Information Confidentiality and the Chinese Wall Model in Government Tender Fraud

Sobhana Rama
Department of Information Systems
University of Fort Hare
East London, South Africa
sobhana_rama@yahoo.co.in

Stephen V Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

Duane Boucher
Department of Information Systems
University of Fort Hare
East London, South Africa
dboucher@ufh.ac.za

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.

Keywords: Chinese Wall Model; information confidentilaity; conflict of interest; Government tender fraud

I. INTRODUCTION

In the past few years, research into Government tender fraud has gained considerable attention [1]. This is often due to a conflict of interest between departmental officials, potentially leading to significant losses.

Paton states that in South Africa "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" [2]. The root cause of these losses is a conflict of interest in the tender process, which results in inflated costs associated with tenders and tender fulfillment by unsuitable service providers [2]. Paton cites Hofmeyr, the head of the Special Investigating Unit (SIU) that there has been an increase in state supply chain corruption [2], even though corruption has been highlighted as something to be reduced in the tender process.

Gordhan [3], in the 2011 South African Budget Speech stated that the "government tender process plays a significant part in the economy and is central to Government service delivery". Gordhan adds that citizens and taxpayers do not receive full value for money, because the tender process is vulnerable to waste and corruption [3]. This results in a biased award of a tender which in turn leads to corruption in the tender process [4].

Corruption is defined 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 contract execution" [5]. When said corrupt activities occur, confidential information in the information system is not safeguarded from unauthorised individuals, and can be used to negatively influence decisions in the tender process. To protect confidential information in the tender process, the Government must have appropriate security policies in place to mitigate instances of corruption associated with fraud [6][7].

The Chinese Wall Model is proposed as a solution to mitigate the risks associated with information security loss, by seeking to halt the flow of information to unauthorised persons [8]. The basis of the model is that it provides an information barrier designed to mitigate the conflict of interest problem in the organisation [8]. This model has been applied to different scenarios where a conflict of interest may exist [8][9]. A conceptual wall is constructed to prevent the leak of insider information. The idea behind this model is similar to that of a personal firewall in a computerized environment [8]. The firewall is a security system designed to permit or deny communications based on a given security policy [8]. The personal firewall is not holistic, but selective in the information

978-1-4673-2159-4/12/$31.00 ©2012 IEEE

it protects. Similarly, the Chinese Wall Model is designed to limit the spread of confidential information to unauthorized persons in a given circumstance [8]. In one circumstance an individual may have a conflict of interest, but in another, may not.

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 [29]. In some countries, legal charges such as insider trading can be enforced [9].

The objective of this paper is to analyse and compare the application of the Chinese Wall Model in existing situations (e.g. Investment Banking) to the tender process thereby seeking to manage information confidentiality and reduce an instance of conflict of interest in the tender process.

To achieve the stated objective of this paper the government tender process will be explained, as well as how a lack of information confidentiality and conflict of interest may occur. Thereafter, the paper introduces the Chinese Wall Model and applies it to the tender process through the use of various cases. This in turn leads to the formulation of a graphical representation and discussion of the Chinese Wall Model in the tender process, thereby achieving the objective of this paper.

II. GOVERNMENT TENDER PROCESS

A. Nature of government spending

The term Government is used in this study to refer to agencies, institutions and organisations under state control that are recognised to serve the needs of the general public. Government usually covers the core civil service, state and quasi-public or state corporations [10]. The Government is the largest organisation in South Africa and spends billions of Rand on infrastructure projects related to buildings, port works, roads, technology and waterworks. Government departments outsource their required work and services to service providers through various methods such as competitive bidding through: Request for Quotation (RFQ) or Request for Proposal (RFP) and Agreement Through Negotiation. Of these, competitive bidding through RFP is the most frequently used method in South Africa for tenders above R500 000 [5]. However, irrespective of the method used there is still the need to follow a set procedure in order to ensure that the process is transparent, so that instances of conflict of interest can be avoided.

B. Steps in 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 applied by the South African Government Departments [11][12][13]. There are twelve steps in the entire tender process. These steps are reflected at a high-level and are generic across the departments in South Africa.

Step 1 - complete a requisition form for the project/tender and ensure it is approved by the accounting officer of the Department.

Step 2 - compile the specification and the application form for the tender and have it approved by the Bid Specification Committee (BSC) and Bid Adjudication Committee (BAC). These specifications include, but are not limited to, invitation to bid, tax clearance certificate, pricing specifications, technical specifications, and special conditions.

Step 3 - advertise the tender in the Government Gazette and other media. A tender briefing session may be held with prospective suppliers/bidders. Tender documentation must be issued to interested bidders.

Step 4 - bidders must submit completed tender documents and application forms to the Department.

Step 5 - observe the tender closure process. The receipt of bids/proposals from suppliers will close at a specified date and time as indicated in the tender document.

Step 6 - the bids are evaluated on price, functionality and preferential procurement objectives. The Bid Evaluation Committee (BEC) will evaluate the bids in terms of the criteria stipulated in the bid documents. The scoring as per the preference point system for each bid document must be completed. The completeness of documents is checked in terms of a SARS tax clearance certificate, company registration, legitimate signatures and necessary required security. A report with the recommendations from the BEC will be submitted to the BAC for approval.

Step 7 - award the bid to the bidder with the highest score. Bids above the departmental delegation are forwarded to the Interim Bid Adjudication Committee (IBAC) at Provincial Treasury for approval.

Step 8 - publish the award of the recommended bid.

Step 9 - notify unsuccessful bidders of the outcome.

Step 10 - finalise any appeals for the tender.

Step 11 - sign the contract with the successful bidder. The supply chain management (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 the purchase order to the successful bidder/supplier.

When following the twelve steps in the tender process there are a number of principles that play an integral part in ensuring that instances of fraud arising from a conflict of interest could be mitigated.

C. Tender principles

Within the South African government context tenders should be aligned with the relevant Batho Pele principles [14][15][16] and the Preferential Procurement Policy Framework Act, 2000 [12]. A limited combination of these tender principles have been adapted and are listed in no particular order of importance with a brief description of each principle.

- *Transparency* - implies that the procurement process must be open and must afford prospective bidders timely access to the same and accurate information.
- *Efficiency* – seeks to ensure standards are met by simplifying procedures.

- *Competitiveness* – requires the satisfaction of the need for competitiveness in bidding during the tender process.
- *Fairness* – requires non-discrimination and fairness when dealing with any bidder.
- *Ethics* – necessitates that all stakeholders conduct business and themselves professionally, fairly, reasonably and with integrity. Personal interests should be disclosed while the breach of information confidentiality and security requirements should also be reported.
- *Uniformity* – that tender procedures, policies, control measures, and contract documentation are uniform, simple and adaptable to advances in modern technology.
- *Accountability* - the accounting officer and management are accountable for their decisions and actions relative to their procurement responsibilities.
- *Openness* - ensures that the procurement process is in line with best practices.
- *Monetary worth* - requires money to be spent in conjunction with cost and quality measures, in order to maximize efficiency, effectiveness and flexibility.

These principles are mentioned because their presence is considered to be an important contributing factor to the reduction of a lack of confidentiality, and an attempt to avoid a conflict of interest among tender officials. However, to appreciate their relevance it is necessary to briefly explain the information security concepts of confidentiality and conflict of interest.

III. INFORMATION SECURITY CONCEPTS

A. Confidentiality

Confidentiality assures that access is confined to those who have authority [17]. The information system used in the tender process has to ensure that information is not made available to any official other those involved in the process. Information available to those who should not have access, is an information security breach [18][19]. A loss of confidential information is at times, considered to be present in the tender process [2][7] [14][16].

This leads to information manipulation and biased decisions are made on the award of a tender [8] [16]. This is fraud that results from a breach of information confidentiality by a government official.

B. Conflict of interest

A *conflict of interest* within a government context is defined as a public servant acting or failing to act on a matter in which they have an interest or where another person or entity that stands in a relationship with them, has a vested interest [5]. Public servants or departmental officials who do not disclose any business, commercial, and financial interest undertaken for financial gain contribute to corruption of the tender process. Conflict of interest negatively impacts the fiduciary responsibilities of the government official. The official is negligent and does not feel accountable for their actions. Furthermore, departmental officials who place themselves under any financial obligation to individuals or organisations that influence them in the performance of their duties will also aid corruption of the tender process [20][21].

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 [22]. 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. 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 [22]. Otherwise the conflict of interest should be declared, although this is not always done.

The Auditor General of South Africa reports that three quarters of Government tenders in the Eastern Cape are awarded to companies owned by government officials and their families [23]. The ANC legislator, Zolile Mrara, stated that a disturbing 74% of tenders were secured by government officials who are conducting business with government [23]. It is clear that the 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 [23]. This raises concerns as to whether the tender principles highlighted in the previous section actually exist and are used to manage the security of information.

The next section identifies various information security models, which ultimately leads to the identification of the Chinese Wall Model. The Chinese Wall Model will address the confidentiality breach arising through a conflict of interest in the tender process.

IV. INFORMATION SECURITY MODELS

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, and in the following section it will be discussed in the context of tenders.

A. Information flow models

An information flow model explains how subjects (*users*) should interact with objects (*associated with data*) in a system [10]. Information should flow between subjects and objects so that there is no conflict with any existent security policy requirements [10]. For example, information cannot flow vertically between a high security level of top secret, to a lower security level of secret. 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 [24]. This model requires subjects to have access to systems that manipulate objects (*associated with data*) rather than direct access to data themselves [24].

On the other hand, the Biba Integrity Model prevents possible data corruption by limiting information flow among objects [25]. This model groups data into levels of integrity rather than confidentiality [8]. A subject cannot read data at a lower integrity level or read and modify data at a higher integrity level [25].

The Bell-LaPadula Model focuses on information confidentiality and controlled access to classified information [26]. This model separates subjects and data according to secret or top secret levels of confidentiality. Subjects need to have authorization to have access to information corresponding to each level. This prevents information flow from higher security levels to lower security levels and vice versa [26].

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 to be discussed next addresses the static nature of the three information models explained, by allowing for a dynamic handling of datasets by the subject.

B. An overview of the Chinese Wall Model

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 [9]. 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 [9]. 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 [9].

C. 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.

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 [24]. With the Bell-LaPadula model the subject does not have 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 [26]. Whereas with the Chinese Wall Model, the subject may choose a dataset they wish to access [9]. However, once that choice has been made, the user is restrained from accessing another dataset within the same conflict of interest class. The information system would create a "wall" separating the subject from any further interaction with any datasets within that conflict of interest class.

TABLE I. 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 I provides a matrix comparison of the key properties of the three information flow models and the Chinese Wall Model, which have been discussed above. 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 can perpetuate 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 this becomes problematic. The investment banking and government tender process 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.

V. 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 [27]. Unauthorised disclosure of this information could influence the advice given to clients who make investments, allowing staff (subjects) to take advantage of facts not yet known to the general public.

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 the technology (***Class A***) and financial service sector (***Class B***), which is represented in Figure 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.

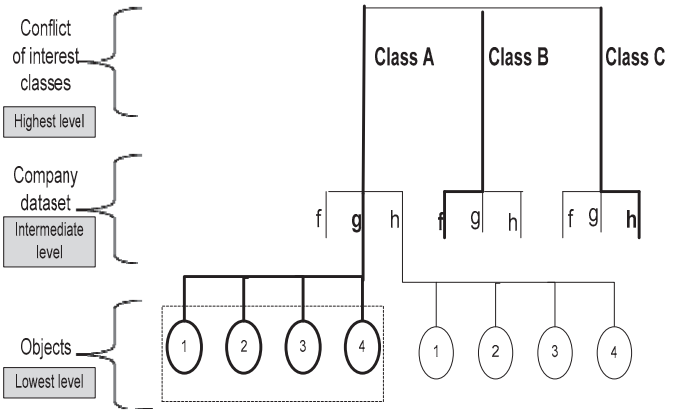

Figure 1: The Chinese Wall Model [9] (adapted)

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 [9].

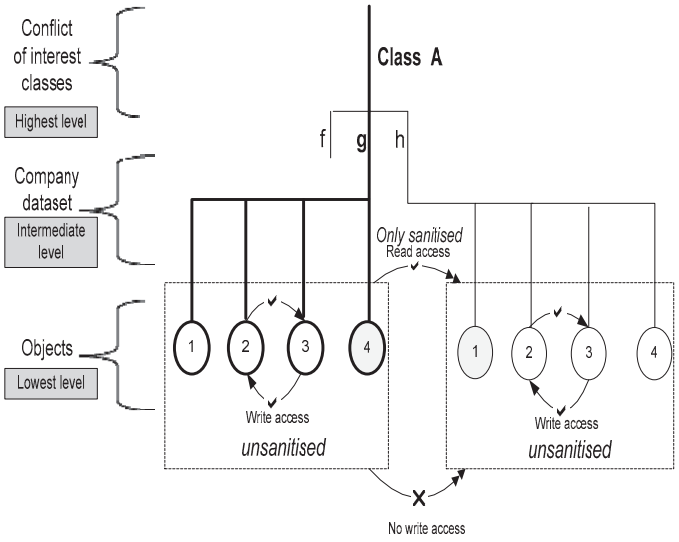

Figure 2: Sanitised and unsanitised information [9] (adapted)

The subject might in some instances need to access datasets in the same class in order 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 [9]. The model refers to this as ***sanitisation***.

Sanitisation can be used as a protection mechanism against the abuse and access to information. Figure 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 [9].

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 mitigates 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 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.

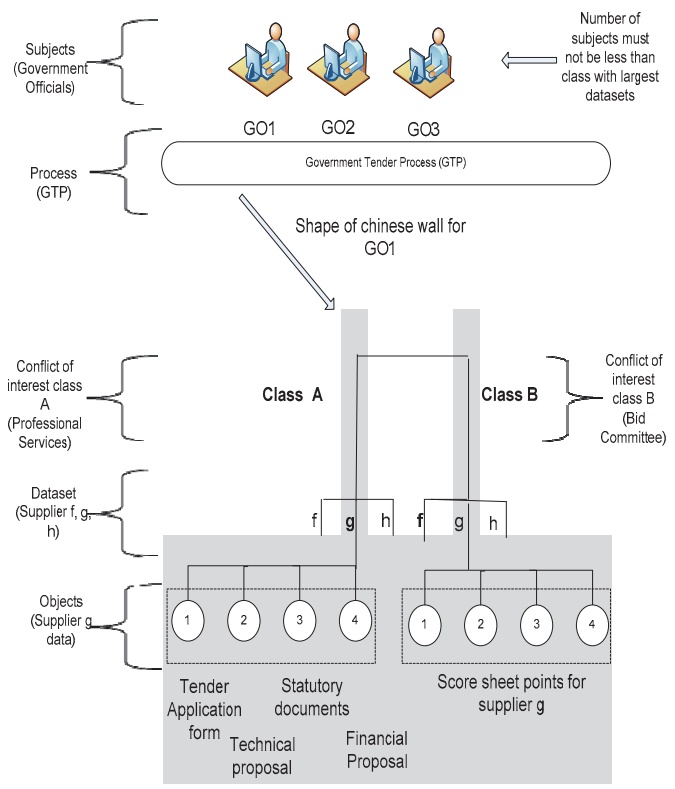

Figure 3: Chinese wall applied in tender process [9] (adapted)

Service provider 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 the particular dataset. By denying GO1 access to the other service providers' datasets, mitigates the conflict of interest GO1 may have across the different service providers.

Service providers are awarded a tender based on preferred methodology and then highest points scored [11]. GO1 does not have access to the other service providers' data, and therefore cannot compare datasets across the other two service providers. GO1 will potentially resist the urge to manipulate the points scored for the service provider g, as GO1 will not be able 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 have the number of officials available as 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 [3]. Also the number of datasets varies for every tender process. The model will be ineffective if this rule is compromised.

C. Real world government tender cases

This section will review three real world cases to understand where and when a conflict of interest occurs in the tender process. The Chinese Wall Model is then applied to these cases.

1) State Information Technology Agency (SITA)

This case refers to allegations against a former senior manager in the Limpopo Province of South Africa relating to procurement irregularities. It is alleged that the former official concluded contracts on behalf of SITA without following the required procurement processes [28]. Tender document completion was not checked. Information access control and non-compliance to the process allowed for a biased award of a tender. Steps five, six and seven were compromised in the tender process.

2) National Department of Housing (NDoHS)

Based on interviews held with Departmental officials, there was a great deal of political interference in the appointment of project managers and suppliers [21]. This case is specific to the delivery of houses to the poor by the South African Government. The local officials were responsible for developing a demand database, managing housing lists, accepting applications for housing subsidies and carry 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 suppliers approved on the Housing Subsidy System and approve suppliers that would normally be rejected by the system. This system was audited by the Auditor General, and it was proven that the system was overridden in order to bypass the national verification process [21]. Steps six and seven were compromised.

3) National Department of Public Works (NDPW)

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 DPW officials and contractors, non-disclosure of outside interests and irregular payments [28]. Step two was exposed to corruption as the specification for the goods/services required from the supplier was not clear and this resulted in an inflation of the bill of quantities. Steps six and seven were exposed to corruption as there were influences on the decisions taken at the bid committees on the recommendation of suppliers / contractors for the emergency tender.

Table II: 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.
Openness and transparency	If a supply chain official has the 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 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 and fairness	The model prevents an official write access to data within the same class 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 currently done

Based on these case studies, it can be 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 the compromised steps such as five, six and seven mentioned in above case studies. 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 all the 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 given individual unless sanitisation of company information is in place.

Managing information confidentiality is essential in reducing tender fraud [29] and upholding the tender principles. These tender principles and recourse for the tender anomalies associated with the cases can further be explained with respect to the Chinese Wall Model (Table II).

VI. CONCLUSION

Confidential information in the government tender process is often not secure, exposing it to possible fraud. Fraud in the sense of a conflict of interest a government official has with a particular supplier, may result in an award of tender to an unworthy supplier. The problem this paper addresses is mitigating 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 tender principles mentioned in this paper. While a limitation of the model has been identified, the initial conflict of interest problem has been solved, and the objective of the paper achieved.

REFERENCES

[1] H. Kaynak and J. Hartley, "A replication and extension of quality management into the supply chain," Journal of Operations Management, vol. 26, pp.468-489, 2008.

[2] C. Paton, "Corruption in government procurement, how are they doing it?," SmartProcurement, April 2011.

[3] P. Gordhan, "Budget Speech", National Treasury, Pretoria, pp. 1 – 25, February 2011.

[4] A. Da Veiga and J.H.P. Eloff, "A framework and assessment instrument for information security culture," Computers and Security, vol. 29, pp. 196 – 207, 2010.

[5] Department of Human Settlements, "Supply Chain Management Policy Framework and Procedure Manual", East London, 2012.

[6] Republic of South Africa, "Prevention and Combating of Corrupt Activities Act, No. 12 of 2004," Cape Town: RSA Government Gazette, 2004.

[7] A. Cerrillo-i-Martínez, "The regulation of diffusion of public sector information via electronic means: Lessons from the Spanish regulation," Government Information Quarterly, vol. 1, no. 28, pp. 188–199, 2011.

[8] J. Slay and A. Koronios, "Information Technology Security and risk management," Milton Qld: John Wiley and Sons Australia Ltd, 2006.

[9] F.C. Brewer and M.J. Nash, "The chinese wall security policy," IEEE sysmposium on Security and Privacy, IEEE, Los Alamitos, CA, pp. 206–214, 1989.

[10] S. E. Coull, M. Green and S. Hohenberger, "Access Controls for Oblivious and Anonymous Systems," ACM Transactions on Information and System Security, vol. 14, no. 1, 2011.

[11] Republic of South Africa, "National Treasury Supply Chain Management Regulations," Pretoria, RSA Government Gazette, 2003.

[12] Republic of South Africa, "Preferential Procurement Policy Framework Act No.5 of 2000," Cape Town, RSA Government Gazette, 2000.

[13] Republic of South Africa, "Public Finance Management Act, No.1 of 1999", Cape Town, RSA Government Gazette, 1999.

[14] G. Kaisara and S. Pather, (2011). The e-Government evaluation challenge: A South African Batho- Pele service quality approach. Government Information Quarterly, vol. 1, no. 1, pp. 1-11.

[15] Department of Public Services and Administration (DPSA). "Batho Pele Principles," Pretoria, Gauteng, South Africa, 2011.

[16] P. Gordhan, "Budget Speech 2012/13", National Treasury, pp. 1 – 34, Pretoria, South Africa, March 2012.

[17] C. Barham, "Confidentiality and security of information", Informatics, Journal of Anaesthesia and Intensive Care Medicine, vol. 11, no. 12, pp. 502-504, 2010.

[18] ISO/IEC 27002, " Information technology - Security techniques - Code of practice for information security management", Standards South Africa, 2005.

[19] S. Flowerday and R. von Solms, "What constitiutes Information Integrity?" South African Journal of Information Management, vol. 9, no.4, pp. 1 – 4, 2007.

[20] V. Huntley, "Data Security In A Real-Time World Requires 'Defense In Depth' Strategy," Malvern: National Underwriter Property and Casualty Risk & Benefits Management, 2010.

[21] M. Tomlinson, "Managing the risk in housing delivery: Local government in South Africa". Habitat International, pp 1-7, 2010.

[22] D. Hellriegel et al., “Management second south african edition”, Oxford Univeristy Press, Southern Africa, 2006.

[23] Z. George, “Officials grab contracts”, Daily Dispatch, 2011.

[24] DR. Clark and PR. Wilson, “A comparison of commercial and military computer secuiry policies”, IEEE Symposium on Research and Privacy, Oakland, CA, pp. 184 – 194, 1987.

[25] KJ. Biba, “ Integrity consideration for secure computer system,” USA, Election System Division, Bedford, MA, 1977.

[26] DE. Bell and LJ. La Padula, “Secure computer system: Unified exposition and multics interpretation,” Mitre Corporaion, Bedford, MA, 1975. URL: http://csrc.nist.gov/publications/history/bell76.pdf.

[27] TechTarget Corporation “Chinese Wall,” [Online]. http://www.whatis.com/chinesewall, August 2011.

[28] Special Investigating Unit, “Annual Report 2010/2011”, Pretoria, 2011

[29] S. Mutula and J. Wamukoya “Public sector information management in east and southern Africa: Implications for FOI, democracy and integrity in government,” International Journal of Information Management, vol. 29, pp. 333–341, 2009.