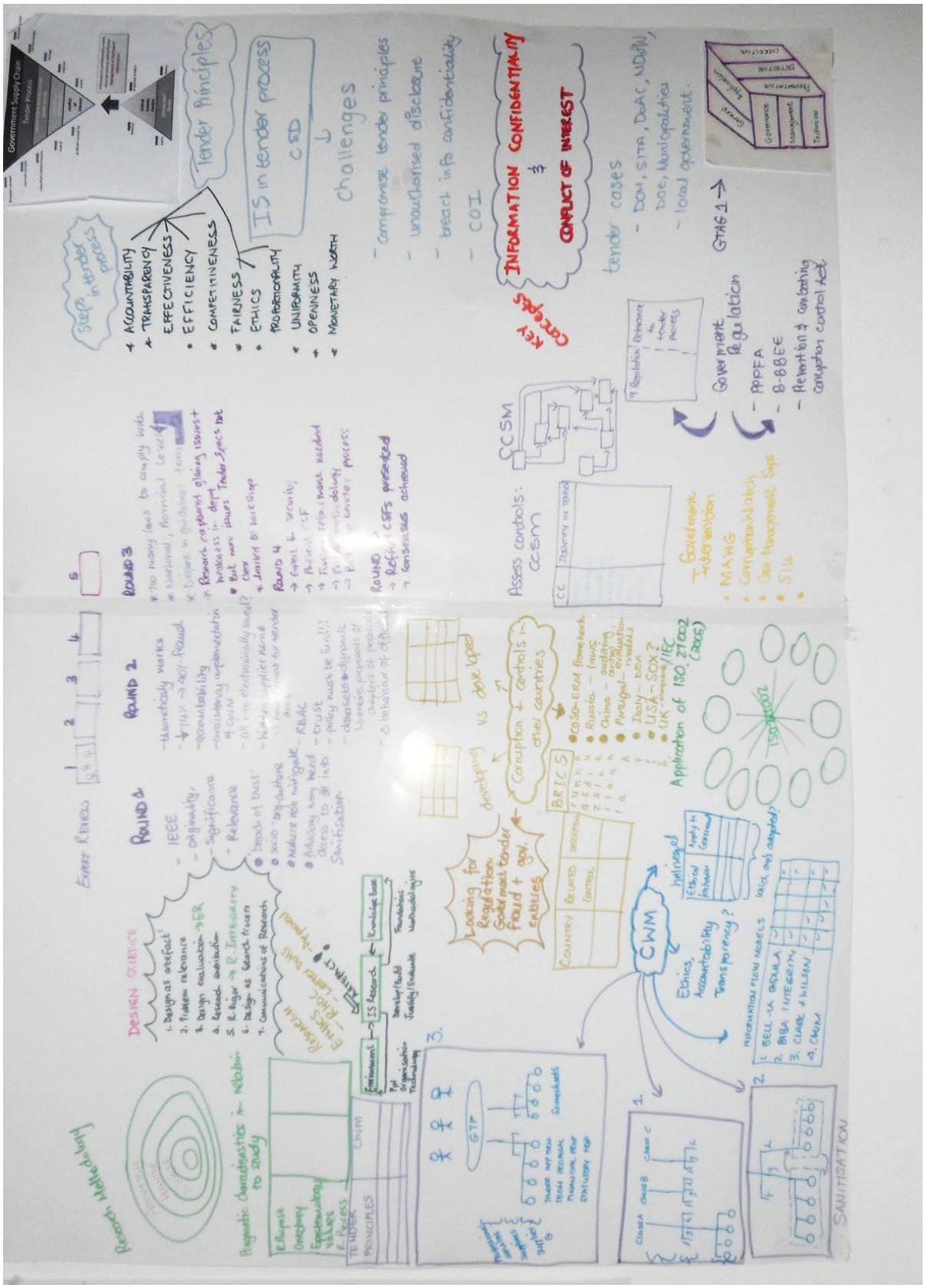
Thank you

[redacted]
Date: 19.08.2011

Cc: Director SCM

Research SCM Page 1

Appendix F : My Critical Thought Mind Map



Appendix G : My Published Paper

ABSTRACT

Instances of fraudulent acts are often headline news in the popular press in South Africa. Increasingly these press reports point to the government tender process as being the main enabler used by the perpetrators committing the fraud. The cause of the tender fraud problem is a confidentiality breach of information. This is accomplished, in part, by compromising the tender information contained in the government information system. This results in the biased award of a tender. Typically the information in the tender process should be used to make decisions about a tender's specifications, solicitation, evaluation and adjudication. The sharing of said information to unauthorised persons can be used to manipulate and corrupt the process. The reliance on uncompromised information during the tender process, points to the need to ensure that information confidentiality is present. A lack of information confidentiality can occur when a government official involved in the tender process derives personal gain by knowingly possessing a conflict of interest. This in turn corrupts the tender process by awarding a tender to an unworthy recipient. This paper addresses the conflict of interest which can arise between government officials and external stakeholders in the government tender process. It suggests that conflict of interest together with a lack of information confidentiality in the information system paves the way for possible corruption. Thereafter, information flow models, and the Chinese Wall Model are discussed as a means of mitigating instances where conflict of interest can occur. The Chinese Wall Model is applied to three existing case studies associated with corruption to determine its viability in the conflict of interest problem within the tender process. Finally, an adapted Chinese Wall Model, which includes elements of the tender process, is presented as a conceptual view of how the Chinese Wall Model can mitigate fraud in the government tender process.

INDEX TERMS

- **IEEE Terms**
  Adaptation models , Companies , Context , Government , Information systems , Investments , Security
- **INSPEC**
  - **Controlled Indexing**
    government data processing , security of data
  - **Non Controlled Indexing**
    Chinese wall model , South Africa , external stakeholders , government information system , government officials , government tender fraud , information breach , information confidentiality
- **Author Keywords**
  Chinese Wall Model , Government tender fraud , conflict of interest , information confidentilaity

Additional Details

Topic(s) : Communication, Networking & Broadcasting ; Components, Circuits, Devices & Systems ; Computing & Processing (Hardware/Software)
Conference Location : Johannesburg, Gauteng
Print ISBN: 978-1-4673-2160-0
INSPEC Accession Number: 13038615
Digital Object Identifier : 10.1109/ISSA.2012.6320438
Date of Current Version : 04 October 2012
Issue Date : 15-17 Aug. 2012

Sign In | Create Account

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» Access Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» US & Canada: +1 800 678 4333
» Worldwide: +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact | Help | Terms of Use | Nondiscrimination Policy | Site Map | Privacy & Opting Out of Cookies

A non-profit organization, IEEE is the world's largest professional association for the advancement of technology.
© Copyright 2013 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.