Factors Affecting Implementation of Enterprise Applications Integration (EAI) with Special Reference to Corruption and Fraud in DOD

by
Mmabore S. H. Phalama

A Thesis Submitted in Partial Fulfilment of the Requirement for the Degree of
Master of Philosophy (Information and Knowledge Management)
At the University of Stellenbosch

Supervisor: Mr Daniel F Botha
Faculty of Arts and Social Sciences
Department of Information Science

March 2012

Declaration

By submitting this thesis/dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

March 2012

Abstract

Corporate mergers and partnerships are common in today's competitive environment and inevitably require organisations to integrate information and telecommunication systems when such unisons take place. One of the most important challenges in each enterprise, especially forced by global markets and the resulting competition, is the capability to efficiently interact, collaborate and exchange information with business partners and within an organisation. Many software systems within organisations are not integrated into a homogeneous structure and therefore the sharing and exchange of information, not being synchronised, leads to possible misappropriation of such information. These isolated systems in organisations, could consequently become possible platforms for corruption and fraud, leading to increase in computer crime. While key risk areas remain, new dangers are emerging. Government stakeholders require departments to be accountable and responsible, which underpins the sharing and exchanging of relevant information, which in turn necessitates the integration of inter- as well as intra-departmental systems. If corruption and fraud is committed in these departments the impact may be significant, including damage to their reputation and image and even detrimental to service delivery to communities.

Government and law enforcement agencies all over the world are faced with challenges of combating corruption and fraud. Fighting corruption and fraud committed via computers necessitates the need to close the gaps created by computers which were designed without consideration for future integration. Hence organisations should seek a way to link systems that were developed in isolation in order to simplify and automate business processes to the greatest extent possible. The aim of this study is to discuss factors affecting the implementation of application systems in large organisations with special reference to the South African Department of Defence (SA DOD). Current systems will be studied and a possible approach on how the DOD Vehicle Management Systems could be integrated will be recommended. This study introduces and defines the problem, describes different research methodologies including the methodology that was used. The topics of corruption and fraud, electronic commerce and e-government will be explored through intensive research of the extant literature, drawing interpretations to be applied to the empirical data gathered on fraud and corruption in DOD and on their ITC systems. Finally the findings and recommendations of this research, based on the theoretical and empirical data, will be presented.

Opsomming

Korporatiewe oornames en vennootskappe is algemeen in vandag se kompeterende omgewing. Dit is dus onvermydelik dat daar van ondernemings verwag word om informasie en telekommunikasie stelsels te integreer by die paasvind van sulke verbintenisse. Een van die mees belangrike uitdagings in elke onderneming, veral in die lig van globale markte met die gevolglike kompeterende uitdagings, is die vermoë vir effektiewe interaksie, samewerking en uitruil van inligting met besigheidsvennote en ook in die onderneming self. Talle sagteware stelsels in ondernemings is nie geïntegreer in ’n homogene struktuur nie en gevolglik, omdat dit nie gesinkroniseer is nie, lei die deel en uitruil van informasie tot moontlike wederregtelike toe-eiening van sulke informasie. Sulke geïsoleerde stelsels in ondernemings kan dus die platvorms word van korrupsie en bedrog en lei tot ’n verhoging van rekenaarmisdywe. Terwyl sleutel risiko areas steeds van toepassing is, is daar ook weer nuwe gevare wat te voorskyn kom. Die Staat se aandeelhouers vereis dat departemente aanspreeklik en verantwoordelik sal wees wat die belangrikheid van die deel en uitruil van inligting onderstreep en wat op sy beurt weer die integrasie van inter- asook intra-departementele stelsels noodsaak. As misdaad en korrupsie gepleeg word in hierdie departemente mag die impak betekenisvol wees. Dit sluit in skade aan hul reputasie en beeld en kan selfs dienslewering aan gemeenskappe belemmer.

Om korrupsie en bedrog wat met rekenaars gepleeg word te beveg, is dit nodig om die gapings toe te maak wat deur ontwerpe geskep is sonder dat toekomstige integrasie inaggeneem is. Ondernenings moet dus ‘n manier soek om stelsels te koppel wat in isolasie ontwikkel was met die doel om besigheidsprosesse tot die grootste moontlike mate te vereenvoudig en te outomatiseer. Die doel van hierdie studie is om die faktore te ondersoek wat die implementering van stelsels beïnvloed in groot ondernemings met spesifieke verwysing na die Suid Afrikaanse Departement van Verdediging (SA DVV). Huidige sisteme sal bestudeer word en ’n moontlike benadering sal aanbeveel word oor hoe die DVV se Voertuig Bestuurstelsels geintegreer kan word. In hierdie studie word die besiheids- asook die navorsings-probleem gedefineer. Die onderwerpe van korrupsie en bedrog, elektroniese handel en e-regering sal ondersoek word deur intensiewe navorsing van bestaande literatuur te doen. Dit word aangevul deur vertolkings van die hierdie toepaslike literatuur gepaard met empiriese data versameling oor bedrog en korrupsie in die DVV en die Departement se “ITK” stelsels. As finale stap sal die bevindings en aanbevelings van hierdie navorsing, gebasseer op teoretiese en impiriese data, aangebied word.

Acknowledgement

In the course of the project, I benefited from the generous participation of the IG DOD officials; Officers Commanding and Transport Officers nationwide; SITA Officials; and CMIS Support Brigadier General A. R. Cumming and Staff.

I would like to acknowledge the support from the following individuals:

- My supervisor Mr Daniel F Botha, on whom the success of this work depended;
- Professor Kinghorn and his Staff (Stellenbosch University), for believing in me;
- Mr D. Dladla: Chief Director: Strategic Management;
- Ms A. Mamabolo from the Department of Education, who provided the research layout and steps to follow.
- Defence Intelligence provided the necessary insights into the administration of security classification of this document throughout the course of this research; and
- My children Mmakgano, Kgaogelo; my grandchildren Koketso and Kgomotso, for their support and understanding.

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

ACC	Anti-Corruption Co-ordinating Committee
ADC	Architecture Development Cycle
ADM	Architecture Development Method
ALMA	Architecture Level Modifiability Analysis
ATAM	Architecture Trade off Analysis Method
BA	Business Architecture
BI	Business Intelligence
B2B	Business-to-Business
B2C	Business-to-Consumer
CAE	Chief Audit Executive
CAS	Crime Administration System
C Dir	Chief Director
C Dir CI	Chief Director Counter Intelligence
CHR	Chief Human Resource
CI	Counter Intelligence
C FIN	Chief Finance
C FIN DFSS	Chief Finance Director Finance Support Service
CICP	Centre for Intelligence Crime Prevention
CIO	Chief Information Officer
CMIS	Command Management Information System
COTS	Commercial off the Shelf
CTA	Concept Technology Architecture
CRC	Criminal Technology Centre
DACAF	Directorate Anti-Corruption and Anti-Fraud
DAF	Directorate Anti-Fraud
dDoS	Distributed Denial of Service
DEISA	Defence Enterprise Information System Architecture
DEIMS DIV	Defence Enterprise Information System Management Division

DEIS	Defence Enterprise Information Systems
DICT	Defence Information and Communication Technology
DISCS	Defence Information and Communication System
DOD	Department of Defence
DOD INFO STRAT	Department of Defence Information Strategy
DOD LFS	Department of Defence Logistical Support Services
DoS	Denial of Service
DPA	Directorate Performance Audit
DP	Data Processing
DPSA	Department of Public Service and Administration
DRA	Directorate Regulatory Audits
DVD	Departement van Verdediging
EFT	Electronic Funds Transfer
EMI	Enterprise Application integration
GAPC	Global Programme Against Corruption
GATs	General Agreement in Service
GDA	General Defence Account
GII	Government Information Infrastructure
GITA	Government Information Technology Architecture
GITOC	Government Information Technology Office Council
GRAP	General Recognised Accounting Paradise
G2B	Government-to-Citizens
G2C	Government-to-Consumer
G2E	Government-to-Employee
G2G	Government-to-Government
HR	Human Resources
ICAC	Independent Anti-Corruption Commission
ICASA	Independent Communications Authority in South Africa
ICSS	Information and Communication Systems Security

ICTs	Information and Communication Technologies
ICSS	Information and Communication Systems Security
IEEE 1362	Concept of Operations
IEEE1233	System Requirement Specification
IG DOD	Inspector General Department of Defence
ILO	International Labour Organisation
IM	Information Management
INCOSAI	International Congress of Supreme Audit Institution
IP	International Protocol
IPR	Intellectual Property Right
IPSAS	International Public Sector Accounting Standards
IS	Information Systems
ITU	International Telecommunication Unions
JWM	Joint Warfare Manual
LAN	Local Area Network
LOG	Logistics
MDC	Military Discipline Code
MDM	Master Data Management
MEC	Member of Executive Committee
MI	Maintainability Index
MIS	Management Information Systems
MPA	Military Police Agency
MPD	Military Police Division
MTEF	Medium Term Expenditure Framework
NACF	National Anti-Corruption Forum
OAIS	Open Archival Information System
OECD	Organisation for Economic Co-operation Development
OSIS	Operational Support Information System
OTS	Off-the-Shelf

PDA	Protected Disclosure Act
PFMA	Public Finance Management Act
PROC	Procurement
PSC	Public Service Commission
SAI	Supreme Audit Institution
SA DOD	South African Department of Defence
SANDF	South African National Defence Force
SAPS	South African Police Services
SARS	South African Revenue Services
SCM	Supply Chain Management
SDA	Special Defence Account
SIB	Standard Information Base
SITA	State Information Technology Agency
SMME	Small Medium and Macro Enterprises
SLA	Service Level Agreement
SWP	Standing Work Procedures
TAFIN	Technical Architecture Framework for Information Management
TCP	Transmission Control Protocol
TRs	Treasury Regulations
TRIP	Trade Related Aspect of Intellectual Property
UNCTAD	United Nations Conference of Trade and Development
WAN	Wide Area Network
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation
ZIFA	Zachman Institute for Framework Advancement

Chapter 1
Introduction and Background

1.1 Organisation of DOD

It has become essential for enterprises in today's business environment to make extensive use of computer systems and applications in order to establish and maintain a competitive advantage. However, as time passes, software systems need to be maintained, modified, and integrated with other systems so as not to become obsolete. It is therefore imperative to ensure that resources for these applications and systems are available to all users and business processes that may benefit from their use, if they are to provide the desired advantage.

The Department of Defence is a Government institution whose business environment is defined by its direct interaction with clients, suppliers, labour unions, government agencies, as well as the general environment. It has established congruencies or alignments between its different subsystems in order to eliminate potential dysfunctions. The DOD could be conceived of as system with interrelated subsystems of a strategic, human, technological, structural and managerial nature which need to be internally consistent and adapted to environmental conditions. This study is based on how DOD operates in terms of these subsystems, in particular, the structural, technological, managerial and human subsystem with regard to vehicle management.

The DOD is considered as a complex organism reflecting increased differentiation and specialisation of function, and which thus require more complex systems of integration to maintain the system as a whole. It maintains a structure with clearly defined jobs vested in formal position in a hierarchy where seniority is important. The problem, currently, is that there are currently various isolated IT systems with regard to transport management within the DOD. The fact that there is no single vehicle management system makes accountability and management difficult if not impossible is some cases. Consequently, this creates a platform for corruption and fraud to be committed. The HM Treasury Report (2001) states that "computer crime is on the increase and, while key risk areas remain, new dangers are emerging. The dynamic nature of technological advances requires careful planning and

management to maintain security and contain developing skills"[1]. Government departments have a broad range of stakeholders requiring them to be accountable and show responsibility. If fraud or corruption is committed against them, the impact may be significant - including damage to their reputation, image and standing in the community.

1.2 The DOD Business Problems

Corruption and fraud has become a serious issue regarding vehicles management (fleet management) in the DOD's organisational entities that could be partially ascribed to the lack of integration between IS (application systems), especially between Vehicle Management Systems (VMS), the Financial Management Systems (FMS) and the Human Resource Management Systems HRMS). These systems, at the moment, are not linked to each other and as a result, they do not provide sufficient control mechanisms or collusion[2]. The following scenario explains the seriousness of the problem:

- It is possible for a member to be allocated a DOD vehicle (VMS) whilst being on leave (HRMS) and claim travel and subsistence, including accommodation allowance (FMS). There is no way that Finance or HR personnel could pick up the problem.

Lack of integration does not apply among functional systems only but also within VMS itself:

- There are two main systems used within the DOD namely, OSIS and CALMIS. These systems are not integrated and as a result, information about a vehicle stored in CALMIS cannot be retrieved via OSIS;
- Vehicle history files are area bound: vehicle history files for one unit cannot be retrieved in another unit, let alone provinces.

It is therefore difficult for management to obtain reliable information in order to make informed decisions. It is for this reason that factors affecting application integration within the DOD need to be identified and acted upon in order to close the gaps created by these systems.

---

[1] The HM Treasury Report: 2008 highlights to us the situation regarding the role managers should play to eliminate corruption and fraud in the area computers.

[2] In his article, Tshivhidzo: 2008 quoted the late Mr Masilela, the then Secretary for Defence stating that " the department, which has one of the largest asset base both of movable and immovable assets, is unable to properly manage its assets due to poor computer systems.

1.3 The Research Problem

Organisations depend on technology to pursue functions within their environments. The dependence on technology has grown over years, resulting in the need to integrate disparate applications into a unified set of systems. There are instances where these technologies have been embraced and adopted across the enterprise and eventually became core pieces of an organisation's IT infrastructure, whereas, in other instances, adoption has been limited to specific departments or technologies which resulted in the creation of islands of automation through generations. Lack of integration for these systems seems to open doors for corrupt and fraudulent activities whereby employees perform illegal transactions knowing that it will be difficult to trace them. Identifying and acting upon such factors could help promote accountability and manageability: using Enterprise Application Integration (EAI) to integrate systems and applications might help organisations to curb or limit corruption and fraudulent activities: especially in the case of public sector organisations that have to manage large numbers of vehicles used in execution of their business operations.

1.4 Research Objectives

The aim of this research is to investigate factors affecting systems integration within the DOD: factors which tend to open doors for corrupt and fraudulent activities. The fact that there is no single management system integrating critical applications makes accountability and management difficult, if not impossible. It has become essential for enterprises in today's business environment to make extensive use of computer systems and applications in order to establish and maintain a competitive advantage. Unfortunately, all too often these applications are not freely integrated within an organisation, preventing the seamless flow of information throughout the enterprise, therefore forming the "information silo", or pooling of information resources. The objectives of this study are therefore to investigate various unsynchronised vehicle management systems within the DOD units; to determine factors contributing to lack of vehicle management systems integration; and to recommend a single management system which will be beneficial for the DOD and other organisations. Recommendations made in this research could also help organisations to meet demands and could find ways of binding these isolation applications into a single, unified enterprise application, in terms of vehicle management.

Many enterprises are facing integration problems due to the fact that until relatively recently there was no expectation that applications should be able to "shake hands or "talk" to each

other". Today however, we expect all of our IT applications to speak the same language. Enterprises therefore have to choose either to start afresh, an option found to be prohibitively expensive and disruptive to the business, or to remain reliant on the old, out of date legacy systems. The challenge, therefore, is to find technical solutions to the problems that arise from application incompatibility[3].

1.5 Importance of Research

It is important to conduct this study in order make decision makers aware of the importance of embracing Information and Communication Technologies (ICT) for achievement of development goals. Organisational systems, particular of a legacy in nature, have been designed to be standalone with little intention for future integration. It is not easy to replace such systems with newer systems as they represent a huge financial implication and tend to embody a significant amount of corporate knowledge. Enterprise Application Integration (EAI), which requires a management vision, commitment, and leadership that get beyond short-term sub optimal solutions to position the enterprise to remain competitive long into the future. The success of this research will help minimise corruption and fraud as well as help reduce bad publicity such as the DOD being quoted "as having one of the largest asset bases, both movable and immovable assets, but also being unable to manage those assets properly due to poor computer systems[4]. These systems are referred to as not being linked to each other. The endeavour is to gain support of decision makers in favour of application integration in order for them to achieve the functionality and quality properties of implementing enterprise networking and the new information technology infrastructure[5].

1.6 The Research Design

This study is based on qualitative research and offers a descriptive scenario of the DOD vehicle management systems. The main source of data was an intensive perusal of the extant scientific and academic literature on the core theme of the thesis as well as on relevant peripheral themes. Furthermore, data were collect by the researcher through examining documents and interviewing DOD relevant members. Interviews and observation during site

---

[3] Software incompatibility is described as a characteristic of software components or systems which cannot operate satisfactorily together on the same computer, or on different computers linked by a computer network , viewed at http://wikipedia.org/wiki/Software_incompatibility

[4] The late Secretary for Defence, Mr Masilela in defence of the unqualified reports received from SCOPA.

[5] Laudon & Laudon: 2004 describe management issues and decisions in terms of information technology infrastructure for digitally enabling the enterprise.

visits allowed the investigator to differentiate between system failure and human factor errors; errors which could not be depicted over telephonic interviews. Failure to incorporate such information might have led to some of the problem areas being left unattended and would restrict recommendations. Journal articles, website articles and DOD reports and policies and relevant cases were used as secondary data to support the arguments for possible solutions. Triangulation for analysing multiple data forms which showed similar relevance/results was attempted. As a result, it became possible to identify human errors which, otherwise, would not have been depicted over telephonic interviews.

1.7 Outline of the Thesis

Emanating from the need to integrate systems in order to fight against corruption and fraud, this study will introduce the following chapters: Chapter 2 which describes different research methods from which the methodology for this research was chosen; Chapter 3 where themes of corruption and fraud are addressed as highlighting two factors: that contextualising the problem of corruption and fraud; and recognizing that they exist must not be the end of the analysis; Chapter 4, on e-commerce and Chapter 5 on e-Government, describe factors that necessitated the need to integrate systems for improved collaboration and communication internationally; Chapter 6 presents the DOD Enterprise Information Systems and Architecture services; and Chapter 7 describes findings and recommendations which reveal concerns related to work-base environment and proposes action that could be taken to bring about change.

1.8 Conclusion

This chapter emphasised how organisations need the capability to efficiently interact, collaborate and exchange information with internal and external business partners. To satisfy this need, organisations should acquire and acknowledge the importance of ICT. However, as time passes, software systems need to be maintained, modified, and integrated with other systems so as not to become obsolete. Whilst faced with the problem of maintaining ICT, managers also have to counter for corrupt and fraudulent activities of employees. The study will maintain that systems be linked/integrated in order to simplify and automate business processes to the greatest extent possible, while at the same time avoiding having to make sweeping changes to the existing applications or data structures. Moreover, managers need to integrate these information and telecommunication systems in order to counter acts of

corruption and fraud. In the next chapter, the relevant theory of Research Methodology will be discussed in order to motivate the methodologies chosen for this research.

Chapter 2

Research Methodology

2.1 Introduction

The aim of this chapter is to introduce to the reader to different philosophies of the research process from which, the methodology for this investigation was chosen. Research methodology considers and explains the logic behind research methods and techniques. It is of great importance to indicate here that this study was conducted with knowledge that one has an obligation to use appropriate methodology in conducting a study, and that an inappropriate methodology result in incorrect reporting as well as inappropriate use of information. Types of research and methods of data collection are discussed.

2.2 Types of Research

Different authors have different views about types of research. Literature holds that research is typically divided into the categories of *basic* and *applied*. These categories are also considered as designs wherein three types are offered as quantitative, qualitative and mixed methods. On the other hand, research could be classified from three perspectives, namely: application of the research study; objectives in understanding the research and inquiry mode employed. Classifications are discussed below[6]:

2.2.1 Application

Two broad categories for examining a research endeavour from the perspective of its application are pure and applied research. Literature informs that pure research involves the testing of theories and hypotheses that are intellectually challenging but may or may not have practical application at the present time or in the future[7]. Undertaking applied research imply that the objective should be improvement of the quality of particular discipline[8]. Research is called applied when the solution to a research problem has practical consequences and the finding thereof, can be applied to solve social problems of immediate concern[9].

---

[6] Kumar: 2005's classification of research from three perspectives.

[7] Booth et al: 2008 define pure research in a similar way.

[8] Merriam: 2009 maintains that other forms of applied research are evaluation studies and action research.

[9] A description of applied research as extracted from Booth et al: 2008.

2.2.2 Objectives

A research endeavour for examining a research study from the perspective of its objectives can be classified as descriptive, correlative, and explanatory. Descriptive investigations are aimed at the accurate estimation of frequency in the population of certain responses[10] and explain a situation, problem, phenomenon, services of or program systematically with the main purpose of describing what is prevalent with respect to the issue/problem under study[11]. The aim is to know more about a phenomenon[12]. In a correlation study, the main emphasis is to discover the existence of a relationships / association / interdependence between two or more aspects of a situation[13]. The researcher's control is said to be limited almost entirely to the statistical data manipulation where data have been from the scene where they were collected and are stored in a format of some sort[14]. While explanatory research attempts to clarify why and how, exploratory research attempts to explore an area where little is known or investigate the possibilities of undertaking a particular research study[15]. Most studies are said to be a combination of descriptive, correlation and explanatory[16].

2.2.3 Inquiry Mode

The third perspective concerns the process one adopts to find answers to his/her research. This consists of the quantitative and qualitative approaches. The structured approach is usually classified as quantitative research and unstructured as qualitative research. In the structured approached everything that forms the research process is predetermined, whereas the unstructured approach allows flexibility in all aspects of the research process. The structured approach is more appropriate to determine the extent of a problem, situation, issue or phenomenon: the unstructured, to explore its nature. Booth et al (2008) maintains that approaches are said to have their own strengths and weaknesses, but we are not to "lock" ourselves into solely quantitative or qualitative research[17]. Different quantitative and qualitative processes will be discussed in detail below:

---

[10] Sapsford et al: 2006 emphasise that the investigator and the reader are concerned with reasonably accurate estimations.

[11] The concept of descriptive research as explained further by Kumar: 2005.

[12] Merriam: 2009 offers the aim of basic research which is classified by Kumar: 2005 as objective research.

[13] Variables are said to be correlated when high values on one predict high values on the other.

[14] Many statistical techniques are said to establish symmetrical relationships between variables and do not attempt to establish causality, while others do.

[15] Kumar: 2005 on the concept of descriptive, correlation and exploratory perspectives.

[16] Kumar: 2005 in support of the idea that we do not have to lock ourselves up in our choices.

[17] An overview of the inquiry mode by Kumar: 2005.

- Quantitative research. This is a method of inquiry aimed at gathering an in-depth understanding of human behaviour by investigating not just *the what, where, and when but also the why and how.* The process of measurement is central to quantitative research because it provides the fundamental connection between empirical observation and mathematical expression of quantitative relationship[18].
- Qualitative Research, as suggested, is exploratory, and the researchers use it to explore a topic when the variables and theory base are unknown[19]. It aims to capture concepts associated with interpretive approaches to knowledge: qualities that are not quantifiable or reducible to numbers, such as feelings, thoughts, experiences, and so on. Qualitative research uses non-numerical data and analysis to describe and understand such concepts[20]. Practices turn the world into a series of representations including field notes, interviews, conversations, photographs, recordings and memos[21].

The following comparison of quantitative and qualitative methods gave guidance when the method for this study was chosen. The comparison of data collection is based on[22]:

- Value of data: quantitative and qualitative provide a trade off between breadth and depth, and between generalisability and targeting to specific populations.
- Scientific Rigor: Collins Pocket Dictionary defines rigor by typically using terms such as "harshness, severity, strictness and sternness" to describe its nature. Herscheim et al (2003) hold that "if it isn't rigorous, it isn't scholarly and shouldn't be published". Academically, rigor means applying the accepted method of science[23]. Better techniques for classifying and analysing large bodies of descriptive data have been developed, due to the awareness by quantitative researchers that some of their data may not be accurate and valid. It is also increasingly recognised that all data collection – quantitative and qualitative – operates within a cultural context and is

---

[18] Information on quantitative research as given by Wikipedia: http://en.wikipedia.org/wiki/Qualitative_research

[19] Cresswell: 2009 maintains that in a qualitative research project, the author will describe a research problem that can best be understood by exploring a concept or phenomenon.

[20] The aim and all concepts associated with interpretive approaches included are offered by Gratton: 2004.

[21] Ritchie et al: 2003 give us properties of qualitative research to differentiate it from quantitative research.

[22] A comparison by Westat: 2002 helped to choose a data collection method for this study with acknowledgement of aspects mentioned in his comparison.

[23] Hirschein & Klein: 2003 argue that an academic view of rigor excludes other forms of scholarly research that do not describe to such positivist standards.

affected to some extent by the perception and beliefs of investigators and data collectors.

- Philosophical Distinction: qualitative research does not start with clearly specified research questions or hypotheses to be tested; instead, questions are formulated after open-ended field research has been completed.
- Costs: it is difficult to generalise about the relative costs of the two methods: much depends on the amount of information needed, quality standard followed for the data collection and the number of cases required for reliability and validity. To obtain robust findings, the cost of data collection is bound to be high regardless of method. Costs involved in this study are those covering allowances; travel and subsistence, accommodation and meals.
- Time constraints: similarly, data complexity and quality affects the time needed for data collection and analysis. Although technological innovations have shortened the time needed to process quantitative data, qualitative methods may be even more time consuming because data collection and data analysis overlap, and the process encourages the exploration of new evaluation questions. If insufficient time is allowed for evaluation, it may be necessary to curtail the amount of data to be limiting the value of the findings.

2.3 Sources

Sometimes, information required for conducting research is already available and need only to be extracted. However, there are times when the information must be collected. Two major approaches of gathering information about a situation, person, problem or phenomenon are primary and secondary data[24].

2.3.1 Primary Sources

Primary sources are said to provide "raw data" used first to test one's working hypothesis and then serve as evidence to support the claim. Primary sources, in history, include documents from the period or person one is studying, objects, maps, and even clothing; in literature or philosophy, one's main primary source is usually the text one is studying, and one's data are the words on the page[25]. Since one can rarely write a research report without using primary

[24] A simplification of methods of data collection as presented by Kumar: 2005.

[25] Strauss et al: 1998 state the importance of research sources.

sources, for this study, DOD members, stakeholders from within and outside the DOD, DOD documents and those from other government departments, and some other text that were studied will be used.

2.3.2 Secondary Sources

Secondary sources are research reports that use primary data to solve research problems written for scholarly and professional audiences. Data from secondary sources can be used to support an argument, but only if one cannot find those data in a primary source. A secondary source therefore becomes a primary source when one studies its argument as part of a debate in a field[26]. In this study, journal articles, website articles and DOD reports and policies will be used as sub-primary data to avoid problems associated with secondary sources, which are: the need to ensure that the data collected was valid, reliable and not subject to any serious methodological error; and the need to be aware of when data was collected and whether is it still appropriate. One must also be aware that the original author of the data may have been subjected to particular constraints or had a particular agenda.

2.4 Data Collection Methods

Data conveyed through words have been labelled qualitative, whereas data presented in numbers form are quantitative. Data collection is about asking, watching, and reviewing[27].

2.4.1 Observation

The observation method is a technique in which the behavior of research subjects is watched and recorded without any direct contact[28]. It is a method through which an individual or individuals gather firsthand data on programs, processes or behaviours being studied. Approaches allow the evaluator to learn about issues the participants may be unaware of, or that they are unwilling or unable to discuss candidly in an interview or focus group[29]. Observation is associated with the *Hawthorne Effect*, which, depending upon the situation, may change participants' behaviour[30]. Two types of observation are participant: one which

---

[26] Booth et al: 2008 inform that one does not have to agree with a source to use its data, and its argument does not even have to be relevant to one's question. .

[27] According to Merriam: 2009, the idea that we "collect" is a bit misleading since data are not "out there" waiting collection, like so many rubbish bags on the pavement.

[28] An explanation of observation as one of the research methods.

[29] Westat: 2002, Kumar: 2005 and Duff: 2008 elaborate on the issues of observation as a method for data collection.

[30] Kumar: 2005 introduces a reactive research on the social phenomena being studied.

involves the researcher's participation in the activities of the group being observed in the same manner as its members, and non-participant wherein the researcher does not get involved in the activities of the group but remains a passive observer.

Observation methods are said to: offer firsthand information; to be simple to use; help verify data from other sources and useful for manual and psychomotor tasks; and provide direct information about behaviour of individuals and groups[31]; observation methods are also said to: permit the evaluator to enter into and understand the situation/context; provide good opportunities for identifying unanticipated outcomes, and exist in natural, unstructured, and flexible settings[32]. Observation methods bear disadvantages such as: expensive and time consuming, need well-qualified, highly trained observers; may need to be content experts, may affect behaviour of participants, selective perception of observer may distort information and behaviour or sets of behaviour observed may be atypical[33]. Though considered time consuming and may bias worker behaviour, *observation* was preferred since it is viewed as providing the opportunity to document activities, behavior, and physical expressions[34] the investigator could have missed out during telephonic interviews.

2.4.2 Interviews

Five issues to be addressed at the outset of every interview are described by Merriam (2009) as: the investigator's motive and intention and the inquiry's purpose; protection of the respondents through the use of pseudonyms; deciding who has final say over the study's content; payment, if any and logistics with regard to time, place, and number of interviews to be scheduled[35]. The concept of "interviewing" covers a lot of ground, from totally unstructured interaction, through semi-structured situations, to highly formal interactions with respondents. Interviewing is done on the phone, in person, by mail or even by computer[36]. Different types of interviews can be categorised in a number of ways. The types of interviews in terms of the amount of structure will be discussed first, followed by interviews originating from different theoretical perspectives, and the focus group.

---

[31] Advantages of observation obtained from http://www.humanresources.hrvinet.com/observation-methods/

[32] More on advantages of observation as obtained from http://www.nsf.gov/pubs/1997/nsf97153/chap_3.htm

[33] Observations are inevitably filtered through the lens of the observer, Westat: 2002.

[34] Additional information on the disadvantages of observation.

[35] Merriam: 2009 further maintains that the interviewer must be aware of his or her stance towards the interviewee, and he or she must assume neutrally.

[36] The concept of interviewing as discussed by Bernard: 2006.

In a structured interview the researcher asks a predetermined set of questions[37]. It is usually used to obtain demographic data.[38] One variety of structured interviews involves use of an explicit set of instructions of interviewers who administer questionnaires orally. Advantages of structured interviews are that: they usually yield richest data; they offer new insights; they permit face-to-face contact with the respondents; they allow the interviewer to experience the affective as well as the cognitive aspects of response and, they allow the interviewer to explain or help clarify increasingly the likelihood of useful responses and they allow the interviewer to be flexible in administering the interview to particular individuals or in particular circumstances. Structured interviews have some disadvantageous like: they are expensive and time-consuming; they need well qualified, highly trained interviewers; the interviewee may distort information through recall error, selective perceptions, the desire to please interviewer; the fact that they are flexible can result in inconsistencies across interviews, and volume of information very large; may be difficult to transcribe and reduce data[39].

In semi-structured interviews, either all of the questions are more flexibly worded or the interview is a mix of more and less structured questions. Usually, specific information is desired from all respondents, in which case there is the more structured section of the interview, but the largest part of the interview is guided by a list of questions for issues to be explored, and neither the exact wording nor the order of the questions is determined ahead of time[40]. Semi-structured interviewing is said to be the best in situations where you won't get more than one chance to interview someone. Formal written guides are an absolute must if you are sending out several interviewers to collect data[41]. In unstructured/informal interviewing, there is nothing at all informal about unstructured interviewing, and nothing deceptive, either. Although informal interviewing seems to be characterised by a total lack of structure or control, there is a warning that one should never mistake the adjective "informal" or "light weight" should never be mistaken, because it is hard work on and can get pretty

---

[37] The researcher uses the same wording and order of questions as specified in the interview schedule, Kumar: 2005

[38] Merriam: 2009 mentions demographic data such as age, gender, ethnicity and education as examples.

[39] Bernard: 2006 on advantages and disadvantages of structured interviews.

[40] Semi structured interviewing as described by Merriam: 2009.

[41] Semi structured interviewing works very well in projects where one is dealing with people who are accustomed to efficient use of their time, Bernard: 2006.

tiring[42]. However, it is flexible and exploratory and used when the researcher does not know enough about the phenomenon in order to ask relevant questions[43]

Interviews by philosophical orientation include census taking, surveying and opinion polling, which are measurement-oriented forms of interviews. A clear analysis of the link between philosophical orientation and type of interview is given in six conceptions: *neo-positive*, a skilful interviewer asks questions, minimises bias through neutral stance and generates quality data and produce valid findings; *romantic interview:* the researcher does not claim to be objective but analyses and reveals subjectivities; *constructivist interview*: the concern is on how tools such as discourse analysis, narrative analysis and conversation analysis are used to construct interview data; *post-modern interview* where the aim is not to come up with a single perception of the self but "various non-unitary performances of selves", presented via creative performance; *transformative and de-colonising* share a critical theory philosophical orientation. Herein, power, privilege and oppression are revealed. While in transformative the researcher "intentionally" aims to challenge and change the understanding of participants, in a decolonising interview, concern is with restorative justice for indigenous people[44].

Focus group interviews are said to be successful compromises between different demands that are difficult to reconcile with one another[45]. Data obtained from a focus group is socially constructed within the interaction of the group; a constructivist perspective underlies this data collection procedure. The focus group interview goes one step beyond the open-ended question as in a structured interview since questions are not written in advance hence they may be tailored to probe avenues of explorations that seem to be yielding relevant information. Literature reveal that the most difficult thing about interviews, particularly in a large study conducted over a long period (longitudinal study), is when some group members will die during the course of the study, or others have to move long distances away or be difficult to re-interview without great cost. This method was not preferred because this study contains sensitive issues and a focus group is a poor choice for topics that are sensitive,

---

[42] Unstructured interviews involve far less procedural reactivity than the standardised format of the interview schedule or the questionnaire, Bernard: 2006.

[43] Bernard: 2006 maintains that the researcher just tries to remember conversations heard during the course of the day in the field. One has to remember a lot and duck into private corners a lot so one can jot things down; and one has to use a lot of deception to keep people from knowing that one is really at work, studying them.

[44] According to Merriam: 2009, other writers categorise interviews based more on disciplinary perspectives, e.g. the ethnographic interview which focuses on culture.

[45] Flick et al: 2004 mention that there are different types and procedures of qualitative interviews.

highly personal, and culturally inappropriate to talk about in the presence of strangers. It is also not always obvious ahead of time to know how appropriate a topic might be[46].

2.4.3 Questionnaires

Questionnaires are one kind of structured interview. A questionnaire is a written list of questions, for which answers are recorded by respondents. The only difference between an interview schedule and a questionnaire is that in the former, it is the interviewer who asks questions and records the respondent's replies on an interview schedule, whereas in the latter replies are recorded by the respondents themselves. A questionnaire is generally mailed or handed to the respondent and filled in by him/her without help from the interviewer. Since there is no one to explain the meaning of questions to respondents, it is important that questions are clear and easy to understand. Hence it should be developed in an interactive style in order to allow respondents to feel as if someone is talking to them. An interactive statement should preface a sensitive question or questions respondents may feel hesitant about answering[47]. This method could not be applied to this study since it is regarded as being not suitable for providing in-depth understanding of an issue[48] and because of its numerous other disadvantages: lack of flexibility; low response rate; no control over environment; no control over question order; cannot record spontaneous answers; difficult to separate bad addresses from no responses; no control over date of response; many questions may remain unanswered and possibly bias the sample[49].

2.4.4 Survey Research

Survey research, consisting of a structured list of questions presented to people, is one of the most important areas of measurement in applied social research, encompassing any measurement procedures that involve asking questions of respondents[50]. Surveys may be written or oral, face to face over the phone. It provides numeric description of trends,

---

[46] The objective of focus group study is to get high-quality data in a social context where people can consider their own views in the context of the view of others, Merriam: 2009.

[47] Questionnaire question formulation as explained by Kumar: 2005.

[48] The disadvantage of questionnaire method as given by Judge: 2008.

[49] Mailed survey is regarded to be superior to the interview for gathering information on sensitive or socially indescribable subjects.

[50] Information about survey research obtained from http://socialresearchmethods.net/kb/questype.php

attitudes or opinions of a population by studying a sample of that population[51]. Though being referred to as paper-and-pencil instruments, evaluators are increasingly exploring the utility of survey methods that take advantage of the emerging technologies, leading to administering via computer-assisted calling, as e-mail attachments, and as web-based online data collection systems[52]. It is possible to cheaply survey large numbers of people, but the data quality may be lower than some other methods because people do not always answer questions accurately[53]. Although survey research has the following as its advantages: good for gathering descriptive data; can cover a wide range of topics; are relatively inexpensive to use and can be analysed using a variety of existing software, its self-reporting element may lead to biased reporting, data may provide a general picture but lack depth and may not provide adequate information on context[54]. Survey research could not be considered as such in this study since the aim is to describe the situation within the DOD.

2.5 Methodology chosen for this study

The *primary* methodology that was used by the researcher was an intensive literature study of the relevant topics that form the core content of the thesis document/research report. Data was collected from this literature research, interpreted and applied to the *secondary* data collected by empirical methods in order to support the evidence found when investigating the entities of the chosen case study, namely the units of the DOD. The study was performed at the DOD units in South Africa. The main study site was a functional unit, namely, the South African Army (SA Army). Other Arms of Services, namely the South African Air Force (SAAF), the South African Navy (SA Navy) and the South African Medical Health Services (SAMHS) also served as study units for comparison of vehicle management systems.

The research question is regarded as a timely, topic-of-the-day research issue for large organisations such as the DOD, and it is hoped that the practicality of this research would ultimately be recognised by the DOD and that the results will be given immediate attention and be implemented timely.

---

[51] Creswell: 2009, in addition, states that survey research includes cross-sectional and longitudinal studies questionnaires or structured interviews for data collection, with the intent of generalising from a sample to a population.

[52] Even the traditional approach of mailing surveys for self-guided responses have been supplemented by using facsimile for delivery and return; Westat: 2002.

[53] The advantages and disadvantages of survey research are listed in many *social research methods* websites.

[54] An explanation of survey research by Westat: 2002.

A qualitative methodology was applied due to the existing need to explore, understand and describe the factors affecting integration of vehicle management systems within the DOD[55]. Choices were made based on information given that we are not to "lock" ourselves into solely quantitative and qualitative research[56]. It is also known to the investigator that all qualitative data collection operates within a cultural context and is affected to some extent by perceptions and beliefs of investigators and data collectors. Although, as supported by Merriam: 2009, interviewing was preferred to be (sometimes) the *only* way to get data, unintended observation emerged and happened to form part. The "Hawthorne effect" was experienced during site visits, depending on which group the investigator accompanied (investigators or awareness trainers); the fact that the investigator is from the Directorate Anti-Corruption and Anti-fraud; as well as the knowledge that there is somehow the presence of non-adherence to policies within a unit[57]. Personal interviews (site visits); telephone interviews and observation were therefore practical, regardless of the geographic spread of possible respondents and time limits.

Data collection and analysis were based on a qualitative research strategy, journal articles, websites and DOD reports and policies. The investigator chose to be the key qualitative instrument since, qualitative researchers collect data themselves through examining documents, observing behavior, or interviewing participants, rather than relying on questionnaires or instruments developed by other researchers. Three types of data collection and analysis methods were merged to achieve improved quality of information and to satisfy the analysis of the subjective area of the DOD vehicle management systems. As to the cost of the study, much depended on the amount of needed, quality standards followed for the data collection and the number of cases required for reliability and validity; more time required for site visits due to postponements. Triangulation was used to check and cross-check that data due to involvement of multiple sources methods and people that pointed to the same data. Triangulation allowed the researcher to ensure that facts are reliable and correct. The investigator's research methodology is represented:

---

[55] Sometimes qualitative research produces narratives, which document the course of the research project itself.

[56] Kumar: 2005 had an influence in making choices. For this study, alternative research method was studied and important points from them were noted, for example, the aim of the study is clearly defined by Craig: 2009 in her attempt to describe action research. Important to note is that action research material was considered for knowledge increase in and comparison of different research methods and not for application.

[57] Consideration was made of the advantage of the "Hawthorne effect" that while conducting an interview or focus group, what could not have been known over the phone could be observed.

Research Methodology

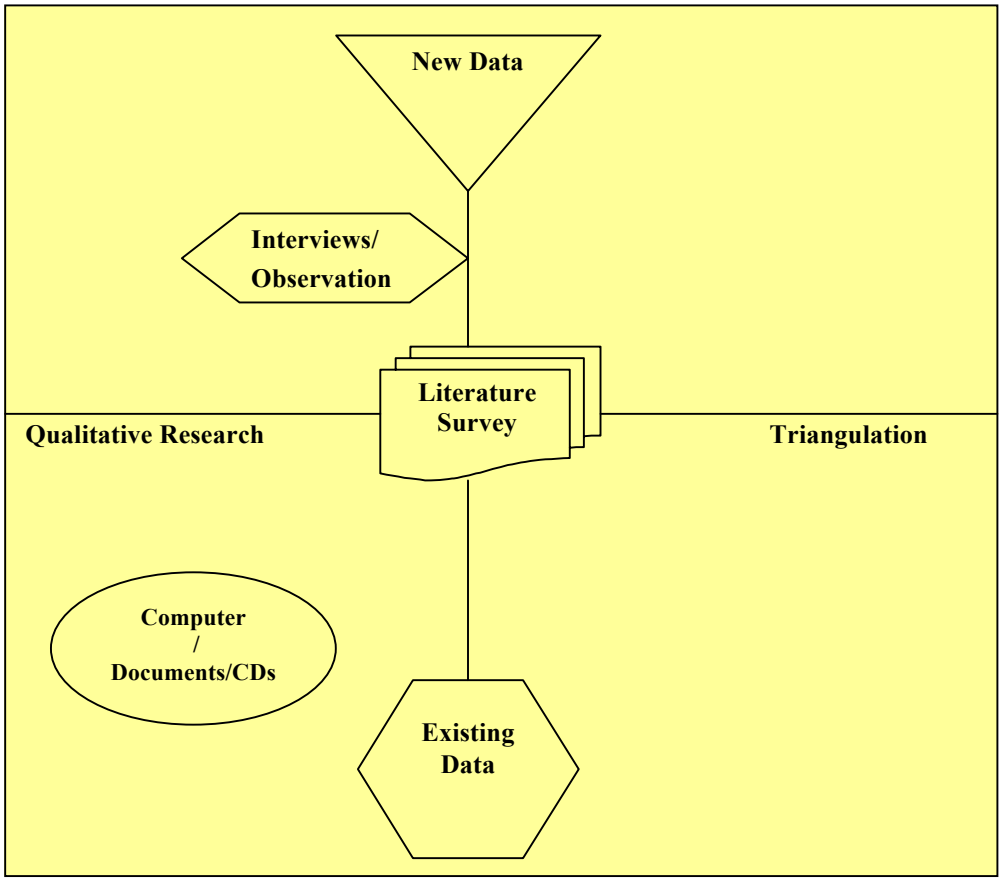

Figure 2.1 Research Method

Source: Investigator's own: 2009

Figure 2.1 represents tools in qualitative research that were used in this study where new data were collected through interviews and observation; extensive literature survey on sources such as books and journals; and existing data obtained from the DOD documentation such as policies, reports and manual. Also included are data obtained from websites and compact discs via the computer. By literature survey the investigator refers to data collected from sources such as books and journals. Since data were collected from multiple sources and methodologies, the investigator chose triangulation as a method to check and cross-reference the data. Figure 2.1 is an attempt to show the relationships between the entities, sources and methodologies, schematically.

2.6 Limitations to this Study

It is hard, if not impossible; to secure appointments with high ranked members due to their ever busy schedules. This study had to rely mostly on site visits conducted due to the fact that: telephonic interviews depended on the availability of interviewees in their offices; non-conformities could not be observed over the phone; some respondents' refusal to participate over the phone once they realised that the investigator is employed within the Defence Inspectorate Division (an auditing division). Moreover, the investigator works in the Directorate Anti-Corruption and Anti-Fraud. Automatically, the investigator gets confused /associated with corruption and fraud investigations. Site visits depended highly on Awareness Training and Detection Investigation Section schedules, which are affected by: on time approval of instructions by higher authority; the availability of trainees and/or investigations in certain units at that time; and involved members' willingness to include the investigator's name in their instruction as well as to travel with her. The names of interviewees and their units may not be made known for security purposes; the document, from time to time, must also be submitted to the Defence Intelligence for security purposes, the turnaround time may affect due dates for submission to the academic institution involved; details of corruption and fraud incidents could not be disclosed for confidentiality purposes.

2.7 Conclusion

Different research methods, their advantages and disadvantages were discussed and literature research supported by qualitative research was identified as the preferred method for this research. Methods for collecting data were also selected and those suitable for this research were described. Triangulation stood out to be a methodology for cross-checking the validity of data. Limitations to this research were also highlighted. The next chapter introduces factors of corruption and application integration as well as attempts by organisations to curb or minimise corruption and fraud.

Chapter 3

Corruption and Fraud Factors and Application Integration

3.1 Introduction

The aim of this chapter is to highlight how this study was influenced by concerns around corruption and fraud that have intensified all over the world in recent years. All government and law enforcement agencies all over the world are faced with challenges of corruption and fraud. Fighting it necessitates the need to close the gaps created by isolated systems which were built without consideration of integrating them. This chapter focuses on attempts by countries to counter corrupt and fraudulent activities. The SA position is discussed in comparison with foreign countries to see whether South Africa is at the same level or not, in order to identify areas that need improvement. The DOD position and problems encountered are indicated with the intent to raise concerns and action. Specific attention will be on government departments with special reference to the Department of Defence.

3.2 Definition and Dimensions of Corruption and Fraud

The term "fraud seems to be defined and categorised differently by different organisations, for example, the term is often used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. Literature clarifies that there is no precise international legal definition of *fraud* existing because these events are covered by national

country acts and no international act exists"[58]. For example, in Australia, fraud against the Common Wealth is defined as "dishonestly obtaining a benefit by deception or other means"; in France, the Social Security Code defines fraud as "actions aiming at obtaining, help obtaining or try obtaining social security benefits which are not due"; whereas the Netherlands is said to have no explicit definition. Its definition is not given on purpose as different implementation use different definitions. There are four main categories of fraud: identity fraud; income fraud; estate fraud and living situation fraud[59].

3.2.1 The Social and Economic Costs of Corruption

Corruption and fraud are significant problems affecting all countries in varying degrees, and organisations should endeavour to create an environment that is unfavourable to corruption and fraud. That corruption and fraud impacts on society is supported by the International Congress of Supreme Audit Institutions (INCOSAI) which noted presence of a strong correlation between corruption and the weakening of state institutions. At their 16th congress, INCOSAI members agreed that corruption and fraud in government waste resources, reduce economic growth and the quality of life, undermine the credibility of state institutions and reduce their effectiveness[60]. Like ignorance and environmental degradation, corruption and fraud are great enemies of development. Some departments within the South African Government could be regarded as considering the subject of corruption as being difficult or controversial to deal with, or as not important to warrant explicit attention. This is confirmed in the Public Service Commission Assessment (September 2004-31 July 2010) whereby 60% of departments are referred to as either having no policies or has very basic poor quality, reported by the Public Service Commission (PSC), as its assessment[61].

An understanding emerged that corruption is often linked to the socioeconomic environment of the population (social injustice, poverty, violence); a country's tradition, principles, and values influence the nature of corruption. Support for this statement was observed when looking into the current situation in South African government whereby corruption and fraud

---

[58] Definition of fraud as described in the HM Treasury: 2001 and the National Audit Report: 2006.

[59] A comparison of definitions of fraud as obtained from The National Audit Office Report: 2006, a summary table for international benchmark of social security Systems.

[60] Results of the conference that looked at the role and experiences of the Supreme Audit Institutions in preventing and detecting corruption and fraud , and the methods and techniques for preventing and detecting corruption and fraud as being given in the Corruption and Fraud Detection by Supreme Audit Institutions.

[61] The PSC reported to the National Anti-Corruption Forum Civil Indaba held 0n 23-24 September in Cape Town.

seems to have escalated. Hope for South Africans when they cast votes in 1994 whereby the once oppressed are the custodians of the vision and would pursue this vision in their leadership on behalf of and for the benefit of all citizens. Unfortunately, it is maintained that most South Africans show signs of stress as rooted in society, the governing party and the government itself. Corruption is hereby referred to as the source of stress: the stress as a result of the maladministration of funds in government institutions[62].

The notion that corruption is rife in government institutions is supported by the statement such as "South Africa is run by thugs and thieves"[63]. In an article titled, "Officials paid R100m for sitting at home"[64], the South African judicial system is accused of dragging its feet instead of expediting cases regarding suspended government officials. This becomes wasteful expenditure since government has to spend a lot of money on officials who could have been on duty, if cleared by the court or who could have been dismissed if so decided. Corruption, given this scenario, leads South Africans to experience a systemic crisis which leads to: economic uncertainty; undermined legitimacy; a weakened ability to promote development; poor accounting standards with undermined financial soundness; and distorted investment priorities and technology choices[65]. A staid intervention is necessary before the country becomes politically instable. Exposure of corrupt and fraudulent activities seems to be one promising form of intervention as the media enlightens the public about such activities. Restricting exposure would mean discarding intervention[66] and that would increase levels of corruption and fraud.

3.2.2 Causes of Losses

---

[62] Ndebele: 2011 states that there was a time when South Africans, particularly the formerly oppressed, believed that democracy would bring out a just constitutional state, but the dream is in danger of being destroyed. He questions if what is currently transpiring within the ruling party is the result of it experiencing a serious ethical decline resulting from internal conflict that corruption is so endemic and has become structurally visible.

[63] The Public Works Minister suggests that the government gives tenders to skilled professionals who will develop the country.

[64] Chauke: 2011 reveals that the government has been paying suspended senior officials (more than R100 million) since April 2009 due to dragging feet its feet in resolving disciplinary matters.

[65] Links between corruption, development and stability as offered by Bottelier: 1998.

[66] The two policies to be mentioned are the Protection of State Information Bill and the Act Disclosure of Assets. An article by Majavhu: 2011 disclosed a proposal by the Department of Public Service and Administration to amend the policy into allowing acceptance of presents, by public servants, from companies doing business with government. The draft Protection of State Information Bill about which caution is made that it will regulate classification of information in the interests of national security, a ruling that will end up covering wrongdoing and threats to public safety under a cloak of secrecy, Underhill & Donnelly: 2011.

Causes of internal fraud are said to include: weaknesses in fraud control plans; inadequate monitoring and reporting procedures; problematic information management and; and poor internal controls or override of internal controls[67]. Examples of incidents causing losses stipulated include, to mention a few, stock discrepancies; vehicle accidents; claims arising from: administrative inefficiency, injury to civilians during operations/exercises, and damage to property during operations/exercises; fraud with intent identified; theft of funds or material; damage to assets, movable or immovable; lost time/productivity; misuse of assets, including vehicles; delays in the timely convening, review and rectification of investigations, which leads to perpetration, and the inability of the DOD to recover losses; personnel related incidents; and overpayment. Sources for this research described causes such as: greed; poverty; intent resulting from the knowledge that no action will be taken against corrupt and fraudulent activities committed; making up for suffering experienced during oppression; preparation for exiting the government as caused by political stance as well a means to prohibit success in the ruling party; etc.

3.3 The South African Perspective

From the SA perspective, corruption appears in various permutations and degrees of intensity. The illustration of the manifestations of corruption is by no means complete or exhaustive. The Department of Sports, Arts and Culture classifies fraud in the following dimensions: *bribery* which involves the promise, offering or giving of a benefit that improperly affects the actions or decisions of public servants; *embezzlement* which is about theft of resources entrusted with the authority and control of such resources; *fraud* which refers to actions or behavior by a public servant or the other person or entity that fools others into providing a benefit that would not normally accrue to the public servant or other persons or entity; *extortion* whereby a public servant uses his or her vested authority to improperly benefit another public servant, person or entity, or using authority to improperly discriminate against another public servant, person or entity; *abuse of power* which includes conflict of interest, abuse of power, favouritism and nepotism[68].

When presenting the 2010/2011 financial year budget vote speech at the provincial legislature, Gauteng Member of Executive Committee (MEC) for Community Safety, Mr

---

[67] The results of a benchmarking exercise investigating issues of fraud and error in the social security systems of eight European and non-European countries by the UK Audit Office.

[68] The department of Sports, Arts and Culture in the Anticorruption booklet as obtained from the website http://www.srac.gpg.gov.za/Anticorruption%booklet.pdf

Khabisi Msunkutu stated ”corruption is like cancer that continues to rob millions of our citizens of their democratic rights. Most people who join government and police agencies do so with the objective of assisting the community. However, over time, a number of individuals start to abuse their official status for personal gain”[69]. A country with the goal of seeking to become a prosperous specialist market economy, while maintaining stability, cannot achieve its goal if corruption is allowed to take over. Corruption and fraud have spread worldwide so that even in countries once considered “clean”, there are no boundaries. Public sector bribery, corruption and fraud have become leading concerns for legislators around the globe, as the diversion of public funds undermines parliamentary control of the public purse. While still on public sector bribe, it is important to say that it is very disappointing to read that in South Africa, “a proposed new anti-corruption policy has stopped short of banning government officials from owning shares in companies that do business with the state”[70].

Successful implementation of the South African anti-corruption strategy, considering the different causes of corruption and fraud as given in paragraph 3.2.2, would require a devoted and hardworking government leadership: the leadership that would be willing to gang up and expose perpetrators of corruption and fraud[71], as well as allow and encourage the media to be more active in exposing corruption[72]; leadership that would promulgate, implement, monitor and evaluate policies that would help develop and sustain this country rather than destroy it further[73], whilst pretending to be enthusiastic[74]. However, not all leaders lack determination. There are leaders who do things right, even though, based on what is exposed by the media,

---

[69] The MEC holds that his statement is the commonly accepted definition of corruption.

[70] Majavhu: 2011, in the “Draft policy lenient on servants”, argues that a scandal erupted two years ago when Auditor General Terrence Nombembe revealed that 2 319 government officials had connections that did business with the government.

[71] In her article “Transparency a cure for the resources curse, Moyo: 2011 maintains that the movement to make mining companies disclose government payments could benefit South Africans. This is said to be the initiative of the United State in attempt to combating corruption, whereby the US President Barack Obama highlighted on how the law can impact on reducing corruption.

[72] Naicker: 2011refers the proposed Secrecy Bill as the “Crocodiles path to plenty, controlled by some members of the ruling party who are corrupt forces, some masquerading as radicals.

[73] Legg: 2010 refers to leaders such as the DPSA Minister who presented a project to fight corruption in the public service while , on the other hand, he proposed that public servant be allowed to accept presents (considered bribes) from companies doing business with government.

[74] Bagraim: 2011 writes “the Department of Public Service and Administration Minister should spare us the “breaking bones” and “zero tolerance” public relations rhetoric in relation to his proposed project to fight rampant corruption in the public service”. This is the very same Minister who allowed amendments in the draft policy on Disclosure of assets referred to in footnote 75, the draft regarded as being lenient on public servants.

they seem to be outnumbered. These leaders deserve credit for their right intentions as well as for executing the duties they promised to perform serving the public. A leader such as the Public Protector[75] and the Finance Minister[76], for example, strengthen constitutional democracy through execution of their mandate, doing so by exercising power without fear, errand or hesitation. Such leaders show commitment and determination; as a result, they should be supported and motivated for their soldiering on and their interventions they make.

3.3.1 The Public Service Commission (PSC)

The South African Government, like other governments in foreign countries, has underlined that successful participation in global capital markets requires the enforcement of rigorous regulatory standards with zero tolerance for corruption and fraud. Numerous anti-corruption campaigns and projects have been put in place by the government, including the hosting of the Ninth International Anti-Corruption Conference in October 1999. All these initiatives serve as proof that the government is committed to countering corruption and fraud and clear instructions were issued in this regard. On 22 November 2000 Cabinet approved that the National Anti-Corruption Forum (fraud included) be established by all organisations (public and private). One of the instructions given was for a Public Service Anti-Corruption Strategy to be developed and be presented to cabinet by July 2001. Following this was the development of the National Strategy incorporating both strategies for public and private sector[77]. DPSA was therefore charged with the responsibility to ensure that the strategy is implemented in all government departments.

3.3.2 The PSC Mandate

The PSC has, as its mandate, to: investigate, monitor, and evaluate the organisation and administration of the Public Service; promote measures that would ensure effective and efficient performance within the Public Service achievements, or lack thereof, of government programs; and promote values and principles of public administration as set by Constitution. The mandate also entails promotion of values and principles which include: a high standard of professional ethics; efficient, economic and effective use of resources; ensure maintenance

---

[75] The Public Protector's mandate is to investigate any conduct in state affairs or public administration in government institutions where suspicion prevails.

[76] The Finance Minister listened to the needs and added steps to the new growth path towards job creation, as outlined by the Economic Development Minister. However, results are being awaited, Bagraim: 2011.

[77] DPSA has a responsibility to ensure that there is an Anti-Fraud capacity within every government department.

of a development-oriented public administration; promote accountability of public administration; foster transparency, etc[78].

3.3.3 The PSC Key Performance Areas

Key performance areas of the PSC include: Labour Relations improvement which include conducting of investigative research and provision of advice on complaints and, grievances; labour relations and policies; Leadership and Human resources Reviews requiring the PSC to promote a high standard of public service leadership and to encourage best practices in human resource policies; Government monitoring involving the promotion of good governance and improvement of governance practices in the public service; Service delivery and compliance evaluations for promotion of service delivery through public participation and monitoring of quality audits; and Public Service investigations where the PSC has to undertake audits and investigations into public administration practices and promotes a high standard of ethical conduct among public servants and contribute to the preventing and combating of corruption[79].

3.3.4 Functions of the PSC

The PSC should: promote the prescribed values and principles governing public administration in the public service; investigate, monitor and evaluate the organisation and administration and the personnel practices of the public service; propose measures to ensure effective and efficient performance within the public service; give directions aimed at ensuring that personnel procedures relating to recruitment, transfers, promotions and dismissals comply with the constitutionally prescribed values and principles; report in respect of its activities and the performance of its functions, including any finding it may make and directions and advice it may give; and to provide an evaluation of the extent to which the constitutionally prescribed values and principles are complied with.

As part of monitoring anti-corruption initiatives, the Public Service Commission (PSC), a wing of the Department of Public Service and Administration (DPSA), assessed the most common manifestations of corruption and their related risks in the Public Service. Assessment was based on the total number of cases (7766) that have been reported to the National Anti-Corruption Hotline (NACH) since its inception in September 2004 to 31 June

---

[78] The mandate of the PSC as obtained from http://www.psc.org.za/press_atatements/2011/20110420.asp

[79] Key Performance Areas of the PSC as obtained from the above website (foot note 78).

2010. The assessment was aimed at raising awareness on common manifestations of corruption and to determine high risk corruption areas and to propose solutions to manage them. The PSC found that common forms in which corruption manifests itself are fraud and bribery (1511), mismanagement of government funds (870), procurement irregularities (720), and appointment irregularities (627)[80]. This information serves as proof that the SA government has delegated the Anti-Fraud Strategy down to its departments.

3.4 The DOD and the Anti-Fraud Strategy

The DOD, as a government department, is constantly in the limelight with allegations of corruption and fraud[81]. This is not the kind of publicity needed by the organisation that the country has to rely on for its security. As a result, DOD is represented in the workgroup that developed the Public Service Anti-Corruption Strategy as well as the National Strategy. The DOD's Anti-Corruption strategy is aligned with the Defence Inspectorate Division, the existence of which is based on the prescripts of the Defence Act, Public Finance Management Act (PFMA), Public Service Act and Treasury Regulations (TRs) and serves to provide internal audit, inspection and forensic investigation functions to the Head of the Department as part of the control system in the DOD[82]. The Directorate Anti-Corruption and Anti-Fraud (DACAF), a wing of the Defence Inspectorate, has formulated and developed an anti-fraud strategy and plan for corruption and fraud prevention. The strategy is currently being reviewed. The final product will incorporate the Anti-Corruption and Anti-Fraud policy, the Whistle Blowing Policy and the DACAF Quality Manual.

3.4.1 Anti-Corruption Policies

Two key documents used in promoting an anti-fraud culture are the Policy Statement and Fraud Response Plan, as emphasised in the HM Treasury Fraud Reports (2003; 2007). These documents are considered to be the minimum requirement for any organisation in managing the risks of corruption and fraud. Anti-fraud policies should make it absolutely clear to all those who seek to defraud the government that such behavior/action is unacceptable and will

---

[80] Information obtained from http://psc.org.za/press_statements/2011/20110420.asp about the National Anti-Corruption Forum Civil Society Indaba held on 23-24 June 2011 in Cape Town, with the aim to address aimed to address challenges encountered by Civil Society sector in effectively coordinating its activities within the National Anti-Corruption Forum.

[81] The DOD position as described in the Anti-Fraud Strategy and Plan for the Department of Defence.

[82] Information about the office of the Inspector General is extracted from the Policy on Internal Audits, Inspection and Anti-Fraud in the DOD, Pretorious: 2001.

not be tolerated, an element missing in the DOD documents which shall be addressed in chapter 7. There are international organisations which could help countries, especially developing countries, in fighting against corruption and fraud. These are the International Organisation of Supreme Audit Institutions (INTOSAI), which is the worldwide federation of Supreme Audit Institutions (SAIs), and the Global Programme against Corruption (GPAC), launched by the Centre for International Crime Prevention (CICP) in 1999. While INTOSAI offers some strategies and ideas for improving SAI performance in detecting fraud and corruption[83], GPAC aims to upgrade and enhance the capabilities of government and civil society in their fight against corruption. It helps to design and implement National Integrity Strategies and anti-corruption action plans. GPAC has developed an evidenced based inclusive, non-partisan, comprehensive and impact oriented approach to its advisory services. It promotes wide usage of the *United Nations Manual for Anti-Corruption Policy* and the *United Nations Anti-Corruption Toolkit*, the two instruments aimed at guiding policy makers and practitioners at national and municipal levels[84].

According to INTOSAI, exposure to corruption and fraud can be mitigated if a government has a set of relevant anti-corruption policies for government and assists in the development of anti-fraud programs. Whilst on anti-corruption programs, it would be appropriate to mention that South Africa is currently failing in terms of management of anti-corruption programs. Political parties were taken aback and infuriated by the PSC in Cabinet when it reported that two thirds of the 7 529 cases received via the National Anti-Corruption Hotline went missing[85]. Failure to manage hotlines properly leads to the conclusion that setting up hotline was a fruitless activity wasting taxpayers' money. This kind of management failure may impact on future whistle blowing.

It should be borne in mind that the NAH may be preferred for reporting allegations for various reasons, for example: members who have no choice due to the fact that their departments have not established such structures yet; members whose grievances were not addressed willingly by their own departments; taxpayers not employed by the government but

---

[83] It is maintained in that the SAIs can test compliance with policies such as these to determine if the government has enabled an appropriate anti-corruption and antifraud regime to be set up throughout and audited by SAIs.

[84] The role of GPAC as obtained from the United Nations Office for Drug Control and Crime Prevention Manual: 2001.

[85] Kotlolo & Mabuza: 2011 hold that according to the report by the PSC, allegations received concern various government and recommendations were submitted to affected departments but feedback received was only on 36% of those cases.

observe wrongdoings by the government employees; and more importantly, concerned and frustrated members for whom NAH is the last resort. These members are looking up to the PSC to come to their rescue in terms of the maladministration and unfairness they experience daily within their work environments. In attempt to remedy the situation, the SA President decided to change the phase of cabinet via reshuffling, whereby seven ministers and two deputy ministers had to vacate their offices, based on demonstration of poor performance. This was done with the hope that those replacing them will "intervene and stabilise departments and several crisis ridden public entities"[86].

DACAF final policy document will address processes and procedures to be followed within the DOD with regard to corruption and fraud prevention; assignment of responsibilities and prescription of procedures with regard to information disclosure (Whistle Blowing); co-operation and assistance between DACAF and all relevant role players; progress monitoring of incidents/cases referred by DACAF to other role players in order to compile and distribute fraud and prevention reports. Under the current organisational structure, DACAF powers and functions include: the development and maintenance of strategic direction (including policy and standards) to ensure the effective prevention and investigation of corruption and fraud; to ensure excellence in service delivery; to serve as the nodal point for forensic audits on behalf of the DOD. However DACAF must still design and include, in their policy, a similar policy statement as that in Appendix B – Policy Statement. This will help emphasise the importance of DACAF existence as well as their seriousness striving for a DOD free of corruption and fraud.

3.4.2 Whistle Blowing

Organisations should make more efforts to encourage "insiders" to provide information and for this purpose those insiders' protection is essential. The success of a hotline program depends upon the willingness of individuals to report what is believed to be acts of fraud, waste, abuse and mismanagement within government. Such individuals are more likely to provide information if they are allowed to report anonymously or be assured that their names will be held in confidence by investigators[87]. Although the South African government has already taken initiative with regard to the establishment of hotlines within government

[86] The Gauteng Provincial Government's cabinet is reported to have been put on hold due to the Gauteng Premier's resistance to the idea.

[87] The hotline needs a formal policy against retribution and reprisals. Access to the source of information needs to be limited and controlled in order to protect sources, Corruption and Fraud Detection by Supreme Audit Institutions: 2001.

institutions, much still has to be done in terms of implementation and management of those hotlines. The Public Anonymity is one of the most important features of a hotline; it is therefore important to protect, if requested, the person who makes a call. Internal operations policies and procedures should be developed to ensure the protection of the source's identity. It is critical to ensure that hotlines are not abused. Disgruntled employees can provide damaging information to a person who may have caused the caller some distress. To avoid misuse of hotlines, they must be designed in a manner that sorts the wheat from the chaff, in order to allow follow-up of only legitimate issues. The system should be designed in a way that ensures that complaints are not fictitious or frivolous. Psychologically designed questions help auditors focus on legitimate claims. *Brown envelopes*, whose authors could not be traced back, were often used for whistle blowing in the past. In many cases the whistle blower simply spoke out to authorities. Speaking out has led many whistle blowers to be punished, as will be discussed in the next topic.

3.4.3 The Risk of Whistle Blowing

The practice of whistle blowing should institutionalised and should include whistle blowing protection. We are given a scenario in support of whistle blower protection of an employee (whistle blower) who, in his attempt to bring his concerns to his supervisors was demoted for his efforts. The whistle blower went over the heads of supervisors, taking his evidence directly to the Court of Auditors. Although he was disciplined by his supervisors and lost pay, his evidence was eventually supported and many senior officials had no choice but to resign. In another incident, the whistle blower who reported allegations that the European Union (EU) accounts were open to fraud, found herself facing discipline charges by the EU. As a result, the whistle blower got suspended from her post as Chief Accountant after publicly declaring that the Commission's accounts were faulty and open to fraud and abuse[88].

According to the whistle blower, there was "very little documentation to support contracts", (lack of control measures) "no check up on accounting information" (lack of supervision), "missing progress and final reports" or simply "no contract files" (removal of evidence as coined in reports/files). The whistleblower claims he was threatened with reprisals from his supervisor for having expressed concerns about the integrity of contract management within the sector. He testified that he was ordered to backdate contracts to match the dates as appearing on requisitions, that appropriate signing authorities were not adhered to, and that

[88] Cutler: 2007 sharing experiences on the dangers of whistle blowing.

financial authorities had not been received from the client at the time contracts were issued. While the whistle blower was raising issues of contract manipulation and management concerns, he did not allege any illegal activity. He identified that issues were systemic in nature and warranted further examination. After he brought his concerns to the attention of his supervisors, his salary was frozen and he was no longer promotable. Eventually, the auditor general reviewed his concerns and Cutler was vindicated. He successfully ran for Parliament in the next election[89]

3.4.4 Protected Disclosure Act

Whistle blower protection is essential in order to encourage people who are often aware of corrupt activities by co-workers but are frightened to report them. Experience is said to be the best teacher. Should people have experiences of the dangers of whistle blowing, they feel they rather turn a blind eye not to lose jobs or lives. Most people have disappeared without a trace, some brutally killed, and some lost their jobs for trying to do what is right. However, it has been observed that the existence of whistle blower laws alone is not sufficient to instil trust in potential whistle blowers. Disclosures by whistle blowers must be treated objectively and even if they prove to be inaccurate or false, the law must apply as long as the whistle blower acted in "good faith". It must also apply irrespective of whether or not the information disclosed was confidential and the whistle blower therefore might have breached the law by blowing the whistle[90].

In South Africa, the Protected Disclosure Act (PDA) , 26 0f 2000, which came into effect in February 2001, aims to provide protection to those employees who, in good faith, blow the whistle on corruption or wrong doing in terms of this Act[91]. Although hotlines are intended to encourage people to blow the whistle, there are a number of policy issues in relation to such hotlines, including the danger that they will provide a "cloak for the malicious". It should be noted that the operation of the PDA is triggered by an occupational detriment, such as harassment or dismissal, and not by the disclosure. Therefore, for a whistle blower to

---

[89] Experiences discussed here about problems encountered for whistle blowing were mentioned in attempt to emphasise the need to have those who punish whistle blowers punished. There should be somewhere the whistle blower runs to for help and justice should ultimately be done.

[90] The UN Anti-Corruption policy: 2001maintains that whistle blowing is a double-edge sword, it is necessary to protect the rights and reputations of persons against frivolous or malicious allegations

[91] It is maintained in the PSC Report: 2002 that the concept underpinning the Protected Disclosure Act is that prevention is better than cure, and that raising concerns at an early stage privately to their employer is more likely to lead to remedial action being taken. The question here is, what if the supervisor befriends the corruptor/s or is corrupt.

attract the PDA's protection, he or she has to reveal his or her identity in order to say to the court "I blew the whistle and I suffered occupational detriment as a result". This implies that it is not possible for an anonymous whistle blower to attract the protection of the PDA without losing their anonymity, unless at the persons making confidential telephone calls are prepared to reveal their identity at that point in time. Would that still be an anonymous/confidential hotline[92]?

Fear of occupational detriment, including lack of proper action taken against some perpetrators (employers), are the most likely reasons why whistle blowers would want to remain anonymous. A survey carried out among public officials in New South Wales, Australia, regarding the effectiveness of the protection of the Whistle Blower Act, proved that laws alone will not encourage people to come forward. Findings reflect 85% of the respondents were unsure about either the willingness or the desire of their employers to protect them. 15% stated that they would refuse to make a disclosure due to fear of reprisal[93]. Disclosure by whistle blowers must be treated objectively and even if they prove to be inaccurate or false. The law must apply irrespective of whether or nor the information disclosed was confidential. Since whistle blowing is a double-edged sword, it is necessary to protect the rights and reputations of persons against frivolous or malicious allegations.

3.4.5 Disclosure of Assets

Excessive assets, income, gifts and liabilities are all indicators of irregularities when they are out of proportion to one's earned salary. Therefore, the disclosure of assets is another effective measure to enhance accountability and integrity of public servants. Transparency of accumulated assets/liabilities and of gifts to government serves as a deterrent to elicit enrichment through corrupt practices. Disclosure of assets/liabilities can assist in the investigation of corruption allegations and may provide evidence for subsequent prosecution.

It is essential for the disclosure to be made upon entry into the public service, and should therefore be updated regularly. The monitoring of these assets declarations and their accuracy should be performed by an independent agency such as an ombudsman, inspector general or an anti-corruption agency. Even though it is unrealistic to expect that laws requiring

---

[92] It is important that Awareness trainers highlight whistle blowers about this clause, so they can make informed decision regarding anonymity.

[93] The United Nations Office for Drugs Control and Crime Prevention: 2001 maintains that the whistle blowing law should contain minimum measures to restore a damaged reputation. Criminal codes should contain provisions supporting/protecting those who knowingly come forward with false allegations because of the costs incurred on investigating false allegations and restoring damaged reputation.

disclosure of illegal financial gains by officials will result in voluntary confession, laws or regulations requiring comprehensive disclosure will provide a basis upon which to monitor unearned income and could provide a basis for prosecution. To be effective enough, penalties for non-disclosure or false reporting must be severe enough to act as a deterrent.

Looking at the South African *Draft policy on Civil Servants*, under the "Department of Public Service and Administration's Public Service Integrity Management Framework, which, according to Majavhu: 2011, has stopped short of banning government officials from owning shares in companies that do business with the state[94]; one questions the intentions of government to fight against corruption and fraud. It is apparent that the aim of the draft policy would be viewed as protecting most corrupt officials who get busted. Hence provision has to be made at higher level, for corruption and fraud to take place in an official manner. This reveals the failure of the South African government to learn from practices of other countries. This also serves as proof that there is a lack of participation by the Public Service Leadership in international forums engaged in the fight against corruption and fraud. The "Draft" is said to have been presented to parliament in August 2011 and it is hoped for Cabinet to give a nod by the end of the year. Giving a nod to such a draft by Cabinet would imply that Cabinet promotes corruption and could ruin the government reputation; it would also open doors for uncontrollable corruption and fraud that will lead to increased poverty amongst SA communities. A further refinement of disclosure should relate to disclosure laws governing political financing. This could be useful for compelling candidates or political parties to reveal contributions received. This would permit the voting public and the media to react to those contributions as soon as they are made public.

3.5 Hotline Requirements

3.5.1 Ethics Programs and Hotlines

Two effective programs that can advance a fraud prevention agenda are ethics programs and hotlines. The DOD has established an ethics program in order to help employees make correct ethical choices relating to environmental legal and social decisions. As a national department with many employees, it would be advisable for a professional ethics Officer employed within DACAF in order to have a link between DACAF and the DOD Directorate for Ethics, since an ethics program is said to address corruption and fraud in a comprehensive

[94] Majavhu: 2011 states that the policy will apply to any employee of a municipality, provincial or national government departments.

fashion that goes beyond a simple code of conduct[95]. The Public Service Commission has instructed departments to address issues regarding appointments of ethic officers within their work environments. Though courses, policies, ethics call lines and other means, such programs align bureaucratic practices with organisational values and beliefs. One effective deterrent to fraud is a strong perception of being detected. A complaint or tip hotline can help strengthen the perception of detection, as calls are monitored and acted upon. It is also critical to ensure that hotlines are not abused. To avoid misuse of hotlines, DACAF may seek psychologically designed questions in order to help investigators to focus on legitimate claims. Much effort has to be made in designing the system to ensure that complaints are not fictitious or frivolous.[96]

3.5.2 Hotline Staffing

The number of personnel required to staff a hotline office will depend upon the known or an anticipated number of complaints that will be received during a given period of time and the requirements established for handling allegations/complaints received. A staff complement for a national department (such as SANDF), which might receive 800-211 200 telephone calls and contacts letters a month, might consist of: staff who receive, evaluate process and refer for examination those matters that warrant such action (4); staff assigned to review and analyse reports of investigation received from the examining agencies to ensure each complaint has been properly examined and corrective, if warranted, taken by the responsible officials (3); staff involved in operations analysis and the conduct of field quality assurance reviews (2); Staff for administrative requirements (4); and staff for management and supervisory functions[97].

DACAF has always been faced with the problem of being understaffed, for example, some posts (in all DACAF sections) have been vacant for more than two years now without being filled; it's been over 2 years now that plans were made to recruit an additional member to help receive, evaluate, process and refer for examination those matters that warrant such

---

[95] Dye addresses ethics issues on ethics programs in his title "Corruption and Fraud Detection by Supreme Audit Institution.

[96] Outsourcing the phone line to a third party vendor provides an added benefit of ensuring that there is no organisational bias in its operation.

[97] An inability to provide adequate personnel support may result in "burnout" due to excessive workload. International experience has shown that staff members could not adequately handle more that 8-10 substantive calls in an 8-hour day. Over an extended period of time, hotline staff exhibited evidence of nervous strain, inaccuracy in reporting details of the interview, as well as not being efficient and tactful in handling telephone sources, PSC Report: 2002.

action. Factors contributing to the problem of understaffing are: a long process involved in staffing of Public Service Act personnel; divisions supply DACAF with uniform members but career management for those members lies with those divisions, DACAF is not informed on time when those members have to leave for promotional purposes or for any other reasons; it takes time for DACAF to request replacements or it takes time for those units to replace members who vacated the posts. DACAF is also affected by a huge volume of calls received especially after training by Awareness officials. Most of the calls are related to personal problems experienced by members in their various working environments. These problems are supposed to be addressed by the Inspector General's Complaints Office. This Office is currently non-functional. Members have already lost faith in DACAF since DACAF only addresses corruption and fraud related matters but has nowhere to refer their matters to.

3.5.3 Equipment Requirements

The appropriate equipment depends on the volume of calls expected as well as the availability of funds. The hotline is said to require a multi-line telephone instrument and a separate dedicated number, to ensure that both government employees and the general public have cost free, easy access to the hotline. DACAF has a toll-free number and machine to record messages after hours thereby providing the opportunities to leave messages regarding reports to be made. The problem experienced by DACAF regarding this machine is highlighted in the PSC Report (2002) where it is maintained that the use of recorders to take complaints during non-operating hours is not recommended since recorded complaints normally lack the detail required to support the initiation of a formal enquiry. Most callers are not aware of what information is required for such matters and generally provide data only when prompted by a trained, experienced investigator. This leads to loss of potentially valuable investigations since there is no way those sources can be re-contacted, unless they chose not to remain anonymous[98].

Also important to equipment requirement is a computerised management system for recording incoming complaints. The UN Report (2001) maintains that incoming complaints should be entered into a computerised management system that allows for the analysis and monitoring of the complaints; tracks the allegations reported; action taken; outcome of any investigation and resulting disciplinary and court proceedings. Information retrieved from a

---

[98] What is suggested in the The PSC Report: 2002 is that hotlines be managed by trained, experienced investigators.

computerised system should help managers track fraud investigations with the following: the number of investigations carried out; value of fraud loss identified; duration of individual investigations; costs of individual investigations; methods of investigations used; and outcome of investigations[99]. The DACAF system does not have all these capabilities and should therefore be revisited in order to ensure that it is designed to meet these requirements; the reason being that the missing capabilities seem to answer for what managers normally look for. Currently, DACAF uses the spreadsheet in order to cater for the missing capabilities.

3.5.4 Detection Investigation

There is a unique relationship between parties involved in corruption and fraud crimes and, in some instances, this relationship prevents authorities from knowing that a crime has taken place. Neither party is going to report the crime. The inherently covert and consensual nature of corrupt activities makes it difficult to obtain information on instances of corruption. The deterrent effects of investigation and prosecution and the direct incapacitation of wrongdoers by their removal from office and incarceration can reduce corruption in the government, but challenges exist in developing a flow of information to overcome the inherent secrecy of corruption offences. Yet virtually, all practitioners involved in anti-corruption efforts would concede that, no matter how draconian or rigorously enforced the penal measures might be, no society could realistically punish more than a small proportion of the officials who abuse their positions. If the level of integrity in government is to be improved, it will be by managerial, administrative and reporting mechanisms[100].

The existence of a response plan may, in itself, help to act as a deterrent since the presence of a response plan shows that an organisation is prepared to defend itself against the risk of fraud. The DOD is currently revising its anti-fraud policy; the fraud response plan and the whistle blowing arrangements. The aim of the DOD response plan is to ensure that timely and effective action is taken to: prevent losses of funds or other assets where fraud has occurred and to maximise recovery of those losses; minimise the occurrence of fraud by taking rapid action at the first signs of the problem; identify fraudsters and maximise the success of any disciplinary/legal action taken; minimise any adverse publicity the organisation suffered as a

[99] The National Audit Report: 2008 adds that Departments also need to look at whether the total number of investigations is commensurate with the potential sums lost from fraud. The cost of investigating cases can be resource intensive. Assessing the financial return achieved on the overall case load, and different categories of cases will indicate the likely benefits of undertaking more investigations or a different mix.

[100] The covert and consensual nature of corruption as described in the UN Office Report: 2001.

result of fraud; identify any lessons which can be acted upon in managing fraud in the future; and reduce adverse impacts on the business of the DOD. All these are achieved through the engagement of investigators.

3.5.5 Awareness Training

Raising awareness training is considered integral to the development of a culture that is receptive to attempts to fight corruption and fraud. It is important for an awareness–training program to include dissemination of the negative impacts of corruption and the expected behavior on the part government collectively and its officials individually. However, curbing corruption in a systemic corrupt environment is said to take time and considerable effort. One of a few existing success stories reads: "Having fought corruption for the past 25 years, Hong Kong's Independent Anti-Corruption Commission (ICAC) continues to allocate substantial financial and human resources in its effort to build integrity to prevent corruption, spending US$ 90 million (1998) per year and employing 1 300 staff who in 1998 conducted 2 780 training sessions to strengthen partnership between anti-corruption agencies and private and public sector. ICAC, in so doing, interfaced, on annual bases, directly with close to 1% of the population"[101]. It is very important for countries to learn from success stories of others and follow their steps or come up with own strategies, rather than being too lenient by developing policies that counter attempts to curb corruption and fraud.

3.6 DOD Structures

3.6.1 Internal Structures

Co-operation and assistance, as stipulated in DACAF Anti-corruption and Anti-Fraud Draft Policy[102], is ensured between DACAF and all role players in attempt to prevent corruption and fraud. Internal role players are:

- DOD Chief of Finance: The DOD abides by the prescripts of the Public Finance Management Act, Act No 1 of 1999. The Chief of Finance ensures that every official of (DOD) is being held responsible for the management, including safeguarding, of

[101] A warning is hereby given that raising awareness without adequate enforcement may lead to cynicism among the general population and actually increase the incidents of corruption. Citizens who are well informed through the media about types, levels and location of corruption but who have few examples of reported cases where perpetrators are sent to jail, might be tempted to engage in corrupt acts where "high profit and no risk appears to be the norm. It is therefore essential for any anti-corruption strategy to balance awareness raising with enforcement.

[102] There is no indication in the Draft Policy that DACAF joins forces with international organisations.

the assets and management of liabilities within that official's area of responsibility[103]. The Chief of Finance ensures that losses and damages the State has suffered through criminal acts or omission are recovered.

- The DOD Legal Services: provides professional, legitimate and deployable military services; has as its mission to ensure an effective , professional, and comprehensive military legal service and support through the participation of law and principles of justice, taking into consideration issues such as transparency, communication and transformation imperatives of the DOD; and provides legal support to democratic peace-support operations in Africa.
- Military Police: Command and Control rests with Chief of the Military Police Agency (MPA); responsible for the control, management, and general administration of the Military Police (MPs) Office. The MP is the only structure within the DOD with powers to arrest and detain. The MP manages matters where there is criminal intent or negligence.
- Defence Intelligence (DI): The Defence Act, Act 42 of 2002[104] states that DI must gather, correlate, evaluate and use strategic intelligence. As put by Smuts: 2001[105], the Chief Intelligence (Sub-Division Counter Intelligence) C Def Int (SDCI) must: determine Information and Communication Systems Security (ICSS) threats; evaluate compliance with ICSS policies; Investigate any event or situation that has compromised or may compromise the security of the DOD, etc. Liaison is made with the MP and the South African Police Services (SAPS).

Liaison is made by DACAF with the MPs and the SAPS regarding cases with criminal elements such as corruption, and fraud, forgery, and theft of assets and other resources. There are many other anti-corruption structures (subsystems) at divisional and unit level. These subsystems used to operate in isolation. DACAF has currently been appointed as a nodal point and is currently trying to incorporate these structures for acknowledgement and integration purposes. The existence, functionality and effectiveness of these many substructures become questionable when the DOD has to be among departments facing the media with incidents of corruption and fraud. Moreover, the approval of the Strategy in 2002

---

[103] Calmeyer & Sullivan: 2000 on the instruction promulgated jointly by the Secretary for Defence and the Chief of the SA National Defence Force, the policy that must be implemented by the Chiefs of Services and Divisions and executed down to the lowest applicable levels of command and management.

[104] The Defence Act is the deciding factor and offers prescripts on what the DOD should do.

[105] Smuts: 2001discusses the role the Defence Intelligence plays on part of information and Communications.

by the National Cabinet for departments to establish the requisite capacity to prevent and combat corruption and fraud in their spheres of operation sounds fruitless when one analyses what transpires currently within government departments.

3.6.2 External Structures

External Role Players include: the South African Police Services (SAPS); the Commercial Crimes Investigations Unit and the South African Police Services Criminal Records Centre (SAPS CRC) where complicated corruption and fraud cases are referred due to lack of expertise and capabilities within the DOD; the Public Service Commission (PSC), the Auditor General (AG); the State Information Technology Agency (SITA), which assist DACAF with information where corruption and fraud has been committed via computers systems are involved; DACAF shall attend the National Anti-Corruption Forum (NACF) and the Anti-Corruption Co-ordinating Committee (ACCC) meetings under the chairmanship of the Department of Public Service and Administration (DPSA). DACAF shall supply top management with information directly as and when needed. Decisions and instructions from NACF are binding: this is the forum where government intensions, instructions and directions are communicated. These forums form a link between Cabinet and the rest of government departments[106].

It is evident that the DOD is not the only department faced with corruption. An article by Majavhu (2010) highlighted "the R3m spent on mismanagement probe" where almost R3 million was spent since 2007 on investigating alleged mismanagement of funds. Whilst one forensic investigation involved money spent in Culture, the other investigation concerns the R150 million allocated to the Cultural Development and 2010 Soccer World Cup projects, which has been reported to have gone missing. The department is said to have failed to reveal the results of a forensic audit into mismanagement at the Robben Island Museum (RIM)[107]. In an article by Dlamini (2010), the PSC quoted the Justice Department to be the most corrupt of them all[108]. One wonders where South African departments are leading, when the Justice Department, established to protect the public and enforce law and order, is referred to as excelling in activities of corruption, fraud, financial mismanagement, theft, misappropriation, abuse and gross negligence by the PSC. While the Justice Department was ranked the

---

[106] All requests for external or forensic audits shall be forwarded to DACAF, which shall serve as the facilitator throughout the whole process.

[107] The RIM Chief Executive resigned, while the Procurement Manager and Chief Finance Officer were fired.

[108] An article by Dlamini: 2010 ranked departments by activities of corruption and fraud.

highest, followed by Home Affairs, Defence Department came out third, followed by the Social Development. It's been reported that in 273 out of 1 204 cases, government departments failed to provide indications whether criminal or any other proceedings were instituted against employees charged with financial misconduct and nothing has been said about recovery of losses.

3.7 Computer Fraud within DOD Systems (FIN, HR, VMS)

It is unfortunate that computers are used as tools through which fraud is committed. The DOD structures fighting against corruption and fraud were discussed in previous paragraphs. Some of the incidents these structures deal with occur as a result of the fact that some employees know that: there are different vehicle management systems (VMS) and these systems do not talk to each other; vehicle management systems are not linked with Human Resources (HR) systems; and that both VMS and HR systems are not linked to the Finance (FIN) systems. Moreover, perpetrators are aware of the weaknesses in DOD internal controls. Some of the problems experienced within the DOD, as extracted from whistle blowing reports as obtained from the DACAF database, are discussed below:

Fleet Management: employee fraud, which occurs when some organisation employees use their official positions to misuse or steal organisational assets or resources, should be managed in a more integrated and effective way. The DOD experiences, within the area of fleet management, incidents such as: theft of vehicles; unauthorised private use of vehicles; theft or substitution of accessories or tools; falsification of vehicle log; use of petrol for private vehicle; and misuse of vehicles. Other activities include misuse fraudulent activities regarding: automobile mileage reimbursement fraud; attainment of fraudulent drivers' licenses; expense account and travel reimbursement: these activities occur mostly via submission of: altered receipts; personal expenses as business related; receipts from closed or nonexistent establishments.

HR Systems: fraud experienced concerning activities around this core function is often perceived to be the result of internal manipulation by one or two employees for personal gain. Taking on many forms, elements of fraud include acts such as: forgery, deception, false pretence, false accounting and identity fraud; and they may require constant attainment of fresh personal identities by common theft or documentation, forgery, and coercion. Members whose identities are stolen find it difficult to resolve such matters, prove their innocence and restore their good names. Investigated incidents regarding most illegal deductions made

against salaries of most DOD new recruits reveal companies such as those offering funeral and insurance policies. In other instances, member identities are used to buy houses or motor vehicles. Investigators experience difficulty in tracking companies doing business or with the DOD, or in other instances, find some companies to be non-existing. Where such companies do exist, supporting documents do not prevail. It is also difficult to stop such deductions.

Finance systems: corruption and fraud activities occur where employees knowingly access computers without authorisation in order to: intentionally engage in fraudulent activities; conduct illegal transfers of funds; knowingly access a protected computer; and intentionally defrauding by creating fictitious accounts such as those of companies and employees. It should be noted that operations within VMS and HR have a direct impact on Finance. It is therefore important to ensure that systems within these core functions get integrated. The fleet software, for example, should be able to flag up fraud on the dashboard of the fleet management system as it links to the organisation's HR database in a way to prevent potential fraud from occurring. It is also important for the fleet department to work closely with HR, so that changes to employee records are instantly communicated to the relevant managers, including fleet and finance. The solution should also allow for full history audits on almost any document or posting. Where money is involved, it would be easy to see who made changes and follow up on them. It is in this regard that application integration is necessary.

3.8 Conclusion

It should be noted that even the most secure Government departments can be susceptible to computer fraud: fraudsters endeavour to be as successful at fraud as organisations are to succeed in their legitimate operations. As a result organisations are still ill-equipped to prevent it from happening, even with heightened awareness of fraud. To curb corruption and fraud, organisations have to walk a fine line between allowing enough slack so that employees are able to do their jobs while maintaining a level of control needed to stop internal fraud. The next chapter introduces Electronic Commerce which requires organization entities and countries to work together to remove barriers in order to promote free flow of electronic products and services via application integration as well as to solve accompanying problems such as application integration and corruption and fraud occurring in business monetary/pecuniary transactions.

Chapter 4
Electronic Commerce as Vehicle for Combating Fraud

4.1 Introduction

The subject of e-commerce was introduced in this study since fraudulent activities performed via computers form the theme of this research. Electronic Commerce (E-commerce) facilitates the integration of innovative applications and services with private and public information infrastructures; thus providing enterprises with a sound basis to achieve higher levels of integration, efficiency and cost-effectiveness. Integration is required due to the fact that the movement of materials, services and end products is no longer executed by single divisional functions, but increasingly, through a single and seamless cross-company process; the concept involving the integration of many elements of technology, infrastructure, business operation, processes and public policy. It highlights the importance and need for faster adoption by individuals, enterprises and governments.

4.1.1 E-commerce Definition

Whilst given a broad definition of e-commerce by the Department of Communications (DOC): 2000 as: "The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses; between businesses themselves; between individuals themselves; within government or between the public and government; and between business and government"[109], Laudon & Laudon (2004) maintain that "e-commerce as the part of e-business that deals with the buying of goods and services electronically with computerised business transactions, using the Internet, networks, and digital technologies". It also

[109] The DOC: 2000 states that this definition encompasses the many kinds of business activities that are being conducted electronically, and conveys the notion that electronic commerce is much more comprehensive than simply the purchasing of goods and services electronically.

encompasses activities supporting those market transactions, such as advertising, marketing, customer support, delivery, and payment[110].

The arrival of widespread networking from Local Area Networks (LANs) to the Internet entered us in a fourth era, where computers begin to look more like information appliances: mere access points to a vast array of services available to all with minimal computing literacy. E-commerce and entertainment has just begun and it is not known yet whether this era will lead to another qualitative identity change into a fifth era of the global e-village. According to a historical perspective given by Hirschheim & Klein (2003), as IT evolved, it has clearly influenced the IS profession. IT is neither the root cause nor the technological fix for the structural patterns which lie at the base of the "crisis". The off-shoring disconnects, and internal communication gaps are not caused by IT, but there is one misconception: "as the IS field embraces technical specialisations, the widely recognised rapid change and proliferation of technology encourages ever finer divisions of labour and with this comes more and more rapid social differentiation contributing to the communication gaps. Otherwise, IT has an enabling mediating role in the underlying patterns[111].

4.2 An International Perspective

The global availability of the exchange of transactions between the buyers and sellers has fuelled the growth of e-commerce. The United States (US) has retained leadership in software innovation in two key technical areas. First is the structure of the "stacks": the industry standard interfaces that define key architectural elements of many systems such as network protocols and principal e-commerce application programming interfaces (APIs) including the frameworks. Second, is the set of core technical and design concepts for many of the infrastructural elements of the architectural stacks on which systems are built, which define the conventional interfaces and elements, generally in the form of de facto industry standards that exist within major complex systems and they include key system frameworks and libraries, as well as the languages, tools, standards, and quality assurance technologies used

---

[110] Laudon & Laudon: 2004 maintain that by replacing manual and paper-based with electronic alternatives, and by using information flows in new and dynamic ways, e-commerce can accelerate ordering, delivery, and payment for goods and services while reducing companies' operating and inventory costs.

[111] From a historical perspective, the discipline that at first used to be called data processing, (DP), then Management Information Systems (MIS), and later Information Systems (IS), has been undergoing another subtle name change to IT, particularly in industry, Herschheim & Klein: 2003.

in systems development[112]. There is a great drive towards coherency and condensation of selective developments in international forums whereby there are specific views and activities by each organisation on various areas of e-commerce.

4.3 The South African E-Commerce Policy

The South African government became enthusiastic about making government more accountable to citizens by creating a more efficient and effective government that facilitates more accessible services and allows greater public access to information. The enthusiasm was displayed by the establishment of a policy framework for e-commerce: an indication that South Africa (SA) has recognised the important role played by ICT tools for reform and transformation. The first step taken by the SA government was the development of the "Green Paper on E-commerce: 2000" which was co-ordinated by the Department of Communications, intended at "providing a platform from which to translate topical issues around e-commerce into government policy"[113]. The South African government sees its role as an enabler, facilitator, educator and law enforcer to prevent cyber crimes and model user of e-commerce. While acknowledging that e-commerce provides new opportunities for business, the government is also aware that it also brings with new threats such as electronic fraud and cyber crime. According to a Green Paper on e-Commerce (2000), these threats form part of the topical issues which, because they are experienced internationally, were subject to negotiations of agreement and to treaties in international forums by government.

4.4 Categories of E-commerce

There are four types of e-commerce, namely: Business-to-Business (B2B), for business integration and involving XML-based Web applications that can enable business integration[114]; Business-to-Consumer (B2C), is regarded as extremely fragmented and problematic, and it is said to operate most efficiently where there is a high density of delivery

---

[112] A leadership position of the US in software innovation as offered in a "Letter Report" by the National Research Council: 2002, obtained from http://www.nap.edu/catalog.

[113] Topical issues revolving around e-commerce policy formulation as highlighted in a Green Paper: 2000, include legal issues such as admissibility of electronic evidence, authenticity and integrity of electronic communications, writing and signature, etc.

[114] Malhortra & Temponi: 2010 hold that some companies have adopted the XML hub prototype. Develop using widely applied web-based technologies; the hub architecture is applicable to smaller suppliers: the architecture is flexible, scalable, extensible and suitable networking environment.

and deliveries are made consistent and daily[115]; Government-to-Business (G2B) transactions include various services exchanged between government and the business community, including dissemination of policies, memos, rules and regulations where services offered include obtaining current business information, downloading application forms, renewing of licenses, registration of businesses, obtaining permits, and payment of taxes[116]; and Government-to-Consumer G2C), which includes information dissemination to the public, basic citizen services such as license renewal, ordering of birth/death/marriage certificates and filing of income taxes, etc. These types are represented in table 4.1.

Business-to-Business: integrating value chains- supplier and customer base	**Business-to-Consumer: on-line shopping**
Govt –to- Business: E-procurement	**Government-to-Consumer: Services and programs Government online**

Table 4.1 Different Types of E-commerce

Source: Department of Communications: 2000

4.5 Enabling Technologies

In order to conduct business transactions in a more cost effective and efficient way, a speedy access infrastructure should be available in order for e-commerce to succeed: The backbone network within should be of high quality and the price should be affordable. According to Friedman (2006), people should not fail to take advantage of e-commerce due to lack of infrastructure or education since the flat-world platforms makes innovation and production more efficient. The growth of e-commerce therefore rests upon broad and affordable access to infrastructure enabled by convergence of technologies, telecommunications policy, robust network infrastructure, sufficient bandwidth and support for targeted applications. This section deals with the infrastructure requirements for e-commerce which are divided into: infrastructure access, telecommunications and convergence. According to a Green Paper on

[115] The problem in the B2C market is the fact that the final delivery is a home delivery probably because a home delivery needs to be repeated several times as a result of absence of the recipient, therefore resulting in increased costs, Paschalidou: 2006.

[116] According to Paschalidou: 2006, the service offered through G2B transactions also assist in business development, specifically the development of small and medium enterprises.

E-Commerce (2000), the deployed infrastructure then, needed to be expanded into under serviced areas with the appropriate capacity, as well as increase the capacity in serviced areas

4.5.1 Infrastructure Access and Telecommunications

Giving people access to all the tools of collaboration, along with the ability through search engines and the Web to access billions of pages of raw information, is regarded as ensuring that the next generation of innovations will come from all over the Planet Flat[117]. The IT infrastructure is the shared technology resources that provide the platform for specific information system applications. Infrastructure necessary for the enablement of e-commerce consist of networks, end-user equipment and access services. The software and network infrastructures are equally important: software provides the bridge between the network infrastructure and applications.

Information and communication technologies required include facilities such as E-mail, Data Interchange Standards, Intranets Portals, etc, End-user and access devices include hardware and software which control access to services and handheld devices. The possibility of participating in the global electronic marketplace is limited by a lack of access and the cost of hardware. The infrastructure needed for e-commerce should have adequate capacity: it should be fast and reliable. However, it should be borne in mind that the more organisations attempt to counter threats, the more the perpetrators increase their skills and their success.

Based on the information given, it could be concluded that e-commerce includes the whole range of electronic commerce activities which are viewed as bearing the risks emanating from various sources, thus requiring protection: "*Information security* requiring that the information asset be protected from destruction or theft and the *e-commerce business* risk which could negatively impact on the well being of the organisation itself"[118]. Associate risks are discussed in paragraph 4.8 below. These are the risks against which organisations have to protect themselves. As a result, organisations have to integrate their systems and should, while developing and implementing their information strategies, include controls against corrupt and fraudulent activities.

---

[117] Friedman: 2006 refers to the convergence as a as a triple convergence of new players, on a new playing field, developing new processes and habits for horizontal collaboration.

[118] It is stated in an article named "Risk-E-Business": Assessing Risk in Electronic Commerce that "three of the most significant sources of risk that arise from developing and operating an electronic commerce strategy are said to be competitive, transaction and business partner risks".

4.5.2 Convergence

Convergence is understood to be the activity of integrating a number of services in a dynamic and scalable manner; however, the number of services to be integrated may be large and continuously changing. The activity of integrating a number of services constitutes an important part of this research, as it is suggested that integration of applications (services), as well as strengthening of controls will help improve efficiency, make better process control, shorten flow times, help make better use of resources and help reduce corrupt and fraudulent activities in organisations. One aspect of market convergence occurring within the telecommunications sector is that between fixed and mobile telephony mostly in developed countries. Mobile data networks, e.g. based on a series of radio towers constructed specifically to transmit text and data, transmit data to and from handheld computers, but, data cannot be transmitted seamlessly between different networks if they use incompatible standards[119]. Other barriers to the development of convergence on e-commerce are: access to users; regulatory restrictions on the use of infrastructure; prices for telecommunications services; availability of content; regulatory uncertainty; market entry and licensing; access to networks; access to systems and content; allocation of radio frequency and other resources; public confidence in new environment; and lack of supporting interoperability[120]. The impact of the new services resulting from convergence will be felt in the economy as a whole, as well as in the relevant sectors themselves, namely: telecommunications services and equipment; computer hardware; computing services; publishing; audio-visual services; and consumer electronics.

4.6 Benefits of E-commerce

Thomas Friedman (2006) states that the flattening of the world started with the falling of the walls; the opening of the Windows; the rise of the Personal Computer (PC); the spread of the Internet and the coming to life of the Web; and finally the emergence of the standardised processes for how certain kinds of commerce work should be conducted[121]. In support, a

---

[119] Wireless networks and transmission devices can be more expensive, slower, and more error prone than transmission over wired networks, although the major cellular networks are upgrading the speed of their services, Laudon & Laudon (2004).

[120] As e-commerce changes the ways in which enterprises work, produce and deliver; as traditional market boundaries blur; and as technology undermines the rationale for the monopoly privileges that are granted to many service activities, competition policy will have to address new types of anti-competitive practices.

[121] This is called the "Genesis" moment of the flattening of the world and all these developments, put together, breed the crude foundation of a whole new global platform for collaboration, Friedman (2006)

Green Paper on Electronic Commerce for South Africa (2000) maintains that e-commerce requires an open, predictable and transparent trading environment, which operates across territorial borders and jurisdictions. To foster such an environment and to realise its full economic potential necessitates international co-operation, which will be instrumental in developing the enabling conditions for its growth. Countries have to work together to remove barriers or impediments to the free flow of electronic products and services across jurisdiction and by resolving problems that may arise due to its borderless character. Government is shown to be the appropriate vehicle to ensure that this is made possible.

The Green Paper goes further to highlight the following benefits: improved response time and competitive positioning; ease at concluding deals and financial transactions; extended market research and thus increased revenue potential; increased consumer convenience and choice; reduced prices; and improved customer service[122]. Information systems play a major role in e-commerce. Laudon (2004) mention other positive impacts by information systems and say that: performing calculations or process paperwork much faster than people; can help companies learn more about the purchase patterns and preferences of their customers; provide efficiencies through service; have made possible new medical advances in surgery, radiology, and patient monitoring; and the Internet distributes instantly to millions of people across the world[123]. Distributed systems, for example, are intended to form the backbone of emerging next-generation communication systems, including electronic commerce, PCs, satellite surveillance systems, distributed medical imaging, real-time data feeds, and flight reservation systems. An obvious benefit of distributed systems is that they reflect the global business and social environments in which we live and work. Another benefit is that they can improve the quality of service (in terms of reliability, availability, and performance) for complex systems.

Although information systems have proven enormous benefits, they have also created problems and challenges managers are to be aware of. The HM Treasury (2001) puts it clearly that “Computer crime is on the increase and while key risk areas remain new dangers are emerging”. The Internet, and the adaptation of Internet philosophies to internal systems, will be the cornerstone of IT activity in the coming years. The dynamic nature of these

---

[122] Benefits of e-commerce as stated in a Green paper by the Department of Communications Republic of South Africa: 2000

[123] Laudon & Laudon: 2004 caution that to use the Internet and other digital technologies, organisations may have to redefine their business models, re-invent business processes, and change corporate cultures.

technological advances requires careful planning and management to maintain security and contain developing risks[124]. More problems are addressed in the next subheading.

4.7 Threats in the E-commerce Environment

E-commerce security is clouded by dimensions of: *Integrity,* which involves the ability to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorised party; *Non-repudiation*, which requires organisations to be able to ensure that e-commerce participants do not deny online actions to be displayed; *Authenticity,* which encompass the ability to identity the identity of a person or entity with whom you are dealing with on the Internet[125]; *Confidentiality*, which is the ability to ensure that messages and data are available only to those authorised to view them; *Privacy,* which requires the ability to control use of information a customer provides about himself or herself to merchant; and *Availability*, referring to the ability to ensure that an e-commerce site continues to function as intended. These dimensions are binding to each and every organisation engaging in IT adoption for e-commerce. However, there is tension between security measures that are added; the more difficult a site is to use; and the security versus the desire of individuals to act anonymously. Apart from the increasing demands on business partners, e-commerce brings along security threats within its environment.

Many new technologies have created opportunities for committing crime. Technologies, including computers, create new valuable items to steal; new ways steal them; and new ways to harm others. Illegal acts do occur through the use of a computer or against a computer system. Computer systems can either be the object of crime or an instrument of a crime. As e-commerce activities continued exponential growth in volume, there have been increasing demands on organisations to change ways in which they interact with customers, suppliers, and business partners. In order for organisations to remain competitive in e-commerce capabilities, it would seem crucial that they assimilate an organisational culture environment that promotes innovation, flexibility and risk-taking. The client, server and communications channel are said to be key points that are vulnerable towards the e-commerce environmental threats. The most common threats are malicious code and credit cards fraud.

---

[124] Internet has been used to manipulate computer software or data dishonestly, the HM Treasury: 2001 maintain that they have had 50 reports of disciplinary action taken in relation to IT misuse.

[125] Laudon & Laudon: 2004 state that

4.7.1 Hacking and Cyber Vandalism

While a hacker is an individual who gains unauthorised access to a computer network for profit, criminal mischief, or personal pleasure[126], cyber vandalism is an intentional disruption, defacing or destruction of a website[127], hacking involves break-ins such as planting of logic bombs, Trojan horses or other software program that can hide in a system or network until executing at a specific time. The overall size of cyber vandalism is said to be unclear and even though the amount of losses are significant but stable; individuals face new risks of fraud that may involve considerable uninsured losses. Malicious code refers to viruses; Cyber vandals use data flowing through the Internet to transmit computer viruses, which can disable computers that they infect. *Malicious code* is about, just to mention a few, viruses, worms and Trojan horses.

A *virus* is a computer programs with the ability to replicate and spread to other files and may be destructive or benign[128]. *Worm* type viruses arrive attached to email and spread from one computer to another rather than from file to file[129]. *Trojan horse* and other software can hide in a system or network until executing at a specific time. A *Trojan horse* is software that appears legitimate and benign, but contains a second hidden function that may cause damage. A *Junkie* is a "multipartite" virus that can infect files and the boot sector of the hard drive and thus cause memory conflicts. *Concept* and *Melissa* are macro viruses that exist inside executable programs called macros, which provide functions within programs such as Microsoft Word[130]. *Phishing* could be referred to as fraudulent activities occurring between organisations such as banks and customers via the internet or mobile "SIM": which allows attainment of victims' details in organisations, and then their banking details. Fraudsters impersonate as legitimate organisations and create fake websites or send emails that seem authentic (McDermott 2011)[131].

---

[126] A definition of a hacker as given by Laudon & Laudon: 2004. They hold that there are many ways that hacker break-ins can harm business.

[127] Cyber vandalism as explain by Laudon & Traver: 2007.

[128] Laudon & Traver: 2007 maintain that there is tension between security and other values: the more security measures that are added, the more difficult the site is to use, and the slower it becomes.

[129] When launched they e-mail themselves to computers running Microsoft operating systems and software, slowing Internet traffic as they propagate and circulate.

[130] Laudon & Laudon: 2004 state further that Junkie strikes the section of a PC drive that the PC first reads when it boots up. Macro viruses can be spread; when Word documents are attached to e-mail; when copying from one document to another and when deleting files.

[131] It is maintained that while the scam is on the rise in South Africa, the ruling is that banks are not held liable for customers' negligence.

Computer threats negates the authenticity and integrity of sites and therefore require site security to protect channels of communication, networks, servers and clients. Through Denial of Service (DoS) attack, hackers flood Web sites with useless traffic to engulf and overwhelm networks. Hackers use numerous computers to attack targeted networks from numerous launch points through Distributed denial of service (dDoS) attacks. A type of eavesdropping program, *sniffing,* that monitors information travelling over a network enables hackers to steal proprietary information from anywhere on a network. All these are the results of corrupt and fraudulent activities. Tools available for achievement of site security are displayed in Figure 4.1:

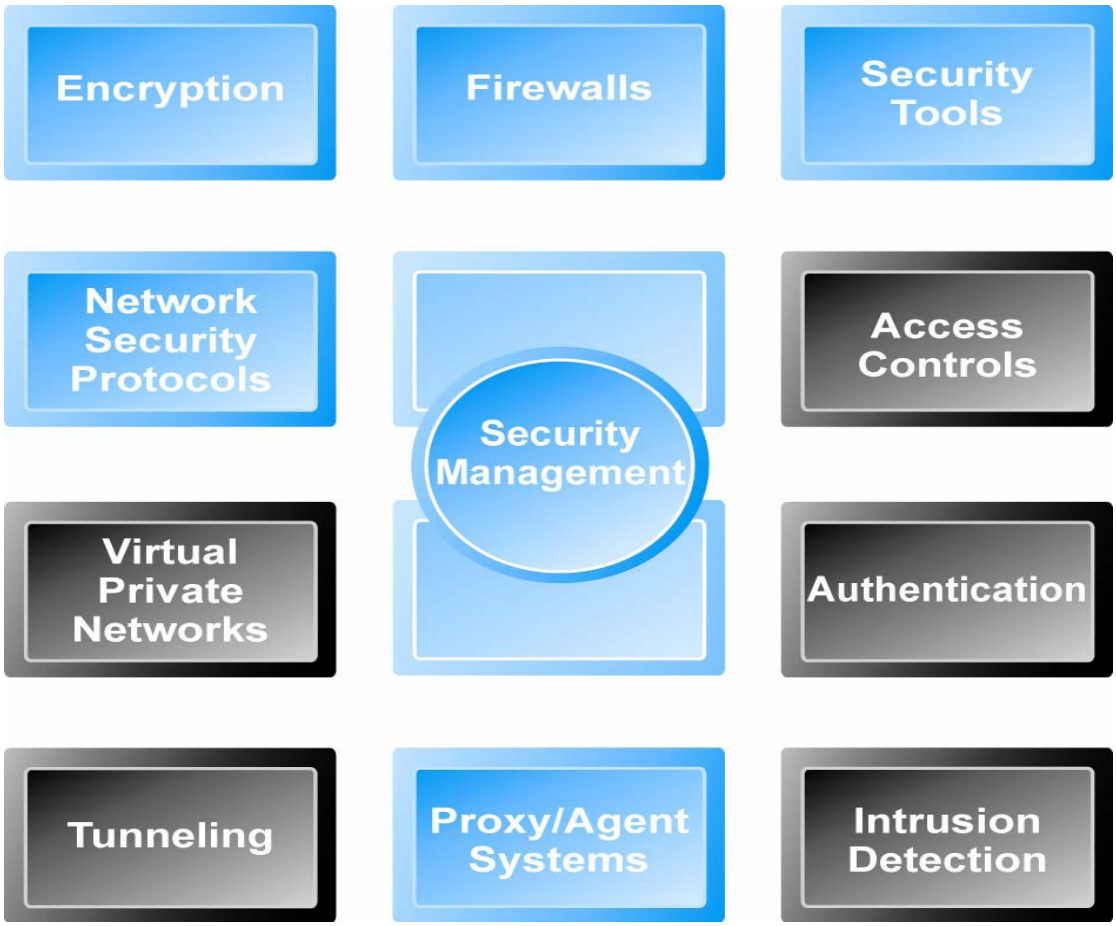

Figure 4.1: Tools for Site Security

Source: Laudon & Traver: 2007

4.8 E-commerce Security: Solutions

4.8.1 Protecting Internet Communications: Encryption

To keep up with hackers, the process known as encryption is implemented. Encryption is the process of transforming plain text or data into cipher, code or text that cannot be read by anyone other than the sender and the receiver. Its purpose is to ensure that stored information and information transmission are secure. Encryption provides message integrity; non-repudiation; authentication and confidentiality. Encryption can be categorised as follows:

- *Symmetric Key Encryption*: also known as secret key encryption, this process requires both the sender and receiver to use the same digital key to encrypt and decrypt messages. It also requires a different set of keys for each transaction[132].
- *Public Key Encryption using Digital Signatures and Hash Digests*: The sender applies mathematical algorithm prior to encryption which produces hash digests that recipients can use to verify integrity of data, whereas double encryption with the sender's private key (digital signature) helps ensure authenticity and non-repudiation[133].
- *Digital Envelopes*: Digital Envelopes address weaknesses in public key encryption such as computationally slow and decreased transmission speed. They increase processing time and symmetric key encryption by ensuring that messages are faster, but more secure. Digital envelopes use symmetric key encryption to encrypt documents but public key encryption to encrypt and send the symmetric key[134].

However, encryption solutions do have limitations in the sense that the protection of private keys by individuals may be haphazard: there is no guarantee that verifying the computer of a merchant is secure[135].

4.8.2 Protecting Networks: Firewalls and Proxy

Firewall involves hardware or software that filters communications packets and prevents some packets from entering the network based on a security policy. Firewall methods include

---

[132] Laudon and Traver maintain that data encryption standard is the most widely used symmetric key encryption

[133] CGI: 2004 states that symmetric key is also important in the implementation of Public Key Infrastructure.

[134] The concept of digital envelope as obtained from www.webopedia.com/TERM/D/digital_envelope.html

[135] Other limitations involve the CAs that are said to be unregulated, self-selecting organisations, and, Public Key Infrastructure (PKI) only applying mainly to protecting messages in transit, is not effective against insiders.

packet filters; application gateways and proxy servers. Proxy servers are software servers that handle all communications originating from or being sent to the Internet. Servers and clients can be protected by operating system controls through the application of authentication and access control mechanisms. Also, anti-virus software is the easiest and least expensive way to prevent threats to system integrity[136]. The DOD is aware of the threats around the ICT environment. Defence Information Systems (DIS) security measures and associated measures are said to be implemented proportionate with the threats to the information and environment it serves to protect. However, the DOD maintains that it is careful not to over-engineer the DIS security due to fear for inefficient utilisation of information and a lack of interoperability amongst systems[137]. These measures are discussed in the next paragraph.

4.8.3 A Security Plan: Management Policies

All methods described in an attempt to keep up with hackers calls for the development of a security plan, which requires managers and leaders to: perform a risk assessment to identify risks and points of vulnerability; develop security policy; have a set of statements prioritising information risks identifying acceptable risk targets and identifying mechanisms for achieving targets; develop an implementation plan; indicate action steps needed to achieve security plan goals; create a security organisation; be in charge of security; educate and train users and keep management aware of security issues; administer access controls, develop authentication procedures and authorisation policies; and perform security audits; and conduct reviews of security practices and procedures.

The DOD designed its own Information and Communication Systems Security (ICSS) Plan[138] based on the degree of sensitivity of its information. Although the plan addressed other issues such as loss control, fire safeguarding and transport control, focus will be on protection against malicious software and the spread of computer viruses. According to the ICSS Plan, the Defence Intelligence (Chief Director Counter-Intelligence (Def Int (C Dir CI)) has to determine ICSS threats. The Chief Command Management and Information Systems (C CMIS), primarily integrates the DOD ICSS systems according to departmental standards and

---

[136] Protecting Networks through firewalls and proxy as obtained from http://www.ehow.com/info_8167378_roles-servers-play-network-security.html

[137] Du Toit et al: 2003 hold that over-engineering is avoided to provide wide access to users in terms of accurate, reliable and consistent information, which leads to greater efficiency and effectiveness in decision making.

[138] Mpofu: 2001 maintains that it is DOD policy to establish and maintain a single, streamlined, uniform system governing defence information and communication systems security.

is responsible for coming up with counter measures ensuring protection against malicious software and the spread of computer viruses. Identified incidents shall be reported to Def Int (C Dir CI) and C CMIS and countermeasures to neutralise threats shall be identified and implemented. Incident response procedures shall be established to cover all types of security issues such as overloads; security threats; access violation; networks and/or information, etc.

For virus protection, the DOD has approved anti-virus software installed on all accessories such as wireless-cable electronic devices, portable computers and workstations that are used to transmit data. Local Area Network (LAN) Support personnel are tasked with removal of viruses from the network and workstations. The DOD shall also obtain spectrum supporting guidance from the Independent Communications Authority of South Africa (ICASA) prior to contractual obligations for the full-scale development, production, or procurement of spectrum dependent devices or systems. Protection provided shall be based on or proportionate to the sensitivity levels of the information and assets involved; and shall take into account identified threats to and vulnerabilities of information systems with respect to accepted versus actual risks. Security audits shall also be conducted by the Def Int (C Dir CI) and/or any other auditor appointed by them before acceptance of a system/product, in order to certify that the system configuration meets all DOD security requirements and standards (programming). Encompassed are all computers and computer-related devices which could pose threats to the integrity, availability, and most importantly confidential information are considered. Measures addressing potential interference (both internal and external), in terms of Denial of Service Attacks are implemented[139].

4.9 E-commerce and the Minimisation of Corruption and Fraud Risks

E-commerce has brought about positive changes with promising results. Development has been made with regard to operations within the banks, for example, the South African Multiple Option Settlement System which links all the settlement banks in the country, and allows real time settlement between banks. Major Banks have data networks connecting their branches and large corporate customers. E- Commerce involves integration of many elements of technology, infrastructure, business operation and public policy. The legitimacy and security of money payment system may “make or break” electronic commerce growth in

[139] It is maintained in this policy that the aim of the ICSS Plan is to describe command, control, management measures and responsibilities that shall be implemented within the DOD, DODI/CMI/00008/2001.

South Africa. For instance, if payment systems are too complex or exposed consumers to on-line fraud and theft, the viability of electronic commerce may suffer a material blow.

Electronic Payment Systems can be categorised as either credit card systems, stored value cards (SVCS) or network money. SVCs or "smart cards" are like debit cards where their store of value is on the cards and not in a linked bank account. The card keeps track of the progressive decline in the inscribed value as the card is used to make purchases. Network money also represents stored value, pre-purchased, but with the difference that the value is stored on the internet. Electronic money can in principle be sent overseas with a little formal difficulty as attaching an enclosure to e-mail and sending it to a supplier. It is secure, not in principle limited to any maximum value, and delivery costs are low. From an audit trail perspective, payments such as these are very unlikely to be monitored. A regulatory distinction should be drawn between accounted and unaccounted payment systems; and principles governing access to the records of electronic money issuers need to be developed internationally.

Within control activities, six specific types of control to detect improper payments recommended are: data sharing; allowing entities that make payments to compare information from different sources to ensure that payments are appropriate; data mining: A tool to review and analyse diverse data. Data mining analyses data for relationships that has not previously been discovered; Neural Networking: A technique for extracting and analysing data. The system analyses associations and patterns among data elements, which allow it to find relationships which can result in new queries. Implementation of all these recommendations emphasises the need for systems integration and as well as controls aimed at minimising the risks of corruption and fraud which centre on the objectives of this study[140]. Taking corruption more explicitly into account, in the formulation of strategies, the policy dialogue, analytical work and the choice and design of individual projects, and learning from international experience, in identifying the complex and pressing financial fraud and corruption problems could help to minimise the risks of corruption and fraud.

[140] The National Audit Office: 2006 offers activities within controls in attempt to detect improper payment through computers.

4.10 Conclusion

In this chapter, different countries efforts to accommodate e-commerce as well as problems encountered were discussed. The chapter displayed the impact of ecommerce worldwide, where countries had to engage in activities such as to: conduct IT readiness tests in order to determine what they have and what they should still acquire and at what cost, in order not to meet technology requirements necessary for e-commerce; develop a methodology that includes an integrated and seamless method of strategic planning and software development; formulate e-commerce strategies; implement new combinations of activities that were not previously possible and develop core services; and elicit system requirements and model multi-user requirements.

The next chapter introduces the notion of e-Government: which enables better policy outcomes, higher quality services and greater engagement of citizens. It includes greater transparency and accountability in public decisions, powerful ways to fight corruption, the ability to stimulate the emergence of e-cultures and the strengthening of democracy.

Chapter 5

Electronic Government

5.1 Introduction

The goal of this chapter is to introduce Electronic Government (e-Government) in support of the need for systems integration within governments. Major issues surrounding e-government will be discussed, including best practices in e-government for developing countries. The idea of e-government followed the private sector adoption of e-business and e-commerce; governments took advantage of available e-commerce technologies and existing practices developed in the private sector. As a move to a new economy, governments organised processes around the functions and the needs of citizens with Information Communication Technologies (ICTs) as a key enabler, leading-edge governments are rethinking their web strategies from their citizens' perspective. While acknowledging that in the realm of government, it should be borne in mind that access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data. The threat might increase with the introduction of systems to meet e-Government targets, but by combining technology with new ways of operating, governments can be made much more effective, accountable, transparent, and responsive.

5.1.1 E-Government Definition

The definition of e-Government is said to be ranging from "the use of information technology to free movement of information to overcome the physical bounds of traditional paper and physical based systems" to "the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees"[141]. What one deduces from given definition is that e-government is about transforming government to be more citizen-centred via technology. Coupled to that is the fact that e-government brings with it the need for government to change how it works, how it deals with information and how officials view their jobs and interact with the public. E-government is therefore a vehicle that

[141] Definition of e-government as obtained from http://en.wikibooks.org/wiki/e-Government

has expedited the rapid and efficient transformation of the public sectors to an information society around the world. Fundamental to e-government is the issue of ensuring that openness and involvement by citizens are facilitated and broadened.

E-government is evaluated through public participation; therefore, access to public services is necessary in an attempt to promote a participatory dialogue and interaction. Interactive dialogues posted on government websites help government to obtain comments on documents such as the Green paper, draft laws and regulations. By engaging the public, government could also benefit since comments may serve as tools with which government evaluates its performance. Issues that trigger arguments between government and the public should be given a critical analysis in order to be used for development and for improvement purposes. A relevant example is the issue discussed in paragraph 3.3 as well as in Chapter 7 regarding corrupt and fraudulent government leadership members. Public intervention led the SA President to taking action against members who were charged with corruption and fraud by expelling them.

5.2 The Role of Government

The emergence of the Internet and other electronic-commerce technologies has fundamentally altered the environment in which government delivers services to citizens, business, and other government entities. The effects of ICTs on societies are both far-reaching and uneven. On the other hand, ICT is fuelling the transition from industrial-based economies to knowledge-based societies. This wide disparity in the impact of ICT around the world today underscores the uneven progress of economic development. It also highlights the critical role of government in the information age, (Pascual 2003)[142]. It is in this light that governments should develop enabling conditions that will promote growth for economic e-commerce by preventing and removing barriers. Corruption and fraud are some of the barriers governments should fight against, since, as mentioned earlier, they weaken the State's ability to promote development and social justice, and that's why corruption and fraud have become leading concerns for legislators around the globe, as the diversion of public funds undermines parliamentary control of the public purse.

[142] The key to e-government is to improve citizens' access to service delivery, not to further expand the role of government.

5.3 General Principles of E-Government

The flattening of the world produces other big shakeouts in the software business wherein a new equilibrium in which all the different forms of software will emerge. A good motto for e-government, as put by Pascual (2003), is to "think big, start small and scale fast", meaning than the initial focus must be on projects which are mission critical applications and which are reliable and manageable rather than large and costly. The United Kingdom's guiding principles for e-commerce are: building services around citizens' choices; making government and its services more accessible; social inclusions; and better use of information[143]. The SA principles for e-government include: identifying government services which will be made available through e-government; setting benchmarks to measure the success, failure, or progress of an e-government project; and identifying key agencies and champions in government that will take the lead in spearheading, developing and implementing the e-government projects[144].

5.4 E-Government Goals

The communicative function of IT have been highly touted since the inception of the computer and it is part and parcel of the American credo that public information distribution should be governed by policies that serve the better good of all. Pascual (2003) offers four goals of e-government as: empowerment of public servants through ICT systems to ensure that they render services with an enhanced knowledge of client needs and expectations; achievement of major improvements in administrative effectiveness for fraudulent behavior due to business process rules implemented in ICT systems[145]. Ultimately, the goal of e-government is to enhance the interaction between three main actors in society, namely, government, citizens and business, in order to stimulate political, social and economic progress in the country.

---

[143] Im & Jung: 2001 state in their paper "Citizens as Partners: Information, Consultation and Public Participation in Policy Making" that citizens had demanded easier access to public information and an opportunity to participate in decision-making from the late 1980s. Responding to this demand, the Korean Government announced plans to construct an "electronic government".

[144] Government should prioritise the services that they will initially offer online; set benchmarks as they offer a way to measure on e-government projects; Identify key agencies only someone from a level high enough in management is able to motivate, encourage and compel others if there is resistance to changes arising from e-government.

[145] The best approach to e-government depends on the individual country, on how its political system works, and on the level of technology competence in each individual government unit.

5.5 Approaches to E-Government

Two approaches to e-government are top-down and bottom-up approaches. The top-down approach is characterised by a high degree of control by the central government and usually includes the development of a strategy. This approach facilitates integration but, developing a national strategy emphasised by this approach often takes years of bickering and the technology decisions tend to be poor. The bottom-up approach involves the moving forward of individual departments and local governments independently with their own projects, common standards are flexible, and overall national strategy. However, this approach is said to be less orderly and tends to cause some redundancy, but it also inspires innovation, resulting in a many grassroots projects (Pascual 2003).

Proposed by the DPSA, the SA e-commerce framework encompassed the management of all e-government projects to be managed by a Systems Development Life Cycle (SDLC). An interdepartmental forum consisting of government stakeholders, particularly those who are presently managing transversal e-government projects was considered. The responsibilities of specific committees responsible for e-government data-related projects were outlined in the Governance framework. The ICT projects were identified via activities such as: increased quality; better cost effectiveness and improved service delivery. All these are said to have been measured by interoperability standards, security of documents and systems, economies of scale in supporting the development of a vibrant ICT sector and Open Source Software usage and development, including elimination of duplication of ICT functions, projects and resources[146]. Based on the information on the SA government one could state SA followed the bottom-up approach, thereby gaining inspiring innovation, even though the approach is said to be less orderly.

5.6 E-Government Transactions

The National Research Council (2002) maintains that the emergence of the Internet and other technologies for electronic commerce led naturally to the development of the "digital government" or "e-government" services, which, is the application of information technology, combined with changes in agency practices, to develop operations that are responsive, efficient, and accountable[147]. Government should therefore realise the ambition of

---

[146] The E-government strategy has raised a number of issues in terms of capacity building.

[147] During the 1990s, legislative and executive branch initiatives and local government efforts, added impetus and fostered experimentation and new programs. Early government Web sites were the pioneering creations

broadening e-government services from information access to transaction support fully: that is, services that enable citizens, businesses, and other government entities to submit information to, engage in financial transactions with, or otherwise interact with government organisations. E-government services are therefore said to focus mainly on four customers: the citizens, the business community, government employees, and government agencies. It aims at making interactions with citizens, business, government employees and agencies, and other governments more convenient, friendly, transparent, inexpensive and effective. Four types of e-government are: Government–to-Citizens (G2C); Government-to-Business (G2B); Government-to-Employees (G2E); and Government-to-Government (G2G). These are represented in table 5.1 below:

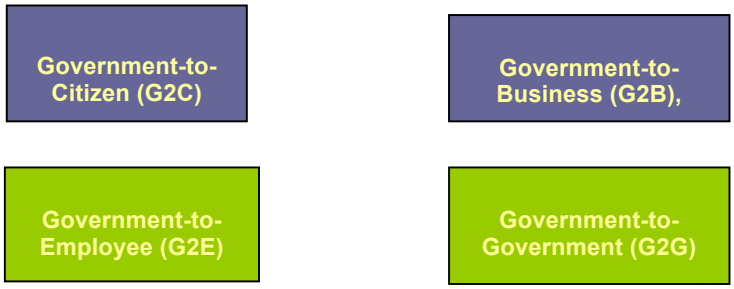

Table 5.1: Types of E-Government

Source: Department of Communications: 2000

G2C includes information dissemination to the public concerning basic services such as licence renewals, ordering of birth/death/marriage certificates and filing of income taxes. G2B transactions include services exchanged between government and the business community such as dissemination of policies, memos, rules and regulations, with services offered including obtaining current business information, downloading application forms, renewing licences, registering businesses, obtaining permits and payment of taxes.

Services offered through G2B transactions call for simplification of application procedures that would facilitate the approval process for Small and Medium Enterprises (SME) requests would encourage business development and also assist in business development, specifically the development of the SMEs. G2B services include e-procurement, an online government supplier exchange for the purchase of goods and services by government. E-procurement Web sites allow qualified and registered users to look for buyers or sellers of goods and

---

of enterprising individuals and groups. Today, government agencies and organisations' Web sites get attention from the highest levels of government and the most senior officials, National Research Council: 2002.

services. E-procurement makes the bidding process transparent and enables smaller businesses to bid for big government procurement projects. It also helps government to generate bigger savings, as costs from middlemen are shaved off and purchasing agents' overhead is reduced. G2E services encompass services and specialised services that cover only government employees, such as the provision of human resource training and development that improve the bureaucracy's day-to-day functions and dealings with citizens[148]. G2G includes online non-commercial interaction between Government organisations, departments, and authorities and other departments, organisations, departments and other authorities[149]

5.7 E-Government Challenges

There are expectations that government will match the private sector in offering direct, rapid, and round-the-clock access to information and services: cultivating the growth of e-government; and the application of information technology and related changes in agency practices to develop more accountable, responsive, efficient government operations while fostering a more informed and engaged citizenry[150]. A number of challenges for government's effective exploitation of IT has been identified and are said to encompass a mix of research and implementation issues. These revolve around: ensuring the interoperation and integration of diverse systems used by different departments and agencies with multiple stakeholders and a significant legacy base; adapting organisational structures so as to maximise their effectiveness in concert with IT-based innovation, which tends to be harder in government than in the private sector; improving trustworthiness, including guarantees of information systems security as well as assurances regarding user privacy and system

---

[148] In an e-government system, individuals are able to initiate a request for a particular government service and then receive that government service through the internet or some computerised mechanism. In some cases, the government service is delivered through one government office, instead of many. In other cases, a government transaction is completed without direct in-person contact with government employees.

[149] G2G systems generally come in two types: internal facing which joins up a single Government department, agencies, or organisations and authorities, or, external facing whereby multiple Governments IS systems are joined up, http://en.wikipedia.org/wiki/Government-to-Government

[150] Government is advised to get involved in continuous improvement to support for transactions with individuals, businesses, and organisations by emulating the commercial trend towards integration of services to improve usability for customers.

availability; bridging significant gaps between current practices and best-available practices; and meeting specific technology needs related to government missions[151].

A Green Paper on the Electronic Commerce for South Africa (2000) highlights that challenges for government revolve specifically around the need for adequate protection; promoting easy and affordable access to information and communications infrastructure; technologies services expanding policy issues associated with greater and faster broadband; deployment and forward looking telecommunications market; promoting and reinforcing education, skills development and awareness; positioning government as a model user of e-commerce in procurement; and service delivery processes; adjusting the existing domestic and international regimes to this new reality and facilitating the development of the coherent SADS e-commerce framework[152].

5. 8 E-Government Opportunities

The emergence of the Internet and other electronic-commerce technologies has altered the environment in which government delivers service to citizens, businesses, and other government entities. For other countries, e-government is part of the national crisis response that brings new expectations, expectations identified by the National Academy Press[153] as follows: that government will match the private sector in offering direct, rapid, round-the-clock access to information and service, are cultivating the growth of "e-government"; and that the application of information technology (IT) and associated changes in agency practices to develop more responsive, efficient, and accountable government operations while fostering a more informed and engaged citizenry. Figure 5.2 illustrates the ultimate benefits:

---

[151] Problems experienced by government agencies seeking to deploy new capabilities as obtained from briefings and workshops organised by the Committee on Computing and Communications Research to Enable better use of Information Technology in Government, and in news accounts from across the country, as stated by the National Research Council:2002.

[152] Government's role will be instrumental in developing the enabling conditions for growth of e-commerce by preventing and removing barriers. To foster a stable environment and to realise the full economic potential of e-commerce requires government participation.

[153] National Academy Press; http://www.nap.edu.catalog/10355.html

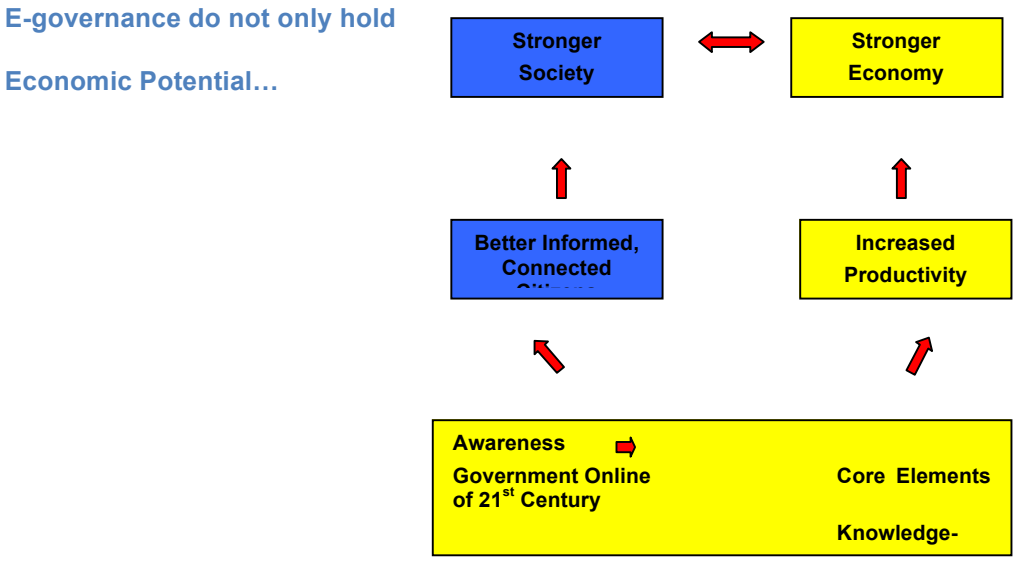

Figure 5.2: The Ultimate Benefits of E-Government

Source: Department of Communications. P.118

Governments are playing a key role in demonstrating the advantages of electronic service delivery. Business drivers include improving customer focus and service, focusing resources on core mission areas, increasing competitiveness in the marketplace. By transforming to e-government, the government will foster entrepreneurial government based on more business-like practices, cost savings and enhanced environment – improved response. The government needs to play a 'catch up' with the private sector and other countries in terms of e-commerce. The Government Information Infrastructure (GII) is a very expensive undertaking that requires cross-agency, cross-government planning agencies, and is needed to ensure that citizens enjoy the full benefits of e-government[154].

E-government—which has diverse constituencies that include citizens and other individuals; business; non-profit organization and the many federal, state, and local agencies—is envisioned as providing some of the following key benefits; more accessible government information; faster, smoother transaction with the government agencies; enhanced ubiquity of

[154] Pascual: 2003 gives an example of the benefits of e-government at the Philippine National Bureau of Investigation (NBI) and states "that in previous years, the Philippine NBI has been the object of many complaints because it took at least three days to secure an NBI clearance. The NBI clearance is required when applying for employment, passports, visas, licensure examinations, and the like". This clearance ensures that the citizen does not have a pending criminal case or existing criminal record. Thus, at any given time as many as 30, 000 citizens wait in line for an NBI clearance at the NBI head office.

access to information and transactions; greater effectiveness in meeting the needs of specific groups of users increased participation in government by all people, forcing a more informed and engaged citizenry; greater ability to meet expectations for advances in government unique areas, including challenges in the newly emerging homeland security mission; and more efficient internal government operation.

More important to e-government is the establishment of a long-term, organization-wide strategy to constantly improve operations with the end in view of fulfilling citizen needs by transforming internal operations such as staffing, technology, processes and work flow management. Thus, e-government should result in the efficient and swift delivery of goods and services to citizens, businesses, government employee agencies. To citizens and businesses, e-government would mean the simplification of procedures and streamlining of processes. To government employees and agencies, it would mean the facilitation of cross-agency coordination and collaboration to ensure appropriate and timely decision-making.[155]. Other opportunities are offered by Hirschheim & Klein (2003) state that IT is enabler of sourcing and off-shoring: the phenomena of outsourcing and off-shoring would be impossible without the high speed and reliable global networks on which industry has come to rely since the mid to late nineties; and it is an enabler and catalyst for commoditisation whereby it can provide an important support function to make them more effective and reduce the costs of communication[156].

The National Research Council (2008) states technical areas impacting on the creation of more advanced capabilities in e-government. Enhancing the number of compatible levels of technologies would greatly facilitate the building of advanced e-government capabilities that include, for example: information infrastructure and e-commerce technologies, which provide the foundation for e-business inside and outside the government; information management technologies, which permit search and retrieval from the very large volumes of information systems; middleware, which provide common service and capabilities that “glue” software components together into larger systems; human-system interfaces, which provide “every-citizen” usability; modelling and simulation, which are important tools underlying government planning and decision making (such as in crisis management); and software

---

[155] The advantages posed by e-government as stated by Pascual: 2003

[156] According to Herschheim & Klein: 2003, once established, IT can provide an important support function to make them more effective and reduce the costs of communications.

technologies, which permit construction of more robust, larger-scale, interdependent software systems[157].

5.8.1 Factors influencing E-Government success

Governments and agencies firmly recognize the importance of embracing ICT to achieve development goals and successfully implement its projects. Introducing an appropriate IT infrastructure and widespread introduction of ICT into everyday life can facilitate the stimulation of economic growth, raising living standards and modernizing cultural activity. Agencies need to attain certain IT foundations; technical skills; and sound processes in order for them to effectively participate in IT facilitated projects and initiatives such as the e-Government Initiative. Several salient technical facets include technical requirements like the agency requirements, architectural demands, infrastructure employed and its project objectives. Pioneer countries embraced e-Government due to reasons such as: the increase in effectiveness, efficiency and productivity of the public sector; improved quality of government service provided to citizens, residents and to the business sector, which inevitably led to economic growth and improved gross domestic product.

Moreover e-Government is a nation-wide initiative that aligns and streamlines the country's different vertical entities and agencies to provide its services in a more convenient way in order to enhance the quality of the offered services as well as to serve citizens, businesses and governmental agencies needs. It is therefore natural to require firm governance to sponsor and lead the initiative, in addition to a sincere adoption from all affected stakeholders to the e-Government initiative plans and projects[158]. Before any government embarks on a big project, it must first determine what it aims to achieve as well as the goals and objectives of e-government. Five steps are involved in a successful implementation of e-government, namely: developing a vision, conducting an e-readiness assessment; identifying realistic goals; getting the bureaucracy to buy-in and develop a change management strategy; and building public/private partnerships[159].

---

[157] IT enhancements as viewed by the National Research Council: 2008.

[158] Yesser: 2007 on the reasons why some country's skyline change overnight and why a country gets its acts together to do all these things in a sustained manner.

[159] Pascual: 2003 on the steps to be followed in implementing a successful e-government.

5.9 Information Technology Readiness

Technical resources (Hardware and Software) and infrastructure are found to be essential requirements to successfully achieve redesigned and e-enablement projects. Deciding on whether an agency is IT ready or not is a crucial mission. That is, due to various technological routes, the diversity in technical solutions and the continuous advancements in technology. Hence it is hard to ultimately decide if an agency is ready or not. IT readiness should be measured against well-defined objectives, in order to determine whether IT resources are adequate to achieve the objectives foreseen or not. Pascual (2003) clarifies that: government services to be made available through e-government should be identified; benchmarks should be set to measure the success, failure or progress of e-government projects; and key agencies and champions in government projects should be identified. It is therefore important to understand that to obtain the desired results from the e-enablement projects, agencies must be technically aware of their capabilities, in terms of technological knowledge and assets. Pascual (2003) states that a government-wide inventory of assets should be taken in order to determine what the government has, and the quality of what it has, as well as what it does not have. A shopping list of what is needed to make e-government happen must then be written out. It is important to have the following aspects in mind when taking an inventory: hardware, software and equipment as well as the laws and regulations[160].

Pascual (2003) offers what he named a "Benchmarking E-Government Progress: The Networked Readiness Index" as represented in table 5.2 below

[160] Pascual: 2003 holds that governments should determine the type of ICT skills people possess, their level of competency, and whether there are enough of them with the skills necessary to turn an e-government project. The types of ICT hardware/software each government agency has, how old or new are the equipment and the physical infrastructure of government's existing telecommunications should be identified. Government should also determine whether there are appropriate policies and regulations in place for the development and implementation of e-government and whether there are policies and regulations that need to be amended or changed in order to implement and facilitate e-government.

BENCHMARKING E-GOVERNMENT PROGRESS:

THE NETWORK READINESS INDEX

The Networked Readiness Index (NRI) was developed by Harvard University's Center for International Development as a macro-level measurement tool to help better understand "how different national environments affect the adoption and use of ICTs."

The NRI is an aggregate index capturing broad "readiness" levels. It is composed of two main component indexes: network use and enabling factors.

Network use is defined by the extent of ICT proliferation in a certain country, measured by five variables: Internet users per 100 inhabitants, cellular mobile subscribers per 100 inhabitants, Internet users per host, percentage of computers connected to the Internet, and availability of public access to the Internet.

Four sub-indexes make up **enabling factors,** constructed to reflect not only the preconditions for high quality network use, but also the potential for future network proliferation and use in a specific country:
• Network Access (Information Infrastructure and Hardware, Software, and Support)
• Network Policy (ICT Policy, Business and Economic Environment)
• Networked Society (Networked Learning, ICT Opportunities, and Social Capital)
• Networked Economy (e-commerce, e-Government, and General Infrastructure)

In the NRI, the **e-government micro-index** is determined by government effectiveness in promoting the use of ICTs, availability of online government services, extent of government Web sites, and business Internet-based interactions with government

Table 5.2 General Principles for E-Government Development

Source: Pascual: 2003. p27.

Government agency technical readiness (IT Readiness) reflects the agency's technical resources, existing IT infrastructure in the agency, and the ability to change and redesign processes. Through the use of the application of an IT Readiness Assessment Framework, governments manage to discover what they have as well as what still need to acquire, in order to engage in e-government activities. In SA a strong political will drove the vision. The readiness assessment addresses issues such as the legal frameworks, governance models, infrastructure models, etc. Alignment of projects with the vision is demonstrated through a number of case studies showcasing innovation in service delivery and customer focus. It is also helpful to apply a methodology consisting of: the *Design Stage*, in which assessment objectives are defined and data collection methods are identified and conducted. The *Evaluation Stage*, based on data collected and the use of a coherent evaluation framework,

the agency IT current status is mapped and evaluated; and *The Analysis of Findings* stage in which the scores obtained from the evaluation stages are analysed and envisaged to plan the agency IT capabilities increment and enhancement. The assessment methodology should follow an evaluation framework that provides a measurement structure and scoring method, in addition to an insight on the technical foundation of the agency for the later enhancements and improvements plans. Therefore, it is crucial for the agencies to address their IT Readiness and identify the technological challenges they might face, as well as identifying the decisions and the projects they need to launch during their quest to become IT Ready agencies[161].

5.9.1 Assessment Evaluation Framework

Achieving IT readiness, an important milestone to sustain and to successfully implement government projects, depends on and relates to several factors. A systematic assessment is performed to determine the agency's actual readiness. Best practices highlight that the use of a comprehensive methodology is important in assessing agencies' IT readiness. The methodology suggests that designing and strategising the assessment objectives, laying out the evaluation framework, and setting boundaries for evaluation results analysis to build up findings and plans for the agency to be ready. The Assessment Methodology used to identify the agency IT readiness status plans the suitable evaluation framework to be adapted in the early stages of the methodology; accordingly, data collection - through questionnaires or other mechanisms – can be aligned to cover all the necessary information about framework dimensions and associated information.

5.9.2 An Approach to Agency's Readiness Self-Assessment

The Saudi e-Government Program offers a set of recommendations to guarantee a comprehensive assessment and analysis accompanied by a coherent methodology to be followed while initiating the Assessment Framework and while conducting the assessment/evaluation and while analysing Readiness Scores. Activities involved, planning IT Readiness Assessment against measurable objectives - indicators include defining the assessment objectives and requirements - and adopting a systematic assessment framework that takes into consideration the agency's technical characteristics and requirements. Analysing requires that the agency readiness level and its overall abilities to fulfil the defined

[161] It's been stated by Yesser: 2007 that the assessment methodology offers a comprehensive set of functions and principles to design the assessment, decide on evaluation criteria, conduct the assessment, obtain results, analysing the results and finally generate the findings about the agency IT Readiness status.

objectives and needs, be investigated; enhancement plans to be mapped along with the evaluation dimensions and factors, and that its IT readiness increment be planned to achieve the desired readiness state acknowledged in the evaluation framework[162].

5.9. 3 Evaluation Framework Dimensions

To evaluate the different technical aspects in an agency, it is critical to: adopt a strategic technique for the evaluation; divide the agency's different technical aspects for measurement; and then collectively generate results and provide overall scoring results. IT readiness does not just cover the technical related aspects, but it covers the process readiness and redesign potentials also. Measuring readiness at the dimension level is not enough: each dimension should be categorised into factors for scoring. Technical dimensions broadness empowers categorisation, as it is possible to subdivide each dimension into tangible technical factors and indicators that shape the dimension characteristics. The technical readiness assessment dimensions to be discussed are: Architecture, Infrastructure and Process Readiness. Categories and measurement characteristics of these selected dimensions should be mapped in the Evaluation Framework[163].

Architecture Readiness refers to the technical structure and orientation. Several technical structure requirements are demanded for Software development to implement e-enablement projects namely: hardware structure and standards, services orientation and design. The term "Technical Architecture" is used to describe the structure of a hardware system, and the process and discipline for effective implementation of the design. The architecture of a system always defines its broad outlines, and may define precise mechanisms as follows: service orientation reflects services, design and point of reference, which can be judged through the: share of services supported by IT; availability of fully automated services; share of data input by database queries; and overall infrastructure. Table 5.3 represents the Architecture Dimension Factors and Criteria:

---

[162] Once the agency assessed its IT readiness, it needs to adhere to a set of recommendations to guarantee comprehensive assessment and analysis, accompanied by a coherent methodology, Yesser: 2007.

[163] According to Yesser: 2007, there are two sides to the evaluation framework. To begin with the evaluation framework must be initiated and its dimensions, factors and scoring criteria set-up and then be utilised to evaluate the agency IT foundation and determination scores. Setting dimensions for evaluation, in which each dimension is concerned with a clear technical aspect in the agency empowers the measurement process and provides clearer assessment outcomes. After scoring the agency IT readiness in each dimension, the framework should provide a scientific and systematic scoring rule and mechanism to collectively calculate the agency overall readiness.

A ASSESSMENT OF ARCHITECTURE READINESS – FURTHER INFORMATION FOR COMPLETION OF SELF ASSESSMENT

	1	2	3	4
Layered structure	Our architecture does not have any separation of dedicated domains differentiating functional units such as business applications, support systems, databases, ERP, and web front end	Our architecture has some separation of dedicated domains, i.e., at least one but not all of the functional units business applications support systems, databases ERP, web front end is separated	Our architecture differentiates all significant functional units such as business applications, support systems, data-bases, ERP, web-front end	Our architecture has the 3 layers presentation layer (including existing portal solution), middle layer (including sepa-rated logic of business and support applications and back-office layer (including data bases, ERP)
Service orientation	Our internal and external interfaces between applications and/or databases are established on 'case-by-case' basis mainly by direct database access and do not obey global standards	Our internal and external interfaces between applications and/or databases are designed similar even though we have no or only few standards	Our external and internal interfaces between applications and/or databases all obey rigid standards, however do not use service oriented interfaces between domains	All our internal and various external interfaces between applications and/or databases obey principles of service orientation
Portal	We have no or only a small web presence; customers can at most find information about general organisation of our entity, addresses, and services we provide	We have a compre-hensive web presence offering extensive in-formation about our entity including a list of services we provide, our organisation, form down load, and online inquiries	Our web presence offers all services listed under 2 and additionally some interactive (portal) ser-vices/such as online tracing of current status of service or even online service provisioning	Our web presence/portal offers all services listed under 3 and is organised obeying principles of customer centric portal design, i.e., services are triggered from portal using shared IT support services such as pay-ment, security, DMS

Table 5.3 Architecture Dimension Factors and Criteria

Source: Saudi e-Government Program: 2007. P. 19

The Architecture dimension factors and their scoring criteria and characteristics are illustrated in a Diagram below. Measurements criteria are mapped against the four scoring results groups in a clear matrix. Represented in this Diagram are factors in the infrastructure readiness: basic hardware and software which include desktop/employee; mainframe availability; server availability; and desktop operating system. Desktop operating system consists of external Data Exchange, that is, exchange with others (yes/no), and share of services with external data exchange (in%) and internal connectivity, which is about percentage of Internal connectivity between departments and agencies at different locations (i.e. intranet connectivity (in %). These are represented in Table 5.4 on the next page:

B ASSESSMENT OF INFRASTRUCTURE READINESS – FURTHER INFORMATION FOR COMPLETION OF SELF ASSESSMENT

	1	2	3	4
Basic hard- and software	In our entity computers are not used to large extent, i.e., at most every third employee in administrative position has desktops; only few servers; major share of desktops running on Windows 98 or NT	Our entity uses computers, but there are obvious lacks in the equipment, i.e., about every second employee in administrative positions has a desktop; good mixture of OS** Win XP, 2003, 98, NT, 2000*; several servers available	Our entity is in general well prepared regarding the availability of computers, there are minor gaps, i.e., about every administrative employee has one desktop; majority of OS is Win XP, 2003; numerous servers or mainframes available	Our entity is entirely sufficiently equipped with computers, recent operating systems, servers, and mainframes
External data exchange	Our entity performs only paper based data exchange with other entities	Our entity performs electronic data exchange with other entities based on data files exchanged via e-mail, ftp, or data media	Our entity exchanges electronic data with some other entities by using common databases or common applications connected permanently	Our entity is permanently connected to all significant other entities; data is exchanged by common databases; there are straight through processes using external data
Internal connectivity	There is only weak internal connectivity within headquarters (less than 50% of desktops connected); no connection between headquarters and branches	The share of desktops within headquarters connected to LAN is above 50%; some branches are permanently connected to headquarters and exchanging business data	Significant internal connectivity; above 80% of desktops in headquarters connected to LAN and all desktops in branches able to access LAN in headquarters; connection used for exchange of business data	All desktops within headquarters and branches linked by permanent connection with sufficient bandwidth; connection used for exchange of business data

* Or comparable releases from other vendors

** Operating Systems

Table 5.4 Architecture Dimensions Factors and Criteria: Operating System

Source: Saudi e-Government Program: 2007.p19

Factors of an infrastructure dimension, scoring criteria and characteristics: Measurement criteria mapped against the four scoring results groups in a clear matrix. Process Readiness: e-Government is about using ICT to enable transformation to an information society, as well as about redesigning and restructuring the agency business related functional processes workflow and components to increase effectiveness, efficiency and performance. Process readiness reflects the existing support for processes and procedures to empower and enable technology, and can be judged through the following factors: support processes, which concern the availability of major support systems (not e-mail); process automation; and data and information flow involving share of manual data input and methods of customer notification. The processes dimension factors and their scoring criteria and characteristics are illustrated in Table 5.5 on the next page:

C ASSESSMENT OF PROCESS READINESS – FURTHER INFORMATION FOR COMPLETION OF SELF ASSESSMENT

	1	2	3	4
Support processes	Business processes do not use common support functionalities, i.e. there are no applications providing security (such as authentication), e-payment, or DMS* for all other processes; if needed these are integrated into individual processes	At least one of the support functionalities security, e-payment, and DMS is offered by an application that is accessed from various business processes; system is either in house development or from small vendor	At least two of the support functionalities security, e-payment, and DMS are offered by systems that are accessed from various business processes; system is from popular vendor and has potential to be used by other entities	Complete portfolio of support functionalities security, e-payment, and DMS is offered by systems accessed from all major business processes; system is from popular vendor and has potential to be used by other entities
Process automation	In our entity most business processes are performed without use of IT, i.e., processing mainly paper based by administrative employee; no processes fully automated	In our entity all major business processes are performed with use of IT, i.e., during major processes administrative employee uses IT for support of process such as database query, form printing; at most one process fully automated	In our entity all every business process is performed with use of IT i.e., during all processes administrative employee uses IT for support of process such as database query, form printing; only few process fully automated	In our entity every business process is performed with significant use of IT; most processes are fully automated, i.e., after initial data input all operation is performed by applications
Data and information flow	Our customers do not communicate with us using electronic media, i.e., data entry either does not take place or is done 100% manually by typing of paper forms; customers are notified either by letter, phone, fax, or in person	To a large extent, our customers communicate with us using non electronic media, i.e., data entry is done above 50% manually by typing of paper forms; customers are notified either by letter, phone, fax, or in person	To a large extent, our customers communicate with us using electronic media, i.e., data entry is done less 50% manually by typing of paper forms; some customers are notified by e-mail or internet besides traditional ways	Major share of data entry takes place by database query, i.e., for example citizen ID is used to avoid data entry by calling historic correspondence; most customers are notified by e-mail or internet besides traditional ways

* Document management system

Table 5.5 Processes Dimension Factors and Criteria

Source: Saudi E-Government Program: 2007. P.20

5.10 E-Government and the Minimisation of Corruption and Fraud Risks

Whilst e-government is defined as involving the automation or computerisation of existing paper-based procedures that will prompt new styles of leadership; new ways of transacting business; new ways of listening to citizens and communities; and new ways of organising and delivering information[164]: to citizens and businesses, e-government would mean the simplification of procedures and streamlining of the approval process. To government employees and agencies, it would mean the facilitation of cross-agency coordination and collaboration to ensure appropriate and timely decision-making. As a major tool in building a

[164] The renewal kiosks are said to have significantly reduced graft and corruption by reducing opportunities to bribe employees to "facilitate" the approval process or falsify documents, as obtained from (http://en.wikibooks.org/wiki/E-government/Intoduction)

tradition of transparency and good governance, it is maintained that e-government can advance the fight against corruption and fraud. However, e-government by itself will not put an end to corruption and fraud. It must be accompanied by other mechanisms to be fully effective in this regard. A report commissioned by the British National Audit office (NAO) (2006) presents the results of a benchmarking exercise investigating issues of fraud and error in the social security systems of the European and non-European countries. The benchmark undertaken considered eight countries similar to the United Kingdom (UK) in terms of wealth and diversity of population. The delivery of social benefits involves large amounts of public expenditure, which is further increased by losses through corruption. Results for five countries considered, were found to be relevant to this study, in terms of the role played by e-government in fighting corruption and fraud are as follows:

***Ireland*:** Since 1987, the IT system of the Department for recording overpayment and recovery details has been a stand-alone system that does not interface with the Department's other computer systems. The Department responded to the then system deficiencies through the development of an integrated IT system for its long-term schemes, which would facilitate a more integrated approach to control activity (e.g. more systematic data-matching). This process is called the Service Delivery Modernisation (SDM). SDM was aimed at: designing a more integrated IT system; managing organisational change; and introducing new consumer-centric approaches in the social security administration. This initiative was the response by the Irish Departments of Social and Family Affairs with regard to acts of fraud and error where overpayments mainly arose from the administration of estates of non-contributory old age pensioners. During the period between 1998 and 2002, about half of overpayment cases resulted from deliberate fraud. The use of false Personal Public Service numbers estimated to have cost the state in the region of €50 million (about £35 million) a year, though the department's accounting officer highlighted that this number was speculative. SDM was therefore adopted in attempt to reduce such fraudulent activities.

Other developments experienced in other countries in their attempts to combat corruption and fraud include: Australia: where it was found that the latest system is the delivery of benefits by way of magnetic strip cards, namely, Electronic Transfer Benefits Cards (ETBC);

The Netherlands: some trends in the direction of and motivation for fraudulent activity, investment in IT equipment including identity card technology (social services and controls, in 2005, to be based on an electronic card system. The Netherlands had a unique fiscal

number for each person, which was used for most interactions with government and allowed comprehensive data exchange between agencies.

New Zealand: maintained that data matching could detect clients who are receiving or have been receiving entitlements to which they are not eligible. Data matching is also believed to provide information to support investigations and prosecutions. The Ministry matches data with five other Government departments or agencies.

Sweden: special measures have been introduced to improve coordination and data matching between unemployed insurance, the social insurance agency, the tax office and the agency for student loans. A new IT system has been implemented, which allows for real time cross-checking of data between the agencies. The results of this initiative seemed promising. A comparison of a week in 2003 and 2004 showed a reduction of cases of overpayment by 27% and a reduction in allowance scheme by 29%.

The United States of America (USA) government recognises that both prevention and detection of improper payments is essential in an effective control regime.

The United Kingdom (UK) expanded data-matching with other government departments[165].

In the ***Municipal Government of Seoul***, there were concerns about lack of accountability and the presence of corruption with the issuing of local government licences and permits. This led to the development of an OPEN (Online Procedures Enhancement for Civil applications) system, an anti-corruption Web portal that provides citizens with a range of relevant information, including the overall goals of the anti-corruption drive and an explanation of the rules and procedures for the permit/license application and processing. The citizens are therefore better informed, the government process is more open, and the rationale for bribery has been largely removed. Feedback from citizens has been very positive, and there has been a dramatic decrease in reported corruption[166].

The examples above highlight the level of impact of corruption and fraud activities and therefore calls for the need by governments in other countries to take initiative. Given the possibility of creating revenue streams from e-government services, the private sector has made it easier for the establishment of e-government and is viewed as an invaluable partner

---

[165] The British National Audit Office: 2006 sheds results of their study on attempts by international countries to curb corruption and fraud through systems integration.

[166] These achievements have been, in a larger part due to an integrated approach implemented, ensuring that technological change serves public sector reform goals rather than vice versa.

in e-government. As a result, governance has become more dependent on public information made available on the Internet: communities are able to pay taxes and utility bills, register births and deaths, apply for drivers' licences and passports, etc. The next chapter gives an overview of the DOD application systems, its preparation for employing a new system that will promote accountability and manageability, and help curb fraud.

Chapter 6

DOD IT Infrastructure

6.1 Introduction

It has been emphasised in previous chapters on e-commerce and e-government that governments need to upgrade their common Information Management/IT infrastructure. It was also mentioned how crucial it is that systems be integrated and interconnected. Since the IT infrastructure is the shared technology resource, providing the platform for the organisation's specific information applications, organisations should therefore determine how to develop an information technology infrastructure that can support their goals when business conditions and technologies are changing so rapidly; and meet new business and technology challenges that may require redesigning the organisation and building a new information technology infrastructure. The aim of this chapter is to examine the DOD IT infrastructure to determine its position in terms of the importance of interconnecting databases, applications, and legacy systems seamlessly into a coherent IT infrastructure. The IT infrastructure within the DOD, for the purpose of this study, will be confined to existing vehicle management systems as well as the introduction of the Integrated Financial Management Systems (IFMS). The degree to which both systems are vulnerable to corruption and fraud will be investigated.

6.2 Brief History: DOD Transport Management

The DOD has acquired legacy systems due to the fact that these systems were developed independently of each other and very often they do not integrate with the evolving IT infrastructure. Yet, these systems still drive the day-to-day business processes. Replacing the legacy systems with new solutions might not be feasible or practical, or it might cost a considerable amount of time. However, immediate integration might be a requirement for a strategic project, such as supply chain management or e-business. The SA Government realised the need to replace these legacy systems within all its departments. The idea of replacing these systems is based on the fact that legacy systems are prone to corrupt and fraudulent activities since they lack integration. Internal computer fraud occurs as a result of

employee knowledge that tracking fraud will be difficult if not impossible. Among others, these systems allow for easy manipulation whereby data becomes easily altered to show some change in quantity, for example, change in inventory levels so that it does not appear that inventory was in fact stolen, change in amount or changing someone's salaries or creating fictitious employees. Hence Government proposed that IFMS be implemented. A brief history of the DOD operations in terms of vehicle management will be given before embarking on the IFMS project.

6.2.1 DOD Internal Operation on Vehicle Management

Information as obtained from DOD policies highlights that the Chief of the Army who is responsible for the DOD vehicle management has ensured that the following documents for governing vehicles are promulgated with respect to the Defence Act, Act 42 of 2002, Section 34 (f). These documents are about Road Transport in the DOD in terms of, to mention a few; Utilising Road Transport outside Normal Working Hours; Subsidised Motor Transport; Reporting and Management of Losses, Damages and Claims in the DOD; The Control and Operation of Duty Buses in the DOD; Maintenance and Repair Implementation Instruction: Toll Plazas; Vehicle History Files; Safeguarding of Military Vehicles; and Unit Standing Security Order. These documents are applicable to all DOD divisions and units, and are binding to all members utilising DOD transport. It is important to mention that DOD drivers are exempted from payment of Toll Plaza fees whilst on duty. The DOD is responsible for payment of such fees: an activity managed via Toll Plaza Forms.

Research reveals that vehicle accidents are one of the most frequent causes of death in South Africa[167]. Income generated from Toll Plaza payments by road users could be used on a program to curb casualties and road deaths. As a result, there is a possibility of hikes in Toll Plaza payments. These road deaths and casualties, are costing the country R60 billion each year[168], therefore the Department of Transport Minister proposes to build additional toll systems that will cost R2.6 billion, whereby only certain taxis and busses will be exempted[169]. Granting permission to such a proposal will imply increased tariff structures (as per different vehicle types and size). This increase, should permission be granted, will have an impact on

---

[167] Gould: 2011 conducted a study in which he identified a number of mistakes the public often make when they think about crime.

[168] The Minister maintains that "focus will be on the United Nations for its effort to place road safety on the international platform and its role in supporting the implementation of Decade of Action for Road safety 2011-2020", Mashaba: 2011.

[169] Serrao et al: 2011 explains how the proposed toll scheme will cause taxpayers to fund rocketing expenses.

owners of vehicles, including government departments. This topic was introduced in order to emphasise the importance of management and control of documents related to toll plazas within government departments. Although petition against this proposal has already been submitted by the opposition party, the final decision is not yet known.

Further on the DOD, this department maintains both a standardised vehicle management manual system as well as different computer-based systems. There are procedures to follow as well as various forms to be completed for one to be able to utilise vehicles. Transport officers are responsible for the control of vehicle movements. History files have to be safely kept. Every record should be kept and the system should be updated in order to produce reports on the status of vehicles when needed.

The two main computerised systems running within the DOD with regard to vehicle management are: Operational Support Information System (OSIS), and CALMIS. The SA Navy has embarked on an Adaptation Project to achieve joint usage of the SA Air Force Application Software in May 1998. This joint venture was named OSIS in 1999, (OSIS was originally developed as the South African Air Force Logistics Information System - SLIS). The Army is on CALMIS. Information obtained from interviews hold that the SA Medical Health Services (SAMHS) is on Vehicle Management System (VMS) program. In the topic: “South African National Defence Force on the road to a better Asset Management”, Tshivhidzo (2008) quoted the late Secretary for Defence reporting that the South African National Defence Force (SANDF) is currently in the process of implementing new systems to enable it to “better account for and manage its assets”. Two observed movements within the DOD are “Project Libidi” by the Army and the Integrated Financial Management System (IFMS).

Project Libidi involves an inventory taking by the Army in order to update its Asset Register. The aim of Libidi is to update the server KURMENU via CALMIS. IFMS is the Government initiation to phase out legacy systems within the whole of government institutions for better manageability and accountability. This inventory taking is said to help to determine what is available, what is not, and the quality of what an organisation has, and what it does not have, Pascual (2003). Project Libidi was conducted with good intentions and its findings, if conducted properly, will enable the DOD to uncover and have knowledge of all its assets. The advantage of this project is that it also involves unique identification of assets by means of bar code allocation. This project is a good preparation for the implementation of IFMS: audit reports data could be used for comparison purposes with information contained in

legacy systems. It is envisaged that the implementation of IFMS, on the other hand, will help government to achieve a seamless flow of information among different core functions such as HR, VMS, and FIN. An integration of such core functions means redeployment of government functions such as human resources and accounting expertise to other departments thus strengthening the capacity and financial management leadership. Applying controls such as passwords, encryption, Console Logs and network security controls could help to fight against fraud whilst improving accountability and manageability.

6.3 DOD Enterprise Information Systems and Architecture Services

The Republic of South Africa (RSA) has identified the State Information Agency (SITA) as the provider of information technology (IT) and information systems (IS) services to Government departments Different Service Level Agreements (SLA) have been made between the DOD and SITA, such as: SLA 1.2[170]: which concerns enterprise information systems and architecture; SLA 2.6: based on ICT acquisition services[171]; SLA 3.1 for information management[172], etc. It is expected that SITA would supply the required architectural support services as well as skilled resources on an in sourced/outsourced basis. SITA will execute systems integration in conjunction with the Defence Enterprise Information Systems Management Systems Division (DEISM Div) based on DOD requirement.

The Defence Enterprise Information Systems Architecture (DEISA) interprets business requirements and strategic direction regarding all information and communication systems (ICS) and services required as enablers of ICS in the DOD[173]. One of DEISA's functions is to compile, maintain and manage the DIS framework, compliant with departmental objectives and policy, and in support of the DOD Information Strategy; and compile, maintain and manage the Defence Information Communication Systems Architecture (DICSA)., with the primary purpose of defining interoperability standards, principles for selection and guidelines

---

[170] The SLA for those activities related to the interpretation of business requirements and the provision of strategic direction regarding all ICS and services required, as written by van Zyl: 2010.

[171] Deliverables include new and renewal project minor and major enhancement and procurement of infrastructure/software, Dannhauser: 2010

[172] SLA3.1, revised annually, is the business agreement for the supply of information systems /technology products as well as services to the DOD, Barker: 2010.

[173] SLA, revised annually, is the business agreement between the DOD and SITA for the supply of information systems/technology products as well as services to the DOD, van Zyl: 2010.

for implementation and design[174]. With the help of the parties involved such as those mentioned above, systems which were developed based on the command and control legislative framework of prior 1994 will be phased out. This is due to failure or difficulty to keep the systems aligned with new legislation and regulations. The phasing out of these systems will enable government and its entities to service communities effectively.

6.4 Integrated Financial Management Systems (IFMS)

The IFMS is a project aimed at enhancing the integrity and effectiveness of expenditure management and performance reporting in order to ensure effective service delivery. IFMS consists of the Zachman Framework for Enterprise Architecture, sometimes simply referred to as the Zachman Framework and also known as The Open Group Architecture Framework (TOGAF). The Zachman Framework originated by and named after John Zachman, is a way of representing the various types of descriptive information and perspectives that might comprise enterprise architecture. It is also a logical structure for classifying and organising the design aspects of an enterprise that are significant to its management; aspects concerning the Who, What, Where, When, Why and How of an enterprise. This is addressed in a six column matrix representing the types of information addressed[175]. The classification is represented in Figure 6.1 below:

	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organizational Unit & Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organizational Unit & Role Rel. Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Specification	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location details	Event Details

Figure 6.1 Zachman Framework Model

[174] In order to execute the responsibilities and functions, DEISA requires skilled resources on an in-sourced/outsourced basis and architectural support from SITA.

[175] Information on the Zachman Framework as obtained from http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap39.html

Source: http://en.wikipedia.org/wiki/File:Zachman_Framework_Model.svg

TOGAF is viewed as a vehicle and repository for practical, experienced-based information on how to go about in terms of the enterprise architecture process: it provides a generic method with which specific sets of deliverables, reference models, and other relevant architecture assets can be integrated[176]. IFMS is used worldwide, the government of Malaysia being the first to embark on the initiative[177].

In SA, the project for an Integrated Financial Management System was led by the National Treasury to review and upgrade legacy systems within government. IFMS is implemented with the objective to enhance the integrity and effectiveness of expenditure for the full government business cycle and would be supported from the beginning to the end of the financial year. Initiatives such as e-government and e-commerce be successful, governments must have access to information that possesses characteristics such as: information must be available, accurate, relevant, authentic, complete, secure, etc[178]. IFMS is described as being capable of providing information in that format.

The scope and functionality of IFMS, as put by Chêne (2009) may vary across countries but sub-systems normally include accounting, budgeting, cash management, debt management, and related core treasury systems. Some countries are said to have chosen to expand these core sub-systems. They have decided to add to these core functions, non-core sub-systems such as tax administration, procurement management, asset management, human resources and payroll systems, pension and social security systems, and other possible areas seen as supporting the core modules. The scale of IFMS may also vary and be limited to specific country-level institutions such as the Ministry of Finance. However, IFMS should be used as a common system across government institutions, including the more ambitious schemes for federal, state, and local governments. The integration of IFMS across board ensures that all

---

[176] According to Zachman: 2003, the framework for Enterprise Architecture is a two dimensional classification scheme for descriptive representation of an Enterprise

[177] Shukor bin Ibrahim, the director of the e-Procurement unit under the Ministry of finance stated that IFMS is another major ICT system based on online strategic reporting to facilitate effective decision-making by top management, http://www.futuregov.asia/articles/2011/sep/23/govt-launch-integrated -financial-management-system/

[178] A Case Study on Financial Records and Information Systems in Tanzania: 2002 states that new technologies provide great potential to improve services and efficiency.

users adhere to common standards, rules, and procedures, with the view to reducing risks of mismanagement of public resources[179].

6.4.1 Implementation of IFMS

According to Chêne (2009), emerging ICT can play a major role in fighting corruption and fraud in public finance systems by promoting greater comprehensiveness and transparency of information across government institutions. Hence the introduction of IFMS has been promoted as a core component and a driver of public financial reforms in many countries. IFMS was implemented to: consolidate and replace aging financial systems with modern integrated financial Management systems solutions; develop systems solutions for the enablement of the implementation of the PFMA and new Human Resource (HR) requirements; and to re-focus SITA towards its legislative mandate of Primary Systems Integrator (PSI)[180].

Yet, experience shows that in spite of the considerable amount of resources allocated to such schemes, IFMS projects tend to stall in developing countries, as they face major challenges of institutional, political, technical and operational nature. Case studies of more successful countries such as Kosovo, the Slovak Republic, Tanzania and Ethiopia indicate that factors supporting successful implementation of IFMS include: a clear commitment of the relevant authorities, and technical and operational nature. Case studies of more successful countries such as Kosovo, the Slovak Republic, Tanzania and Ethiopia indicate that factors supporting successful implementation of IFMS include: a clear commitment of the relevant authorities to financial reform objectives; ICT readiness, (as was described in paragraph 5.7); a sound project design; a phased approach to implementation; a project management capability; as well as adequate resources including human resource capacity allocated to the project[181].

6.4.2 IFMS Benefits

IFMS is capable of offering easy and quick retrieval of information and easy communication within and across Ministries/Departments. It can enhance decision making capabilities and can help organisations keep abreast of new technology through upgrading. New technology

---

[179] Chêne: 2009 maintains that the implementation of the Integrated Financial Management System (IFMS) has proved a real challenge.

[180] Maake: 2007's presentation regarding IFMS to National Treasury / State Committee on Public Accounts (SCOPA) members.

[181] An additional benefit is that high speed comparison of data can help identify, promptly, promptly, weaknesses and expectations and alert managers to suspicious patterns of activities.

can improve the running of government to enhance cooperation within departments and across. Improved efficiency and effectiveness will cut costs through the use of a Central Payment Office (CPO); an electronic instruction for payment; one bank account for all ministries; bank account by category of payment and reconciliation of accounts. Advantages and disadvantages of IFMS[182] are offered by Maake (2009) in appendix A. The core components that could usually be managed by subsystems in IFMS include: budgeting; accounting; cash management; debt management; asset management; personnel management; and procurement. With IFMS, data is entered only once and then reused appropriately: unlike in the case of separate systems where there is a possibility for one system to be updated and the other to be neglected, or rather where some accounts could be opened on one system and not appear on the other system in cases of fraudulent activities. Technology enables IFMS implementation practicality: data entry takes where transactions occur and then rolls through the various parts of the application, updating accounting reports against budget estimates and aggregating across units and finally across departments, to provide a whole picture of government expenditure. It is maintained that electronic records generated by the system ensure that transaction records are complete, accurate and authorised: this allows audit trail transactions to be traced through a system forward to its ultimate destination and backwards to relevant source transactions. More sophisticated logging techniques also record who had access to the system at a particular time; what data was viewed in addition to normal logging; and what data was added, deleted or changed. IFMS therefore offers computing techniques that will protect organisations against corrupt and fraudulent activities as well as provide capabilities to detect them[183].

6.4.3 IFMS Challenges

Implementing and maintaining IFMS is a complex task that involves the Ministries of Finance and all line ministries. A number of challenges given are IFMS U4 Expert Answer[184]:

- *Institutional Challenges*: IFMS implies both efficiency reforms that change existing procedures, which should be seen as organisational reforms that deeply affect work

---

[182] Customised Best of Breed COTS; In-House Development Systems and Multiple Options Solutions, Maake: 2007.

[183] The International Record Management Trust holds that In an IFMS, one central database contains all aggregated data and facilitates the flow of information between the inter related system part.

[184] IFMS challenges as offered by U4 Expert Answer.

processes and institutional arrangements governing the management of public finance. Failure to undertake parallel reforms required by IFMS impedes successful implementation. Therefore, the following should be considered: a coherent legal framework governing the overall public finance system must underpin IFMS; IFMS generally imply fundamental changes in operating procedures and should be preceded by a detailed functional analysis of processes, procedures, user profiles, and requirements that the system will support; implementing IFMS requires that many government structures start working with common tools.

- *Political Challenges*: IT reforms are complex, risky, resource intensive and require major procedural changes, often involving high-level officials lacking incentives for reform. Decision makers must be convinced that benefits exceed risks, while the incentive structure that may undermine political "will" for reform has to be adequately assessed from the early stage of the project. Successful implementation requires agencies to recognise the need for a new system.
- *Technical Challenges*: IFMS requires that the basic system functionality be clearly specified from the onset of the intervention. IFMS must be carefully designed to meet agency's needs and functional requirements, including the accounting and financial management tasks the system should perform. In some cases, interfaces with existing IT systems have to be created to fit the country's specific circumstances.
- *Capacity*: IFMS implementation involves considerable human resource requirements and capacity building needs throughout the entire government. The low level of computer literacy in developing countries must first be adequately addressed. The current salary structure and terms of employment in the public sector are usually not attractive enough to compete with private sector employment conditions and to offer better incentives to candidates with required IT-skills. Trained staff leaving for better job opportunities also poses a risk.

It seems a significant move to bring the entire management in Government departments under Integrated Management System (IFMS). However, change management is critical in order to overcome resistance to change by those from the "old way of doing business, those whose work might be profoundly altered by the new system. The integration capabilities offered with regard to government subsystems, raise hope that IFMS, if implemented appropriately and utilised to its full capacity, (as discussed in paragraph 4.3) will help to close the gaps created by isolated systems.

6.4.4 DOD IFMS Contextual Architecture

Brand (2006) and Maake (2009), state that the National Treasury pursued the IFMS project as a State-wide initiative, under the auspices of the Government Information Technology Officer Council (GITOC). The DOD adhered to this calling; hence requirements for the IFMS are being adequately included in the specifications. The Command Management Information Services (CMIS): has established the DEIS Master Plan for the DOD. The DOD representatives' participation in the IFMS project aims at aligning the state of adopting IFMS within the DOD, through the development of the DEIS Master Plan. Initially, a DOD representative acted as nodal point for the interaction between the DOD and the IFMS project members. There has been a shift in this regard which has resulted in this responsibility being allocated to Command Management Information Systems (CMIS) and Defence Information and Communication Technology (DICT) established. The liaison arrangements between the DOD and the IFMS project is a result of discussions with all the relevant role players such as the Chief Director Financial Systems for National Treasury, the Chief System Engineer for IFMS as well as discussions with representatives from the DOD Services and Divisions that will be participating in the IFMS Project. The positioning of DICT as nodal point for interaction purposes is represented in Figure 6.2 below[185].

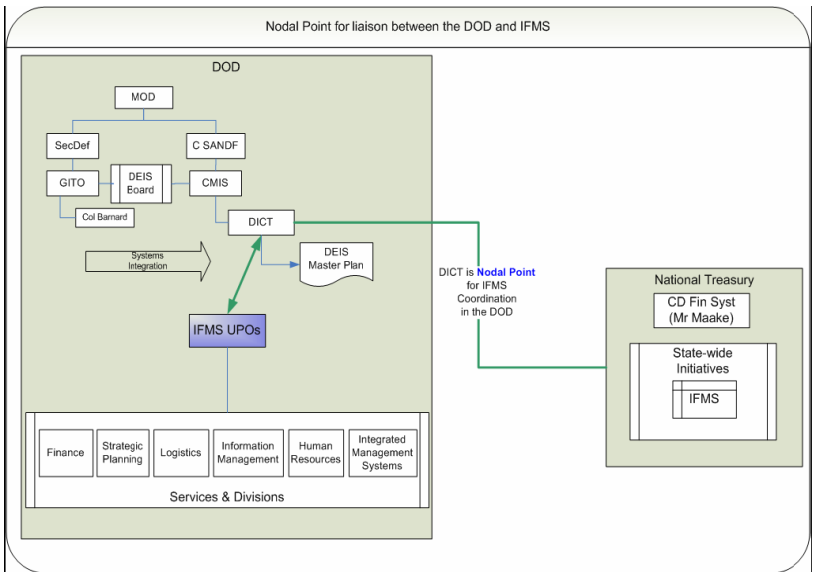

Figure 6.2 Positioning of the Nodal Point for Integration

Source: Brand: 2006. P5.

[185] This positioning is to ensure that all role players are kept informed; and coordinate all internal DOD communications, as well as communication external to the DOD.

All these activities are attempts by the DOD to prepare for IFMS adoption which is hoped will help minimise corrupt and fraudulent activities by promoting a seamless flow of information and offering computerised audit trail where sources and destination of transactions can be tracked.

6.5 Shortcomings of Legacy Systems

6.5.1 Shortcomings of the SCM Transversal Systems

Transversal systems are general administrative systems which were required by all Provinces and departments which include: Financial Management Systems, Human Resource & Payroll Management Systems and Integrated Supply Chain Management Systems. These SCM Government transversal systems' main shortcomings emanate from the need for: support for current, leading and appropriate open standards and technologies; one unified SCM solution for all departments; an integrated solution ensuring user confidence in terms of data, Business Intelligence (BI) accuracy, etc; one support organisation; infrastructure capacity to support a government-wide SCM solution; and functionality shortfalls that include Legislation adherence namely, the South African Assets Management Learners Guidelines version II; Asset Management Framework and Public Finance Management Act (PFMA); Asset Register and administration; Item Identification in terms of National Codification Classification Standards and government-wide roll-out; Operational Management in terms of strategic planning interpretation to service delivery plans and subsequent planning, as well as service delivery logistic support planning; Simplex equipment maintenance management; Infrastructure project delivery management; Procurement in terms of contract management; Inventory management; Sales (Disposal) management; Service (Service provided) management: Distribution management; and Requirements (Demands) management[186]. The growing dependence by organisations on technology requires that they integrate their systems. Having to deal with legacy systems, management has to decide on whether to stick with those legacy systems,

[186] Van Niekerk: 2008 holds that the state of SCM government transversal systems as observable from shortcomings brings out, as the primary opportunity, the development of an integrated SCM business solution to enhance Government's ability to improve core business processes whilst enabling it to facilitate better decision making through the use of information at its disposal. Key SCM business processes within the scope of the IFMS Program are: Strategic Planning and Budgeting processes; Integrated Supply Chain Management Processes; Asset Management Processes; Procurement Management Processes; and SCM Business Intelligence Processes.

which were built without consideration for future integration (stand alone), only because they contain valuable information, or to replace them. The SA Government's move to adopt IFMS displays the intention to get rid of desperate, ineffective unsynchronised systems which tend to open doors for fraudulent activities.

6.5.2 Shortcomings of Financial (FIN) Transversal Systems

IFMS, as maintained by Balim (2008), will address the current FIN transverse system problems and shortcomings in terms of functionality, business systems integration, support interoperability and cost effectiveness. The IFMS FIN solution will be based on an integrated bespoke solution. Shortcomings of the FIN government transversal systems are the lack of: support for current, leading and appropriate open standards and technologies; infrastructure capacity to support government-wide FIN solutions; and functionality shortfalls that comprise: Legislation adherence namely Asset Management Framework and Public Finance Management Act (PFMA); Asset Register and Administration; Generally Recognised Accounting Practices (GARP) and International Public Sector Accounting Standards (IPSAS) compliance; One uniform FIN system solution for all government departments; an integrated solution ensuring user confidence in terms of data, BI accuracy, etc; and one support organisation[187]. Reviewing the performance of these systems and identification of the problems as described has brought about the opportunity for the development of an integrated SCM business solution to enhance government's ability to improve core business processes whilst enabling it to facilitate better decision-making through the use of information at its disposal.

O'Sullivan (2008), on the other hand, maintains that a number of problems that will be addressed by IFMS in transversal systems are that: aging proprietary technologies are reaching the end of their life-span; systems are fragmented and data integration is difficult; and economies of scale are not being realised. SCM systems are problematic in the sense that updating one transaction affects multiple systems; neglecting one system automatically results in confusion, leading to attainment of unreliable information. Obtaining a whole picture of expenditure is impossible due to lack of the rolling through of data entries to various parts of the application and across units. IFMS is viewed as having the capability to offer solution that will provide functionality to National and

[187] A Cabinet memorandum 16 of 2005 was published to address concerns about transversal systems and proposed a new IFMS programme to provide the solution.

Provincial Departments for: Financial Management; Supply Chain Management; Human Resources Management; and Business Intelligence. Laudon & Laudon describes these as applications that focus on gathering, storing, analysing and providing access to data from many different sources to help users make better business decisions[188].

Systems described above are listed in Table 6.2:

PERSAL	**OSIS (DOD & SAPS)**	**YELLOW PAGES (DOJ)**
BAS	**CALMIS (DOD)**	**WALKER (North West)**
LOGIS	**IID (DOD)**	**FINEST (Limpopo)**
VULINDLELA	**VAS/PAS (DCS)**	**SAP (Gauteng)**
PERSOL (DOD)	**OAS (DOD)**	**Premont (NT)**
POLFIN (SAPS)	**SAPVAS (SAPS)**	**PROQURE (NT and DOD, amongst others)**
FMS (DOD) PERSAP (SAPS)	**LIMS including DIMS and UIMS (DOD)**	**Various Departmental Asset Registers and other local systems**

Table 6.1 Financial Transversal System

Source: Van Niekerk: 2008

6.6 Enterprise Application for IFMS

Development of the IFMS architecture is guided by The Open Group Architecture Framework (TOGAF) processes, as stated by Boatwright (2008); Erasmus (2008); Rabie(2008); Bothma (2008); van Niekerk (2008)[189]. Government-wide Enterprise Architecture (GWEA), for South Africa is still work-in-progress. The IFMS Architecture has taken into account previous architectural work done in the Public Service, in particular, the Government Information Technology Architecture (GITA) framework and other work done by the DPSA and SITA. It draws heavily on the experiences and approaches taken by other Governments, including the United States, Canada, and Australia, O'Sullivan (2008), and the Slovak Republic, Kosovo, Tanzania, and Ethiopia[190]. This then informed the choice of the

---

[188] O'Sullivan: 2008 states that transversal systems used by the Public Service vary widely according to age, architecture and technology. They are fragmented, they do not support new legislative requirements and they do not realise economies of scale.

[189] The architecture will comprise a number of principle dimensions: Business Architecture, e.g. organisation, users and required business processes. Application Architecture, e.g. the business application supporting the business processes; Data Architecture: e.g. the data to be processed by the application; and Technology Architecture, being the overall technical infrastructure.

[190] In spite of challenges involved as well as many failed implementation attempts across the world, there are a number of countries where IFMS implementation is viewed as having been a relatively smooth and successful process.

framework (Zachman) and the architectural methodology (TOGAF) used to develop the architecture. By using internationally accepted tool–and technology-neutral approaches, the IFMS Architecture will integrate easily with other architecture initiatives in Government, O'Sullivan (2008)[191]. The following frameworks, as given by Tuganadar (2008), will guide policies and processes for the governance of IFMS as a minimum, *CobiT,* automated control objectives; *TOGAF* and *Zachman*: IT architecture; ITIL: IT Service Management; PMBOK and PRINCE2: project management; and ISO 17799: security.

6.6.1 Architectural Framework and Methodologies

There is correlation between the structure of an organisation and that of its software. According to Tuganadar (2008), numerous frameworks have been considered to produce an Enterprise Architecture (EA) model for IFMS. Only four complementary frameworks, namely, Zachman Framework[192], the Open Group Architectural Framework (TOGAF) and ISI 12207[193], and the Federal Enterprise Architecture Framework (FEAF)[194], were chosen and applied. O'Sullivan (2008) holds that the Zachman proposes a logical structure for classifying and organising the descriptive representations of an enterprise. The Zachman framework is said to be flexible in that it allows each organisation to determine what type of documents and models it will include in its enterprise architecture (EA). The main strength of the Zachman framework is in the collective description of the organisation and its assets. TOGAF is introduced to counter for the lack of adequate methodology processes and tools in the Zachman framework[195].

6.6.2 IFMS Approach

The Open Group, an international vendor and technology-neutral consortium, developed the TOGAF Version 1 in 1995, based on the Technical Architecture Framework for Information Management (TAFIM). Erasmus (2008) states that TOGAF provides a best practice model for the implementation of IFMS within departments. Used for architectural development as

---

[191] O'Sullivan: 2008's contribution on IFMS framework and the architectural methodology.

[192] Land: 2003 states that the Zachman Framework for Enterprise Architecture", promoted by Zachman Institute for Framework Advancement (ZIFA), is a framework within which a whole enterprise is modelled.

[193] ISO 12207 provides guidelines on the content that should be included in a software development lifecycle, O'Sullivan: 2008.

[194] The set of Reference Models used by IFMS was adapted from the US Federal Enterprise Architecture Framework (FEAF, which has been used by a number of other Governments internationally.

[195] The framework is structured around the views of different users involved in planning, building, and maintaining organisational Information System.

well as for support in building business, applications, data, and technology architectures; Pienaar (2007); and O'Sullivan (2008). TOGAF has an Architectural Development Model (ADM), a Technical Reference Model that provides taxonomy of generic platform services, and a Standards Information Base (SIB) – a database of open industry standards. The use of internationally accepted approaches, which are tool-and-technology-neutral, will help the IFMS Architecture to integrate easily with other architecture initiatives in Government.

The TOGAF framework is composed of ADM, referred to as the core of TOGAF, a step by step approach providing the processes and method to developing enterprise architecture; the Enterprise Continuum, being the set of architectures, reference models and products used to create the organisation specific enterprise architectures; and the Resource Base, which is considered the basic best practice tools and techniques used to guide and create the architectures[196] in the Enterprise Continuum - O'Sullivan (2008). However, Tuganadar (2008) states that the Zachman Framework, TOGAF ADM and ISO 12207 do not spell out how the architecture can be realised. The widely used FEAF by Governments in the USA, Australia, Canada, and so on, is used as the model to realise the IFMS architecture. IFMS has taken the TOGAF architecture development cycle (ADC) and customised them to provide adopted processes that will be undertaken by IFMS to deliver the architecture. Phases that will be covered into five major milestones have been summarised by Tuganagar (2008) as: Preliminary Phase; Framework and Principles; Phase A: Envisioning the future state. Phases B; C; and D: Developing architecture specifications; Phase E and F: Developing release plan for solutions; Phase G: Managing deployment and realising value; and Phase H: Managing Change[197].

An iterative process must be followed in order for the architecture to be realised at each level of abstraction. Each iteration evolves the Zachman Framework's perspectives (level of abstraction) further with the defined reference models hierarchy, as depicted in Figure 6.4

---

[196] According to van Niekerk,: 2008, the SCM conceptual Application Architecture addresses the following views: Business Applications, Application Integration and External User Interfaces. It supports Phases "C" of TOGAF. Balim: 2008 holds that the IFMS Conceptual Architecture: Financial Management (FIN)is a product of the IFMS Enterprise Architecture (EA) framework supporting the conceptual viewpoint and data, function, people and motivation aspects as defined in the Zachman Framework for Enterprise Architecture and adopted by the IFMS EA framework. It also supports the TOGAF Business and Information System architectures cycle also adopted by the IFMS EA framework.

[197] O'Sullivan: 2008 adds that the Master Systems Plan (MSP) detailing the project objectives and functional scope. Phase II, Capacitating and architecture, was primarily aimed at preparing SITA to assume its role as the Prime Systems Integrator (PSI) and to produce this overall IFMS Architecture as its initial key deliverable. In Phase III: Development and implementation detailed system specifications will be developed for each function requirement identified in the IFMS Conceptual Architecture.

above namely *Architecture Iterative Process*. The first iterative results in the contextual "City Planning" view and the second iteration results in a conceptual "Enterprise Model" view. This is basically the Enterprise Architecture deliverables of IFMS. The third iteration provides the logical "System Model" view or system specifications. This will use the adopted ISO 12207. The lifecycle, caters for software, has been extended to include a system perspective that includes technology. The lifecycle will include the Concepts of Operation (IEEE 1162) user view of the system. The System Requirements Specification (IEEE 1233) will define the release specification as the development view of the system and this includes application, data, and technology requirements. The next iteration, namely, the system engineering phase, realises the software specifications. The build, test, support and maintain phases are not described in the framework but will be further elaborated on in the System Engineering Master Plan (SEMP). This will include software development methodologies such as the Agile Methodologies[198]. An Architecture Iterative Process is represented in Figure 6.3 below:

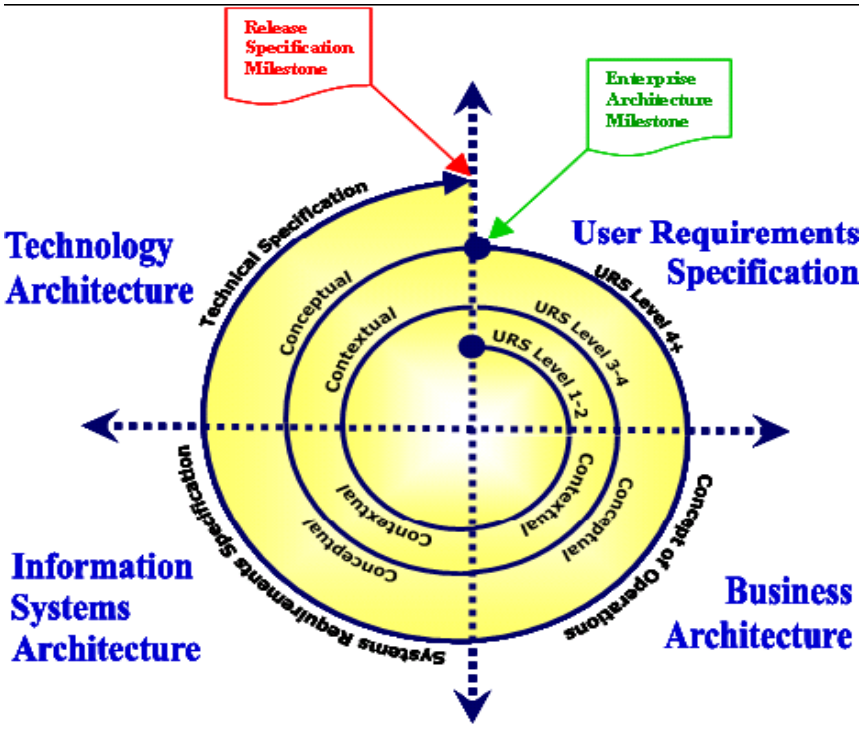

Figure 6.3: Architecture Iterative Process

Source: Tuganadar: 2008. P26

[198] The integration team shows determination in developing a basic system to link all the information the system needed into one structure. The system will gradually move forward, becoming what some will consider being one of the most effective IFMS. IFMS implementation team will then set out to install and configure the basic system architecture that would work for the entire future administrative structure, based on an assessment process identifying available human resources and system requirement.

6.7 Solution Scope: DOD Vehicle Management Systems: The Proposed IFMS

Tuganadar (2008) clarifies that full control and visibility of the Government assets and supply chain functions will be supported by comprehensive IFMS SCM sub-system solution from requirements through planning, acquisition, procurement, and logistic support to service delivery (operations)[199]. Van Niekerk (2008) goes further to identify the solution functional scope as including: Operations Policy Administration; Operations Delivery Planning; Operations Support Requirements; Operations Activity Execution Planning; Operations Technical Support Administration; Accident/Incident Management; Operations Execution Monitoring; Operations Management Reporting; and Operations Management Performance Monitoring. The operations management subsystem will support effective government operations (service delivery) planning and execution management (primarily for equipment operations execution such as vehicles). Legacy systems will be replaced by the common operations management functionality of OSIS and CALMIS, which are government transverse legacy systems within the DOD[200].

6.7.1 Prioritisation Conditions

IFMS functionality requirements will include both common current transversal systems functionality and new functionality. The priorities for developing the IFMS Roadmap and Release Plan have taken the fast-tracked COTS systems, namely: Human Resources Management, Procurement Management and the bespoke Asset Register, as first priority: any system functionality that replaces the current transversal systems with priority, given first to National Treasury system (BAS), PERSAL, LOGIS, and VULINDLELA to be second priority; and thirdly, system functionality that addresses Government objectives and priorities. Different Roadmap options, based on the considerations, principles and priorities, will be evaluated and a recommendation will be provided. The IFMS Steering Committee will decide upon the final accepted roadmap (Tuganadar - 2008).

---

[199] IFMS is inclusive of all SA national and provincial departments. This includes a total of 140 departments: 91 national and 49 provincial departments.

[200] SCM subsystems include Item and Service Identification; Asset Management; Operations (Service Delivery) Management; Maintenance Management; Service Management; Inventory Management; Procurement Management; Distribution Management; Sales (Disposal; Administration; and Requirements Management.

6.8 IFMS Roadmap Model and Options

In an attempt to adhere to the government proposal of the implementation, the DOD-SITA designed and proposed 3 options. These options are still to be presented to government for approval. Government is expected to choose a viable and preferred option from the three proposed options. As a result, it is not known which option is going to be followed. Information about the IFMS roadmap Model and Options was described by O'Sullivan (2008), who maintains that government operates within a cycle that goes through strategic planning, operational planning, budget implementation, and year-end reporting. The cycle is informed by policy development that is provided by parliament, provincial legislature and municipal council (excluded from IFMS). IFMS will be a key support service to Government as it enables management information and knowledge. This implies that for IFMS to be aligned to the needs of Government, the roadmap of IFMS will be shaped by the planning, budgeting and reporting cycle of Government so that the priorities of Government are supported by the delivery of IFMS. Figure 6.4 represents the IFMS Roadmap Framework:

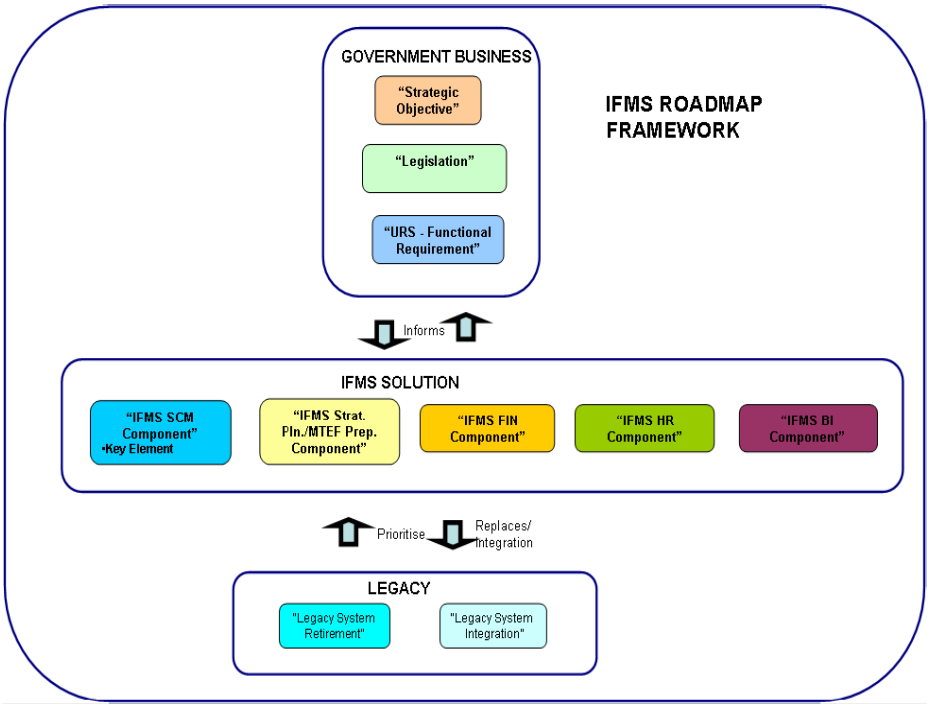

Figure 6.4: IFMS Roadmap Framework

Source: O'Sullivan: 2008. P38

Three major perspectives include: Government Business; IFMS Solutions; and Legacy Transversal Systems have been contextualised in the IFMS Roadmap Framework. Also included are relevant artefacts that are considered and modelled for the IFMS roadmaps. The

Government Business are said to include government strategic objectives determined by the planning, budgeting and reporting cycles. This is the proposed solution, which determines all aspects of the user requirements. IFMS Solution is aligned to legislation found to be driving all aspects of the user requirements, with current transversal systems functionality incorporated. Current Legacy Transversal Systems will be eventually retired, even though transitional period might require interfaces. In the roadmap, each release builds towards the full solution, and provides intense functionality with each of the strategic planning, budgeting, monitoring and accountability reporting annual cycle iteration. The first layer of the roadmap is said to indicate the Government Business perspective. The releases focus on the functionality needed to meet the requirements of the Public Finance Management Act, including GRAP for accrual accounting, Budget and Treasury guidelines.

Key processes will be used to present the User Requirements Statement (URS), which is aligned to relevant legislation. These key processes are: Supply Chain Management; Integrated Strategic Planning and Medium Term Expenditure Framework (MTEF); Financial Management including Budgeting Execution; Human Resources management; and Integrated Business Intelligence. The next layer, as maintained, indicates the IFMS Solution and the relevant functional components that should be built or acquired to fulfil the Government Business Layer. Functional components of the Government Business Layer are divided into two segments, whereby the upper deals with primary segment which directly support the Government cycles. The releases focus on functionality transactions that bear support components that may be required by primary components to fulfil its objectives. Although the dependencies to support components form part of the overall roadmap options, the primary components are considered the critical path for IFMS[201], IFMS options by Maake (2007) are given in Appendix A.

IFMS was adopted and developed to meet challenges around a lack of systems integration in functions such as HR, where there was a need to modernise and consolidate a historically fragmented administrative environment into one that is integrated, with the aim to ensure improved effectiveness accountability and manageability. After seven years SITA, in collaboration with DPSA, has been involved with making sure that IFMS is delivered, and

[201] The number of legacy systems involved, and the wide functional scope of the business domains, means that the phasing-in of IFMS is necessarily complex because of the inter-dependencies between the systems. A number of different sequencing options is possible, depending on: the appetite for risks of Government systems; the complexity of the sequencing and the dependencies between modules; the costs incurred to develop the new system; and costs saved by phasing out legacy systems, O'Sullivan: 2008; Tuganadar: 2008.

that e-commerce, in terms of technology, has laid a foundation for the adoption of IFMS via its requirements for organisation to be IT ready. The first module, the HR module, has been delivered and its delivery marks the commitment by government to modernise and consolidate a historically fragmented administrative HR environment into one that is integrated, to ensure improved effectiveness and efficiency.

It was observed in Chapter 3 that corruption and fraud thrive within SA government departments, threatening good government in the country and the public service. Therefore, fighting it remains a major challenge. Through the completion of the remaining IFMS modules, government will be in a better position to eliminate activities of personal gain, which, in the HR environment, are often perceived to be the result of internal manipulation of the systems for personal gain. Such activities include transactions such as fictitious (ghost) workers, abuse of leave and identity fraud. The module will enable us to better manage the disciplinary process in the public Service. It is envisaged that the completion of the VMS will help to counter fraudulent activities such as vehicle theft, unauthorised private use of vehicles, theft or substitution of accessories or tools, falsification of vehicle logs, misuse of vehicles, use of petrol on private vehicles, etc. On the FIN module part, IFMS capabilities will help to combat fraudulent transactions where employees knowingly access computers without authorisation, promoted by the nature of existing legacy systems. Employees intentionally defraud without authorisation and conduct illegal transfers of fund.

6.9 Conclusion

This chapter presented the DOD IT infrastructure and highlighted some problems experienced by the DOD and the SA government in general. IFMS was discussed as the government initiative to replace existing legacy systems in order to promote accountability and manageability, finally resulting in something more tangible to make fraudulent and corrupt activities more visible and transparent. This expected outcome of curbing fraud and corruption could be further enhanced by the integration of IFMS with the VMS. Progress in terms of the IFMS was also highlighted in the previous paragraph where government has experienced the first presentation of the IFMS module, namely the HR module that will help to counter corrupt and fraudulent activities in the HR environment. The findings as to what factors affect application integration perceived as a possible combatant against fraudulent activities will be presented in the next and last chapter.

Chapter 7

Findings and Recommendations

7.1 Introduction

The findings communicated here are presented with regard to factors affecting systems integration. These finding are drawn from site visits, observation and interviews conducted with different organisational members and from the DACAF database. DACAF whistle blowing reports regarding the DOD system reveal that corrupt members use the system's weaknesses to their advantage. Factors impeding application integration are divided into two levels, namely, government level due to the role played by government oversight; and departmental level which refers to the DOD as the unit of study.

7.2 Factors impeding Systems Integration: Government Oversight Level

Firstly, some functional application software were decided on/prescribed by the Government, such as for Finance and Human Resources. Integration with any other organisational programs/applications was prohibited until further investigation could be concluded. Today, it is expected that all IT applications should be able to speak the same language, i.e. to communicate across functional silos. The challenge is therefore to find technical solutions to problems arising from application incompatibility. The findings of the research identified the factors, outlined in the following paragraphs, which could be perceived to be of significance.

7.2.1 Aging of Software Applications

The legacy systems currently in use provide financial, human resource and supply chain functionalities. They were developed before 1994. As a result, it becomes difficult to keep them aligned with new legislation; it therefore becomes difficult if not impossible to support the needs of government departments. It was unfortunately found that the structures and cultures of these departments prevented seamless flow of information throughout the governmental organisations which by association include the DOD and its IS/IT systems.

7.3 Factors Impeding Systems Integration: Departmental Level

7.3.1 Organisational Culture

Be it due to internalised norms, beliefs, or resistance to change, the DOD however, displays culture as a factor hampering integration of applications. The fact that high ranked posts are perceived as political posts, brings with it changes with regard to who occupies these posts and for how long. New occupants to these posts bring along dramatic changes with them, whereby each occupant prefers to run things his or her own way. Members occupying these positions should at least have the knowledge that IT adoption/integration processes, especially those that require changes in business processes, may require changes in culture. It was found that unfortunately, the importance of systems integration is not given the necessary consideration as perceived by those in authority.

7.3.2 Organisational Structure

The DOD consists of a hierarchical bureaucratic structure wherein everyone is accountable to someone and authority is limited to specific actions. Authority and actions are further limited by abstract rules or procedures (standing operating procedures - SOPs), politics and culture. The structure consists of divisions and represents the military arms of services. This study was focussed on the four Arms of Service in terms of its vehicle management systems. These Arms of Service offer different services and this resulted in an organisational design that attempts to deal with technology by means of different processes of control at different levels, thus creating problems. The leadership in these services tends to wheel and deal in pursuit of their own organizational interests, which is somewhat common to most government departments. Attempts made to integrate vehicle management systems in these services failed because leadership define integration in terms of their area of operation rather than focusing on the DOD as a whole.

7.4 Corruption and Fraud Factors

7.4.1 Government Level

Considering the factors of corruption discussed in Chapter 3, evidence was found that indicates that the SA Government is faced with serious problems in terms of corruption and

fraud. Most respondents, when tackling the issue of causes of corruption and fraud mentioned factors such as greed, boredom, intent, poverty, etc. Whilst on poverty, the latest research on "Poverty and Inequality in South Africa", by the European Union (EU) Program to support Pro-poor Policy Development (PSPPD)[202] also highlighted, besides education and unemployment, other critical issues considered to be structural in nature because of possible legacy systems such as those that was created due to "apartheid"; systems which created different opportunities for people based on race, gender and/or class. Some respondents went further to mention that a significant part government leadership is composed of members who experienced the apartheid era and that some of these members attempt to make up for the inequalities created during the apartheid regime by rejecting possible useful legacy systems.

Some respondents focused on the government as a starting point for corrupt and fraudulent activities that transcend throughout organisations and mentioned that: the negative impact created by poverty and hostility on member's lives during apartheid holds that change will not happen overnight; the process followed on the appointment of leadership members by political parties is not based on the level of education of candidates but to their political commitment; changes will occur with the next generation; lack of member vetting/profiling which could have helped to identify potential fraudsters; a yearning to fill the inequality gaps created during apartheid; lack of commitment displayed by government leadership and weak systems that attract some corrupt and fraudulent migrants; and the misuse of authority to benefit family, relatives and friends as a means to uplift their standard of living before their term ends[203].

7.4.2 The Operation of the PSC

South Africa has responded actively to the fight against corruption, since it is a global concern that seriously hampers development and diverts resources from where they are needed most. As part of monitoring the anti-corruption strategy, the PSC assessed the most common manifestations of corruption and their related risks in the Public Service. It is revealed in a report titled "the Anti-Corruption Forum Civil Society Indaba", dated June 2011 that 40 percent (40%) of the sampled departments have anti-corruption policies of reasonable quality with evidence of implementation. The remaining 60 percent (60%) either has no

---

[202] This research came out of 13 research projects which were funded by the European Union aiming at understanding how economic and social policies impact on people's lives.

[203] Prince: 2011 maintains that the spy boss registered his relatives, girlfriend and their families as covert intelligence operators and paid them as such.

policies or has very basic policies of poor quality. As indicated in Paragraph 3.4, Cabinet approved the National Anti-Corruption Forum in the year 2000. The role played by PSC as well as the importance of having anticorruption structures becomes questionable if there are still, to date, departments referred to as not having established anticorruption structures[204]. The following are concerns regarding the PSC mandate:

- The way in which the PSC could ensure that each and every Government department adheres to the Government instruction to have anti-corruption structures;
- The effectiveness of PSC in overseeing/monitoring the activities of structures at departmental level; and
- How the PSC ensures that reported incidents are not closed by officials before they are even investigated; where officials use their own discretion but concerned whistleblowers keep insisting on investigations to be conducted.
- Lack of integration between PSC and the rest of the organisations for corruption and fraud databases.
- Lack of capacity to investigate and monitor reported incidents caused by lack of experience; a factor that could be attributed to structure of recruitment procedures[205].

7.4.3 Departmental Level

DACAF is observed as clouded by, as per PSC requirements, the following:

- *Substructures*: The many DOD substructures lack system integration aimed at attempts to fight against corruption and fraud.
- *Equipment*: DACAF computerised system (ARS) does not record each and every incoming complaint as maintained in the UN Report of 2001. Only those incidents where officials, by using their discretion, decided to investigate are entered into the system. A spreadsheet is used separately to record incoming complaints. Information retrieved from the system does not involve:
    - Value of identified fraud loss
    - Duration of individual investigations
    - The cost of investigations

---

[204] The PSC Report: 2000 states a database as one of the Hotline requirements. No specification has been made of the software application specification was stipulated: the application that will promote standardisation and integration between the PSC and the departments it is to observe and evaluate.

[205] Different political parties raised their views regarding the management of the anti-corruption strategy as follows: "appointing people with no experience…makes a mockery of government's commitment to fight corruption"; and "institutions expected to deal with corruption are toothless", Kotlolo: 2010.

- *Staffing*: DACAF experiences incapacity due to understaffing. According to the Defence Secretariat Annual Performance Plan (2011), the department has a large number of vacant posts (Civilian) across all levels[206]. Staffing on the part of uniform members also has a tremendous impact on DACAF performance. Staffing of uniform members depends on Chiefs of Services recommendation as well as on who should be promoted based on military course qualifications. This might have a negative impact should the member accept transfer for promotional sake, whilst not interested in the key responsibility areas of the member's present posting.
- *Alignment*: The Anti-Corruption Strategy which is the initiative of the Public Service Commission, should have been used as the basis to review the DOD strategy, as such

The SA Government anti-corruption and anti-fraud strategy is viewed as an important factor regarding the findings of this research. However a factor that will be even more important will be the actual successful implementation of such a strategy

7.5 Problems to be Solved to Enhance Integrated Systems

7.5.1 Human Resource Practice

Most units display failure adhering to DOD transport management policies and procedures as stipulated in 2.1, as well as to perform well due to lack of structures or sufficiently qualified personnel. Detached duty is common practice in the DOD, especially as applied on uniform members. Accomplishment of most DOD activities/objectives depends highly on transport, however, it was discovered during site visits and interviews that while some units do not have proper transport management structures, some suffer from lack of enough personnel to manage these sections. This, to some extent, is the result of members being wrongfully placed and members being detached to perform duties they never received training for, in those specific fields. Being on detached duty means one is not permanently placed in the post detached to. Members detached in units where there are no transport structures displayed lack of satisfaction and motivation due to the belief that they could have been placed permanently in those posts. Lack of motivation leads to underperformance, which affects updating of records, non adherence to policies and leads to supply of incorrect reports to senior managers.

---

[206] The Department has therefore, as its desired standard, to reduce the turnaround time of filling the posts to six months from the date of their becoming vacant.

The eventual result being lack of accountability and manageability toward state funds and subsequently, lack of accountability and manageability opens doors for corruption and fraud.

7.5.2 Transport Policies and Procedures

The South African National Defence Force (SANDF) offers training to its members in different fields. One such field is training offered to members to become technicians in the field of Motor Repairs and Maintenance. There is an outcry from some units that processes and procedures with regard to taking vehicles for repairs and maintenance are too long and exhausting; too long in the sense that processes might take two to three months just for preparation; exhausting in the sense that, for example, quotations obtained from civilian companies, expire whilst awaiting approval from authorities or budget managers. With expired or almost expired quotations, the whole lengthy process has to be repeated. In some cases, after having undergone the whole process and after approval has been obtained, funds are no longer available. These factors lead to unacceptable levels of unserviceable vehicles.

7.5.3 Equipment

The DOD historically lacked knowledge of all state assets it owned as a result of the lack of proper recordkeeping systems, be it manually or electronically. For this reason, the Chief of the Army instructed that a census project, “Project Libidi 2009” be conducted. This project is aimed at enabling management to know what is available and what is not, as well as to make informed decisions as to how to manage different conditions of vehicles and to assist units to engage in disposal of surplus and redundant items. An instruction was issued bearing the objectives to: determine the quantity, types, makes and models of vehicles and serviceability of available vehicles in the SA Army; determine the accuracy and correctness of records in the Equipment Asset Register (ER) and the National Codification System (NCR); and, if needed, to update the records and population of vehicle records on CALMIS; determine the owner or holding unit; create a profile of each military vehicle in the SA Army; mark vehicles with unique identifications to indicate census application; obtain credible information of the SA Army Vehicle Master Plan; obtain credible input for the phasing out and disposal of vehicles; and initiate and implement system changes to CALMIS to improve control of vehicles. Some members involved with updating CALMIS regarding this project felt that the project might prove fruitless if the Army does not attend to the problem of lack of personnel within transport sections. Their concern revolve around the fact that some members updating CALMIS are Reserve Force members who got called up only for the project; on

completion, they will have to leave and the then Army has no guarantee that the usual staff members will keep the system updated and concurrently running satisfactorily. Thus situation again lends itself to promote fraud and corruption. The integrity of a sound database is therefore, a critical factor to asset management and dependable systems integration in the fight against fraud and corruption.

7.5.4 Toll Forms

One of the documents mentioned in paragraph 6.2: C LOG/DSSS/R/401/2/2/B dated 28 September 1995 (Implementation Instruction: Toll Plaza's) is about the utilisation of Toll Plazas within the DOD. Members are allowed to produce Toll Plaza forms obtained from DOD transport offices, authorised and approved; members get exempted from payment at tollgates by merely producing these authorised forms. Control measures around the management and safekeeping of these toll forms pose corruption and fraud threats. Even though most respondents maintained that safeguarding of toll forms are ensured, the possibility for corruption and fraud to occur was observed as follows:

- In some units, the toll gate template is saved on the officer's memory stick, which could be misplaced or lost: whoever picks it up may print out as many forms as possible and they could be approved and utilised fraudulently;
- In other units, copies are in paper format and it is maintained that they are locked un-safely but: in most cases, these copies were just lying around and could even be reached by those with wrong intensions.

These cases illustrate that not only should the systems integration and integrity be addressed but that serious attention should also be given to systems abuse and manipulation through addressing the human factor of organizational culture and attitudes.

7.6 Recommendations

Government Oversight

It is an expectation that the implementation of IFMS will cover the lack of systems integration within the DOD, including all other government departments. Since its aim is to integrate functional systems, the problem of lack of systems integration could be solved and fraud and corruption could be curtailed. Departments should ensure that new applications in

planning are integrated in order to avoid re-creation of previous lack of application compatibility and adaptability.

Ageing of Software Applications

The perusal of IFMS Project by the National Treasury serves as proof that Government chose, though regarded as the most expensive option, to replace the legacy systems within government institutions. A positive step, as explained in paragraph 6.3 above, will be that government organizations be allowed to expand their IFMS with non-core subsystems in addition to core-subsystems. This step could once again enhance compatibility and adaptability.

Organisational Culture

The DOD leadership should approach strategy formulation by appreciating that, in terms of application integration, "strategy making is a process of enactment that *produces* a large element of the future with which the organisation will have to deal; this can empower the DOD leadership to take responsibility for the future in an active way and help them appreciate that they themselves often create the constraints, barriers, and situations that cause them problems", Morgan (2006).

Organisational Structure

The transport management environment needs to be revisited. DOD leadership should start to strive towards one goal, especially with respect to centralised functions. Although there is a need for changes in technology, rules, systems, processes, and policies, leadership should note that change programs must give attention to the kind of corporate philosophy required in the new situation and find how this can be developed.

Policy statement and Fraud Response Plan

All department should ensure that the anti-corruption policies, as discussed in paragraph 3.4.1, include features such as: reporting of all losses of money and allegations of offences; fully investigating illegal acts against the government and other improprieties; and reporting all suspected offences to the responsible law enforcement agency. Departments should ensure that employees are aware and being periodically reminded of their personal responsibility to report any knowledge of a contravention of government laws or regulations. Steps also to be taken are reasonable measures by departments to protect the people reporting offences and improprieties and people against whom allegations are made; people should be made aware

of these measures and procedures to deal with tip-offs about alleged losses, offences, and improper practices, however obtained or received, whether anonymous or otherwise. Managers who fail to take appropriate action or directly or indirectly tolerate or condone improper activity should be held to account.

SA Anti-Corruption Strategy:

- Ten if not eleven years went by after the approval of the Anti-Corruption Strategy: yet there are still departments who never adhere to the Government's calling. To counter acts of non-adherence, the PSC came up with a policy such as that in Appendix B; which could also be coupled with the principles given in Appendix C. The PSC could also develop and implement imposition of penalties to those departments not fighting against corruption and fraud as required.
- The issue of failure to integrate anti-corruption databases between the PSC and other government departments could still be addressed with the implementation of IFMS. The PSC, to be enable to execute its mandate which could ensure that a system be designed and communicated to SITA. This computerised system should consist of fields as described in paragraph 3.5.3 above, which will allow the PSC to monitor the activities of subordinated departments.

International Intervention

Nothing stops the SA government from seeking international intervention with regard to corruption and fraud issues. The PSC, as per its mandate and in conjunction with other departments, may receive co-operation of organisations such as CICP and SAIs in order to learn and adopt good practices that will upgrade the level of standard for fighting against corruption and fraud. DACAF should consider offering education and training to members through the following: investigative journalism workshops which should aim to create a more active role of the media in describing the negative effects of corruption and fraud; and utilisation of international instruments such as *The TI Sourcebook* and the UN's Anti-Corruption *Toolkit*, both of which are presenting experiences of other countries in combating corruption[207].

---

[207] To emphasise on the role of investigative journalism, the UN Office for Drug Abuse and Crime Prevention: 2000 states that Uganda began to train its investigative journalists with donors help in 1995. A preliminary assessment, which will be validated by context analysis, shows that training and awareness-raising among journalists has had a positive effect on the frequency and quality of reporting on corruption. The lessons learned from investigative journalism workshops in Uganda have been transferred to Tanzania, Mauritius, Benin, Malawi, Ethiopia, Ukraine and Nicaragua through regional workshops, study tours, and exchanges.

DOD Anti-Corruption Structures

DACAF requires restructuring and realignment. It could be beneficial to the DOD should DACAF be re-aligned and placed within the Secretary for Defence (Sec Def), simply because as it is a Public Service initiative, the issue of member levels hampers investigations by uniform members, whereas there should not be any such limitations on the part of Civilian members. By directly reporting to the Sec Def, DACAF will be in line with the Directorate Risk Management, which reports directly to the Sec Def. There are many anticorruption substructures within the DOD that are disparate and not aligned. DACAF should therefore serve as a nodal point for those substructures. Having a centralised model operating within the department could have benefits such as sharing of best practices and quality control processes.

Complaints Office

Some whistle blowers have started losing faith in DACAF because their perceptions are that DACAF does not address their problems. This occurs despite of DACAF's mandate to expressly address corruption and fraud related matters. Problems used to be referred to the Complaints Office where the necessary action used to take place. Now that the Complaints Office does not function anymore, DACAF refer such matters to the relevant authorities and/or to the individuals themselves. Members not being aware of the DACAF mandate now feel neglected and unattended. It is therefore important that the Complaints Office be re-established which should attend to members personal problems regarded as not being corruption or fraud by DACAF. DACAF would be able to accommodate the complaints office, should the personnel and their capabilities be increased. This could be a viable solution since DOD members are now used to reporting to DACAF. Combining DACAF with the complaints office will help DACAF to perform a clearing house in order for those complaints alleging inefficiency rather that corruption and fraud to be forwarded to the appropriate authorities.

Awareness Training

DACAF should put in more effort on making people aware of possible consequences of committing corruption and fraud by strengthening awareness training programs and by publicising details of success stories where action has been taken against perpetrators of fraud. DACAF is also required to develop its own website where members could blow the whistle and even sign the pledge. The website could also assist members to make comments

about how, what they reported, was handled by DACAF. This could help DACAF assess and evaluate its activities.

Training of Anti-Corruption Structures Personnel

Any fraud committed with the aid of a computer or network is considered computer fraud. Foiling computer-based fraud, in today's highly automated business environment, has therefore become a top priority since skilled computer experts, international criminal organisations, and even seemingly honest employees steal identities, re-route data for personal gain, and alter data for fraudulent purposes. The existence of this pervasive crime serves as motivation enough for government employees involved in combating corruption and fraud to engage in seminars that will train them to: examine the key risks surrounding computer-based fraud and explore the who, what, and how; investigate specific IT controls that must be in place to reduce the risk of computer fraud and logical access controls, reduced privileged access, networks controls, encryption, and application system controls, and benefit from real-life examples of their effectiveness. High impact seminars will expose them to the types of monitoring software tools; help them perform data analysis and moving to continuous monitoring, integrated roles of IT and business process owners, security policies and awareness and information classification.

Human Resource Practice

The Arms of Service could conduct a human resource project to, investigate/audit units in need of personnel (Transport Officers), determine the number of Transport Officers required, and ensure that enough personnel is supplied to affected units. The allocation of such needed personnel should be made based on individuals trained specifically for the kind of jobs required and not on the basis of which personnel, regardless of competency is available at the time of need. If need be such, then on-the-job training should be implemented and officially monitored for adherence to standards. Structures should be developed in areas where there is a need for improved management functionalities. (it is now more that 2 years that the anti-corruption structure has been promised a head with the rank of Deputy Director General, an activity that will help align the anti-corruption structure correctly within the Secretariat of DOD - to date, a candidate has not yet been appointed and employed).

Transport Policies and Procedures

Leadership responsible for policies and procedures within the transport environment should respond to the lack of proper structuring by revisiting these policies and procedures in attempt to shorten procedures that hamper progress in vehicles repairs.

Equipment

Project Libidi 2009 is good practice by the Army, but it could have been more valuable if it were conducted simultaneously in all DOD spheres of transport; especially in preparation for the implementation of IFMS. This could have ensured feeding IFMS with accurate data/information of all DOD assets; attempts should also be made to maintain continuous updating of the systems.

Standardisation of Toll Forms Control

IFMS should be re-designed to produce "Electronic Toll Forms" in order to strengthen control measures over toll forms. Manual forms may only be used when systems are down. The DOD could also make it a point to obtain printouts of transactions made against its name, either quarterly or bi-annually, for comparison purposes, as well as to determine how much is spent on toll forms at the end of the financial year.

7.7 The Way Forward

7.7. 1 Government Level

It is important to refresh the minds that a new democratic society was hoped for and established as the outcome of casting of votes by South Africans in 1994, the products (hope and spirit) of which was recorded in the Constitution of South Africa. However, hope was lost in many government leaders as a result of allegations of corruption and fraud reported against some of those leaders, such as "Police chief expected to be suspended this week"[208]; "Dirty secrets of SA's spy Agencies"[209]; and "Minister has no credibility"[210]. The way forward starts by addressing issues at government level since it has as its duty and responsibility to offer oversight activities to government institutions. The situation gets even worse to realise that the "inquiry into alleged irregularities in strategic arms-procurement packages could implicate senior ANC and governing leaders, including President Zuma and

---

[208] Hofstatter et al: 2011 wrote about what they call two dodgy police deals worth R1.-billion which implicate the National police commissioner.

[209] Kgosana: 2011on the financial mismanagement that rocks the South African Intelligence Services.

[210] Zwane: 2011 the Public Works Minister is said to have finally admitted that her department is in crisis and riddled with corruption.

possibly former president Thabo Mbeki"[211]. Given such a situation, government leadership, including the President, should start rebuilding the image of a government of integrity, responsibility and accountability towards its citizens, before things get worse. The necessary change should start from top downwards, and attempts should include:

- Maintenance of a decisive position by the President – the President could avoid further disorientation of the masses by avoiding what the masses could consider to be delaying tactics like in the case whereby after receiving a report from the Public Protector involving the National police commissioner, the president maintained that he needs time to go through the report – the masses need immediate, spontaneous and responsible response;
- The President decision should be final: it should be ensured that a decision made by the president is implemented without challenge, for example, when reshuffling of the Gauteng Provincial Government was put on hold after Gauteng Premier's resistance to the idea[212]. A situation like this could prove insubordination to the masses and that the President's decision was not valued;
- The process of reshuffling should involve replacement of those acquitted with credible individuals rather than moving around those under-performing from one organisation to another;
- The president to consult with the National Executive Committee before disclosing in public any decisions made in order to save embarrassment, like when some members of the ANC are said to have privately accused him of taking major decisions without engaging them: a decision with regard to an inquiry into the arms deal. (Letsoalo et al., 2011);
- Government leadership to be encouraged to focus and engage in researching and learning from success stories of other countries in order to build a better SA;
- The President could consider tightening the rules and regulations, as well as penalties governing corruption and fraud; and
- Consideration could be made to promote good governance by putting more effort on ethics programs.

---

[211] Letsoalo & Mataboge: 2011 in their article "Zuma had no choice but to call inquiry".

[212] Ndaba: 2011 describes the resistance as unexpected and states that it plunged the ANC provincial executive committee.

All in all, the President is to be congratulated on the steps already taken to prove that he is aware of the hope lost in the organisation (ANC) as a ruling party, and that he is prepared to act upon results from the reports handed in by the Public Protector. However, the PSC could help further by filtering down promotion of ethics within government departments, starting from top downwards: this could be coupled with internalised strategies to evaluate the performance of all government employees. The PSC should be tasked with:

- Ensuring that the National Hotline is fully operational;
- The PSC not playing a facilitator role only but to go further by employing the "management by wandering around" method in all anti-corruption structures, a technique which could help in:
- Establishment of how members in anti-corruption structures value and evaluate the structures within which they are employed: this could help identify irregularities such as: those occurring in terms of those allegations reported directly to anti-corruption structures without being considered for investigation (partly because they implicate individuals who, in the eyes if senior members involved, should not be investigated); staffing irregularities; and environment which turn to be non-conducive to employees as a result of managers who cannot criticism from employees based on senior members unprofessional behavior;

Furthermore, the PSC should establish requirements in terms of qualifications required for those to be staffed within anti-corruption structures; one of the reasons why the anti-corruption structure should be aligned within the DOD Secretariat.

Whistleblower Protection

More emphasis should be put on protection of whistleblowers within government departments as emphasised in paragraphs 3.4.2, 3.4.3 and 3.4.4. Proper investigations should be conducted to avoid situations such as that reported by Sosibo (2010) whereby an "Affidavit claims the council's former finance director was suspended and accepted an exit package under duress"[213]. An incident of this nature will scare away prospective whistle blowers whom, by reporting, would have saved South Africa as a country a lot of money. Protection should be given to everyone including prominent figures such as the Public Protector Thuli Madonsela who is described as "committed to a mandate granted by the

[213] Sosibo: 2010 is the Eugene Saldanha Fellow in social justice and inequality reporting, who reported the Midvaal council whistleblowers alleged the systematic victimisation of council employees.

supreme law of this country as well as to good governance"[214]; and Deborah Patta who is said to be exposing South African Government corruption and is considered to have the guts to ask the questions that many others cannot even formulate[215]. The marketing of the necessity of whistle blowing should therefore be coupled with a clear unambiguous whistle blower protection policy.

7.7.2 Departmental Level

It is encouraging to observe that the implementation of IFMS will attempt to fulfil the objectives of this study. Successful implementation of IFMS, on the part of fighting corruption and fraud, would require that: the replacement of various transversal systems for vehicle management be reduced to only one system that could be applied to the whole of the DOD; that the nature of allegations made regarding corruption and fraud committed through the use of computers be studied in order to close the gaps, e.g. the HR system should link all active members to get involved (an employee who is on leave should not be entitled to claim Travel and Subsistence or should not be allocated a military vehicle); that activities of corruption and fraud detected by members be submitted to the relevant authorities; that deductions be made from the salaries of members perpetrating through relevant policies and processes; that an audit of all DOD active employees be conducted and the report be submitted to SITA to counter the existence of posts created, funded and activated whilst not occupied by any known employee - an activity clearly stated by Prince (2011) whereby "the suspended police boss used money from the police informants' fund to pay salaries to his lovers as much as R18 000 in one instance and to a number of their relatives"[216].

In addition when addressing corruption and fraud factors, it is recommended that leadership consider to combine the vehicle management system that will be in operation (as part of IFMS) with a web based fleet asset management system that will ensure that vehicle management becomes a dynamic process integrated with the daily management of any institution, (http://en.wikipedia.org/wiki/Fleet-management). Improvements of control systems around vehicle management should include upgrading the manual systems of

---

[214] SOWETAN: 2011 maintains that Thuli Madonsela must be congratulated on the manner on which she has stood her ground in executing the duties of her office

[215] Seageng: 2010 holds that Debora Patta is in investigative journalism itself

[216] It is maintained that the Hawks spokesman would not mention the charges involved but confirmed that they relate to corruption and fraud. The charge sheet alleges, among others, the conducting of some police work without authority; misuse or selling of information or material acquired during the course of his duties; abuse of authority; breach of the police trust; etc.

managing vehicles, as well as the adoption of a single centralised framework that would integrate disparate vehicle management processes in order to uncover all anomalies. DOD leadership should agree upon the supplier and the type of fleet management system, a product that should have the following qualities:

- *Vehicle Tracking System*: a product said to be the most basic function in all fleet management system components; usually based on a Global Positioning System (GPS). It can offer the DOD a "Satellite tracking" communications for vehicle tracking in secluded environments without interruption.
- *The Principle of Geolocation*: depends on GPS for position determination and the Global System for Mobile Communication" or telecommunication satellite network for the data transmission.
- *Mechanical Diagnostics*: which allows concentration of the system to the vehicles' "onboard computer", and gather data for the user, wherein details such as mileage and "fuel consumption" are gathered into a global statistics scheme.
- *Driver Behavior*: by combining received data from the vehicle tracking system and the on-board computer, it is possible to form a profile for any given "driver".
- *Fleet Management Software*: this software enables people to accomplish a series of specific tasks in the management of any or all aspects relating to a company's fleet of vehicles. Specific tasks encompass all operations from acquisition to disposal; software allows functions such as driver and vehicle profiling, trip profiling, dispatch, vehicle efficiency, etc.
- *Management of Ships*: Fleet management is said to refer, also, to the management of ships, while at sea. Ships are normally given to fleet management companies that handle aspects like crewing, maintenance, and day-to-day operations.
- *Fleet Security and Control*: includes security of vehicles while stopped or not in operation and the ability to safely disable a vehicle while in operation. This allows the fleet manager to recover stolen or rogue vehicles while reducing the chance of lost or stolen cargo. It also gives a fleet card manager preventative measures to address cargo damage and loss.
- *Remote Vehicle Disabling Systems*: the disabling system provides authorised users at remote locations the ability to prevent an engine from starting; prevents movement of a vehicle, and to stop or slow an operating vehicle.

- *Duty of Care*: Directors and business owners are said to be unaware that privately owned vehicles used for business journeys, are supposed to be treated exactly the same way as company owned vehicles. Directors have an equal responsibility under the law to ensure that these vehicles are also roadworthy and correctly insured (DOD B-Scheme Vehicles and Subsidised vehicles) and organisations should verify conditions of such vehicles before allowance claims be payed.
- *Fleet Management Replacement and Lifecycle Management*: for timely replacement of vehicles and equipment is a process requiring the ability to predict asset lifecycles based on costing information. The industry standards for asset lifecycles calculated numbers are used to establish the expected date for a type or class of equipment, which can be used to identify replacement dates and funding requirements.

The proposed system is represented in figure 7.1:

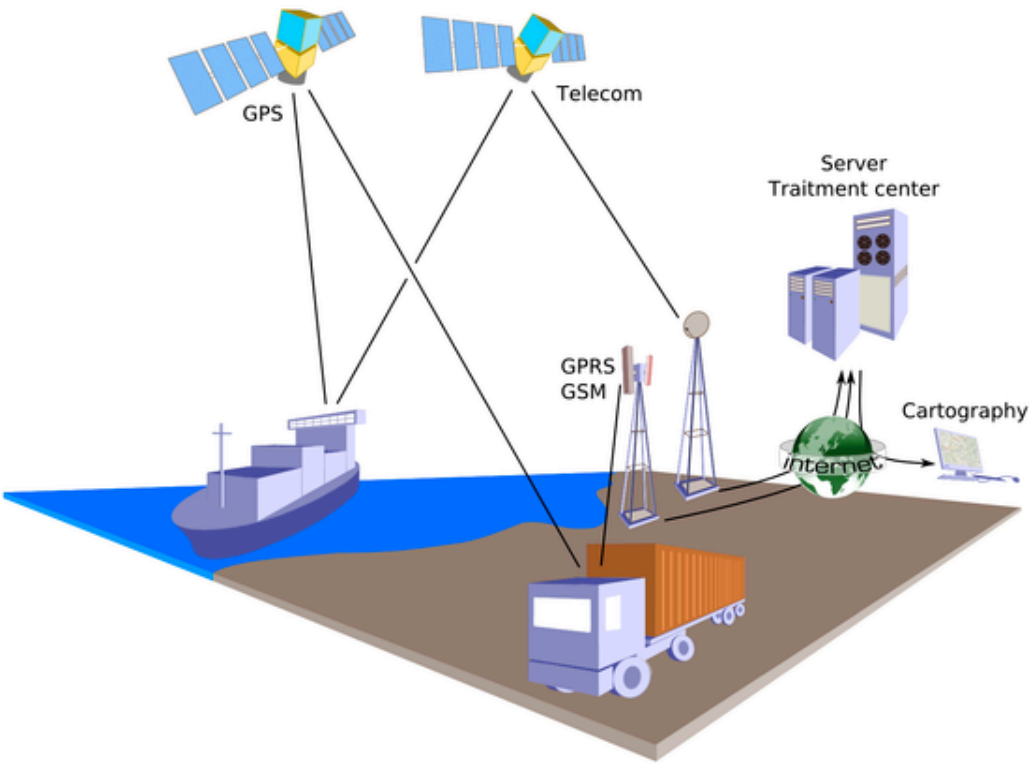

Figure 7.1: Proposed Tracking Device

Source: Wikipedia

7.8 Conclusion

In conclusion it could be stated that the research demonstrated the importance of Enterprise Application Integration (EAI) as but one methodology to curtail fraud and corruption in government organizations in general and in the DOD specifically. The research focussed on the integration of the Integrated Financial Management System (IFMS) and the Vehicle Management Systems (VMS) in the different Arms of the SANDF and found it to be of critical importance in the solution of the DOD's Business Problem namely to combat fraud and corruption. Furthermore a spin-off finding was that the integration of these systems with the Human Resource (HR) Management System could also be seen as a future investment to support the fight against fraud and corruption. It was also stressed that apart from having an official strategy akin to this issue the implementation and subsequent management thereof is likewise of critical importance.

Bibliography

ADM and the Zachman Framework. http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap39.html: viewed 19/02/2012

BALIM A. 2008. IFMS FIN Conceptual Application Architecture. SITA Strategic Services IFMS PMO SITA: Revision: 2.1

Being Poor Matters: Poverty and Inequality in South Africa. Mail & Guardian: 16-23/09/2011, p1

Being Poor Matters: School System Failing our Children. Mail & Guardian: 16-23/09/2011, p2-3

BERNARD HR. 2006 (ed). Research Methods in Anthropology: Qualitative and Quantitative Approaches. Alta Mira Press: Oxford

Blowing the Whistle on Fraud and Corruption http://www.gdard.gpg.gov.za/HTML/PDF/Anti-corruptionbooklet.pdf: viewed 22/10/10

BOATWRIGHT L. 2008. Conceptual Technology Architecture, (CTA) Integration. SITA Strategic Services IFMS PMO.SITA: Pretoria

BOOTH WC, COLOMB GG, WILLIAMS JM (eds). 2008. The Craft of Research. University of Chicago Press: Chicago

BOTHA D. 2008. Conceptual Technology Architecture, (CTA). Data Management Architecture. SITA Strategic Services IFMS PMO.SITA: Pretoria. Revision 2.00

BOTHMA D. 2008. Conceptual Technology Architecture (CTA) Data Management Architecture. SITA Strategic Services IFMS PMO. SITA: Pretoria. Revision 2

BOTTELIER P. 1998. Corruption and Development: Remarks for International Symposium on the Prevention and Control of Financial Fraud. Beijing, World Bank, (http://go.worldbank.org/0NCTH9XR0): viewed 12/03/2011

BRAND CG. 2006. DICT Information Systems Management Request 24/2006: Interim Liaison Arrangements between the DOD and IFMS. 1.0. SITA: Pretoria.

CASE STUDY: 2002. Financial Records and Information Systems in Tanzania: Evidence Based Governance in the Electronic Age. A World Bank/International Records Management Trust Partnership Project. http://www.irmt.org/documents/research_reports/case_studies/financial_recs_case_studies/tanzania/IRMT_Finan_CS_Tanzania.pdf: viewed 12/02/2010

CGI. 2004. Public Key Encryption and Digital Signature: How do they work? http://www.cgi.com/files/white_papers/cgi_whpr_35_pki_e.pdf: viewed 16/02/2012

CHAMPION FEJ. 2011. SA Army Headquarters Instruction/ DIR ARMY F STRUC/069/09: Project Libidi: Census for Vehicles in the SA Army. DOD: Pretoria

CHAUKE A. 2011. Officials Paid R100m for Sitting at Home. The Times. 23/09/2011, p5

CHENE M. 2009. The Implementation of Integrated Financial Management Systems (IFMIS) www.transparency.org: viewed 05/10/10

Collins Pocket Dictionary. 1998. Oxford University Press. Oxford

CORDIER A. 2003 (ed). Policy on the Management of Revenue within the DOD. DOD I INSTRUCTION: FIN NO 00025/2002

COWDERY N. 2008. Emerging Trends in Cyber Crime: New Technologies in Crime Prosecution: Challenges and Opportunities – Singapore. International Association of Prosecutors 13th Annual Conference

COWDERY N. 2008. Emerging Trends in Cyber Crime. New Technologies in Crime and Prosecution: Challenges and Opportunities Singapore. International Association of Prosecutors13th Annual Conference. http://www.odpp.nsw.gov.au/speeches/IAP%20-%2013%20Annual%20Conference%20-%20New%20Technologies.pdf: viewed 29/02/2012

CRAIG D V. 2009. Action Research Essentials. Josse-Bass: San Francisco

CRESSWELL JW. 2009. Research Design: Qualitative, quantitative, and Mixed Methods Approach. SAGE: California

CUMMINGS FA. 2002. Enterprise Integration: An Architecture for Enterprise Application and Systems Integration. SITA: Pretoria

CUTLER AS. 2007. The Whistleblower Speaks: The Sponsorship Scandal. AS Cutler: Canada

DANNHAUSER P. 2010. The Service Level Agreement: SLA 2.6 for ICT Acquisition Service. SITA: South Africa

DEFENCE ACT, ACT 42 of 2002: file:///T/shared/Library/Admin%20Shared/Acts/Defence/422002/DEFENCE%20ACT%202002.htm (1 of 77)4/2/2007

DEPARTMENT OF DEFENCE INSTRUCTION. 2011. (ed). Policy, Process and Procedures of Information and Communications Systems Security in the Department of Defence. DODI/CMI/00008/2001: promulgated 27/01/2011

DEPARTMENT OF COMMUNICATIONS: 2000. A Green paper on Electronic Commerce for South Africa: http://www.gov.za: viewed 02/10/10

DIGITAL ENVELOPES: http://www.wepopedia.com./TERM/D/digital_envelope.html: viewed 16/02/2012

DLAMINI P. 2010. Justice is Most Corrupt of All. SOWETAN: 23/09/2010, p2

DU TOIT MJ, BARNARD GJ, HEFER JP. 2003. Information Strategy. Joint Support Division. Version 2.1: dated 15 September 2003.

DYE KM. Corruption and Fraud Detection by Supreme Audit Institutions http://siteresources.wporldbank.org/INTWBIGOVANTCOR/Resources/CorruptionSupreme.pdf: viewed 23/10/2010

http://siteresources.worldbank.org/INTWBIGOVANTCOR/Resources/CorruptionSupreme.pdf

E-Government. http://www.apdip.net/publications/iespprimers/eprimer-egov.pdf: viewed 24/02/2010

ERASMUS P. 2008. IFMS Conceptual Technology Architecture (CTA): Secure Business Enablement. SITA Strategic Services IFMS PMO: SITA, Pretoria

EU/PSPPD. 2011. NEC Members Deny Prompting Halt of Secrecy Bill. Mail & Guardian: 23-29 September 2011

FENELLY R. 2003. HM Treasury Report on Managing the Risk of Fraud: A Guide for Managers: London. http://archive.treasury.gov.uk/fraud/mriskf.pdf: viewed 19/10/2011

FLEET MANAGEMENT http://www.fleetmanagement.co.za: viewed 13/06/2011

FLEET MANAGEMENT. http://en.wikipedia.org/wiki/Fleet_management: viewed 13/06/2011

FLICK W, KARDORFF E, STEINKIE I. 2004. A Companion to Qualitative Research. SAGE: London

FRIEDMAN T L. 2006. The World is Flat: The Globalized World in the Twenty First Century. Penguin Books. England

GOULD C. 2011. It's not as bad as You Think. CITY PRESS: 11/09/2011, p31.

GUIDE TO THE PREVENTION AND COMBATING OF CORRUPT ACTIVITIES: ACT No 10 of 2004 http://www.nacf.org.za/guide-prevention-combating-corrupt-activities/reporting_corruption.html: viewed 20/10/2011

GREAT BRITAIN HM TREASURY. 2001. Fraud Report: An Analysis of Reported Fraud in Government Departments and Best Practice Guidelines. http://archive.treasury.gov.uk/fraud/fr9900.pdf: viewed 22/10/2011

GREAT BRITAIN HM TREASURY. 2008. Fraud Report: An Analysis of Reported Fraud in Government Departments. http://www.official-documents.gov.uk/document/cm74/7408/7408.pdf: viewed 22/10/2011

Green Paper on Electronic Commerce for South Africa: 2000 http://www.info.gov/za/view/DownloadFileAction?id=68917: viewed 02/10/10

GUILDENPFENNIG E. 2008. Conceptual Technology Architecture (CTA): Development, Testing and Integration Architecture: SITA Strategic Services IFMS PMO: Pretoria

HIRSCHEIM R, KLEIN HK. 2003. Crisis in the IS Field: A Critical Reflection on the State of Discipline. *Journal of the Association for Information Systems* 4(5): 237-293

HOFSTATTER S, MZILAKAZI WA AFRICA, ROSE R. 2011. D-Day for Cele. Sunday Times: 25/09/2011, p1-2

HOSKEN G, TERREBLANCHE C, PIETERSON M, DU PLESSIS C. 2010. Zuma Wields Axe. Pretoria News: 1 November 2010, p1

HYALIJ BA, GORDANE PS. System Analysis and Design Flexibility in the Approach Based on the Product Definition. *International Journal of Computer Applications* 1(20): 46-51

Implementation of Integrated Financial Management Systems http://www.u4.no/helpdesk/helpdesk/query.cfm?id=196: viewed 28/05/2010

Integrated Financial Management System. 2011. http://www.futuregov.asia/articles/2011/sep/23/govt-launch-integrated-financial-management-system/: viewed 10/10/2011

IM B, JUNG J. 2001. Using ICTs to Strengthen Government Transparency and Relation with Citizens in Korea. Organisation for Economic Co-operation and Development: Korea

Key Performance Areas Public Service Commission. http://psc.gov.za/about/key_performance: viewed 19/10/2011

KGOSANA C. 2011. Dirty Secrets of SA's Spy Agenda. Sunday Times: dated 25/09/2011, p. 1.

KINGMAN J, MAWHOOD C. 2008. Tackling External Fraud: Good Practice Guide. National Audit Office: http://www.nao.org.uk/guidance__good_practice/idoc.ashx?docid=ed397377-07cd-40ae-88da-cda7fbe41131&version=-1: viewed 01/01/2010

KOTLOLO M, MABUZA K.2010. Corruption Hotline is Corrupt: Taxpayers' Money Wasted. SOWETAN: 29 October 2010, p. 4.

KUMAR R. 200. Research Methodology: A Step-by-step Guide for Beginners. SAGE: London

LAND R. 2003. An Architectural Approach to Software Evolution and Integration. Västerås: Sweden

LAND R 2003 An Architectural Approach to Software Evolution and Integration. Arkitektkopia, Västerås, Sweden

LAUDON KC, LAUDON JP (eds). 2004. Management Information Systems: Managing the Digital Firm. Pearson: New Jersey

LAUDON KC, TRAVER CG. 2007. E-Commerce: Business, Technology, Society. Prentice Hall: New Jersey

LEGG R. 2010. Baloyi's Breaking Bones" Rhetoric is a Publicity Stunt. Business Report: dated 1 November 2010, p14

LETSOALO M, MATABOGE M. 2011. "Zuma had no Choice but to Call Inquiry". Mail & Guardian: 23-29/09/2011, p2-3

MAAKE B. 2007. Integrated Financial Management System (IFMS): NT/SCOPA Quarterly Meeting. National Treasury: South Africa http://www.epa.gov/privacy/assess/ifms.htm: viewed 01/10/2010

MAJAVU A. 2010. R3m Spent on Mismanagement Probe. SOWETAN: 29/10/2010, p4

MAJAVU A. 2011. Draft Policy "Lenient" on Servants. SOWETAN: 22/08/2011, p2

MALHOTRA R, TEMPONI C. 2010. Critical Decisions for ERP Integration: Small Business Issues. *International Journal of Information Management* 30 (2010) p28-37

MANAGING FINANCIAL RECORDS: http://www.google.co.za/search?q=MANAGEMENT+FINANCIAL+RECORDS&btnG=Search&hl=en&source=hp&gs_sm=e&gs_upl=11221133531011633611417101510101221813109 16-1.9-11210 : viewed 29/10/2011

MASHABA S. 2011. Bid to Reduce Road Deaths. SOWETAN: 23/09/2011, p14

MCDERMOTT A. 2011. Phishing can Cost You, Big Time. Mail & Guardian Business: 23-29 September 2011, p3.

MERRIAM SB. 2009. Qualitative Research: A Guide to Design and Implementation. Jossey-Bass: San Francisco

MLHONGO JK. 2010. Standing Work Procedures: Vehicle Management (VFM): Defence Inspectorate Division: South Africa

MORGAN G. 2006. (ed). Images of Organisations. SAGE: London

MOSUNKUTU K. 2010. Gauteng Government to Intensify Fight against Aggravated Crime: Budget Vote Speech by MEC Mosunkutu: dated 28/05/2011

MOYO S. 2011. Transparency a Cure for the "Resources Curse". Mail & Guardian: 23-29 September 2011, p32.

NAICKER S. 2011. Bill is Crocodiles' Path to Plenty. SOWETAN: dated 23 September 2011.

NAIDOO K. 2011. Poverty and Inequality in South Africa. Mail & Guardian: dated 16-24 September 2011

NAO Report. 2006. Central Government's use of Consultants: Methodology. http://www.nao.org.uk/idoc.qshx?docId=4de7de3f-2339-410d-ae12-02cd0f26b76d&version-1: viewed 21/10/2011

NDABA B. 2011. Reshuffling of Provincial Cabinet put on Hold. Pretoria News: 01/11/2010, p1

NDEBELE N S. 2011. Our Dream is Turning Sour. Sunday Times: 25 September 2011, p1-2

NATIONAL RESREARCH COUNCIL. 2009. Achieving Effective Acquisition of Information Technology in the Department of Defence: http://www.nap.edu/catalog/12823.htm

Observation Method http://www.humanresources.hrvinet.com/observation-methods/: viewed: 25/06/2010

Observation Method www.nsf.gov/pubs/1997/nsf97153/chap_3.htm

OOSTHUIZEN R, WOLMARANS D, ERASMUS P, O'SULLIVAN GS. 2008. IFMS Conceptual Data Architecture. SITA Strategic Services: South Africa

OSLER O. 2008. Conceptual Technology Architecture (CTA): Communications Architecture. SITA Strategic Services IFMS PMO 2.00: South Africa

O'SULLIVAN GS. 2008. IFMS Architecture Executive: 2.01. SITA: South Africa

PASCUAL PJ. 2003. E-Government http://www.apdip.net.publications/iespprimers/eprimeregov.pdf: viewed 19/10/2011

PASCHALIDOU C. 2006. Third Annual Thematic Research Summary. DG Energy and Transport. www.transport-

research.infi/Upload/Documents/200608/20060831_110509_06030_EU-accession-issues_D2E_issues1-0.pdf: viewed 19/10/2011

PIENAAR a. 2007. Principles for Application Architecture Bulletin. SITA: Pretoria. Revision 1.0

PRETORIUS LWO. 2001 (ed). Policy on Internal Audit, Inspection, and Anti-Fraud in the Department of Defence. Department of Defence Instruction: IG/0.0002/2001

PRINCE C. 2011. Top Spy's "Discount" BMW: Police Spy Boss Bust for Fraud. The Times: 23/09/2011, p1-2

PSPPD. 2011. Being poor Matters: Poverty and Inequality in South Africa. Mail & Guardian: 16-22/09/2011

PUBLIC SERVICE COMMISSION. Mandate. http://www.psc.gov.za/about/functions.asp: viewed 19/10/2011

PUBLIC SERVICE COMMISSION: Profiling and Analysis of the Most Common Manifestations of Corruption and its Related Risks in the Public Service: http://www.psc.gov.za/press_statements/2011/20110420.asp: viewed 01/08/2011

Qualitative Research. http://en.wikipedia.org/wiki/Qualitative_research: viewed 23/10/2010

RABIE E. 2008. Conceptual Technology Architecture (CTA) Hosting. SITA: Pretoria. Revision 2.00

RICHIE J, LEWIS J. 2003 (ed). Qualitative Research Practice: A Guide for Social Science Students and Research. SAGE: London

"Risk E-Business": Assessing Risk in Electronic Commerce. http://www.decisionsciences.org/decisionline/vol133/33

"Risk E-Business": Assessing Risk in Electronic Commerce. http://www.decisionsciences.org/decisionline/vol33/33_3/33_3ecom.pdf

SA ARMY ORDER. 2003. SA Army Vehicle Management Strategy.

Sapa. 2011. SA Run by Thugs and Thieves. SOWETAN. 23/09/2011, p4

SAPSFORD R, JUPP V. 2006 (ed). Data Collection and Analysis. SAGE: London

Saudi e-Government Program. 2007. IT Readiness Assessment for Government Organisations: http://ebookbrows.com/it-readiness-assessment-booklet-en-pdf-d77668740: viewed 19/10/2011

SEAGENG K. 2010. SA Women should be inspired by Patta. SOWETAN. 25/08/2010, p12

SELOWA M P. 2006. Guidelines and Procedures for General Police Duties. Military Police Instruction: MPAIN007/1999

SERRAO A, FLANAGAN L. Toll Scheme now Costs R35bn. Pretoria News: 27/09/11, p1-2

SMUTS D. 2008 (ed). Policy on Information and Communications Systems Security in the Department of Defence Instruction: DODI/CMIS/ 00008/2001. Department of Defence: South Africa

SOCIAL RESEARCH METHODS: http://www.socialresearchmethods.net/kb/questype.php: viewed 20/10/2011

Software Incompatibility: http://en.wikipedia.org/wiki/Software_incompatibility: viewed 20/10/2011

SOSIBO K. 2010. Midvaal Council Whistleblowers Allege Witch-Hunt. Mail & Guardian: 18-24 November 2011, p20

SOWETAN. 2011. SOWETAN SAYS: Doing the Right Thing. 23/09/2011, p16

State of E-government in South Africa: Department of Public Service and Administration. Pretoria: South Africa

STRAUSS A, CORBIN J. 1998. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE: London

THIVHIDZO E. 2008. South African National Defence Force (SANDF) on the Road to a Better Asset Management http://buanews.gov.za/view.php?ID=08030416451002&coll=buanew08: viewed: 25/09/2008

TUGANADAR N. 2008. IFMS Roadmap and Release Plan: 2.00. SITA Strategic Services IFMS PMO: South Africa

TUGANADAR N. 2008. IFMS Contextual Architecture. SITA: South Africa

UNDERHILL G, DONNELLY L. 2011. NEC Members Deny Prompting Halt of Secrecy Bill. Mail & Guardian: 23-29 September 2011, p8-9

UN ODCCP. 2001. Draft United Nations Manual on Anti-Corruption Policy. GPAC: Vienna

VAN DEVENTER L. 2008. Conceptual Technology Architecture (CTA) Technology Architecture Overview 2.00. SITA Strategic Services IFMS PMO: South Africa

VAN NIEKERK B. 2008. IFMS SCM Conceptual Business Architecture 2.00. SITA Strategic Services IFMS PMO: South Africa

VAN ROOYEN A. 2005. Research Methodology. Oxford University Press: Oxford

VAN VUUREN L, WRIGHT AJ, ROSSOUW P. 2001. Department of Defence Instruction IG NO 1/2001

VAN ZYL P. 2010. Service Level Agreement (SLA) 1.2 for Enterprise Information Systems and Architecture Services. SITA: South Africa

WEICK KE. 1995. Sensemaking in Organisations. SAGE: London.

WESTAT JF. 2002. The User Friendly Handbook for Project Evaluation. National Science Foundation

What Roles Do Firewalls & Proxy Servers Play in Network Security? http://www.ehow.com/info_8167378_roles-servers-play-network-security.html: viewed 16/02/2012

Zachman Framework. http://en.wikipedia.org/wiki/File:Zachman_Framework_Model.svg: viewed 19/02/2012

Zachman J A. 2003. The Zachman Framework for Enterprise Architecture: Primer for Enterprise Engineering and Manufacturing. http://www.businessrulesgroup.org/BRWG_RFI/ZachmanBookRFIextract.pdf: viewed 1/02/2012

ZWANE M. 2011. Minister has no Credibility. SOWETAN: 23/09/2011, p16.

Appendix A

IFMS Options *(Source: Maake: 2007, p3)*

SYSTEM OPTIONS	ADVANTAGES	DISADVANTAGES
Customised Best of Breed COTS (Commercial off the Shelf)	•Improves Functional fit •Allows system synchronisation with policy development •Improves competition in different functional spheres	•Imposes Commercial Best Practices •Turns project to in-house development •Requires development of integration software •Commits project to specific versions of COTS or unsynchronised system life-cycle for different COTS options •Commits system development to multiple COTS development environments Requires effective change management strategy and highly skilled user community
In-House Developed Systems	•Control on functional fit •Control on system life-cycle •Synchronisation of system life-cycle to policy development •Control over functional fit vs change management Control over development standards	•May take long to deliver results •May lead to conflict over priorities May compromise on industry standards and best practices
Multiple Options Solutions	•Provides for organisational autonomy •Centralised standards setting	•High levels of duplications and costs •Risk of non-compliance to inter-operability standards •Difficulty to synchronise system developments to policy changes •May take very long to deliver results across all organisations •Fragments available skills levels

Appendix B

Policy Statement *(Source: The Investigator)*

Anti-Fraud Policy Statement

The DOD does not tolerate fraud of any type or in any conditions, whether committed by any type of claimants or our employees. As the DOD:

- **We are committed to fighting fraud, corruption and dishonesty in all of our activities.**
- **We are determined to root out fraud and corruption carried out by employees who are abusing their position, and by others who try to get assets or services from us to which they are not entitled.**
- **We expect all our staff to demonstrate the highest standards of honesty at all times. These standards are clearly set out in our Code of Conduct. Our disciplinary procedures make sure that managers take firm and appropriate action wherever fraud or corruption by employees has been proven.**
- **All of our managers are responsible for putting into place and maintaining effective systems of internal control (making sure staff keeps to procedures; monitoring how well officers are maintain the set systems; dealing with any problems with procedures) and making sure that our resources are used on the activities they are meant for. This includes being responsible for the prevention and detection of fraud and corruption**
- **We aim to prosecute anyone who commits fraud and corruption as this is an important way of discouraging other people from committing fraud in future.**
- **In cases of benefit fraud, we will charge a fine or issue a formal caution wherever appropriate.**
- **We consider the abuse, by employees, of financial or other benefits, from us or any other public organisation as gross misconduct.**

As a result, the DOD has set up the Directorate Anti-Corruption and Anti-Fraud (DACAF) to lead our fight against fraud and corruption. It is an independent unit, which reports to the IG DOD. One of its purposes is to make sure that all allegations of fraud and corruption are properly investigated. The Officers commanding, heads of Divisions and Managers must report all suspicions of fraud and corruption to DACAF and DACAF will advise and support them in this. Where appropriate, DACAF will investigate the matter independently. Also, DACAF has set up a programme of checks to detect, deter and prevent attempted fraud and corruption.

Appendix C

The Seven Principles of Public Life *(Source: HM Treasury: 2003, p23)*

THE SEVEN PRINCIPLES OF PUBLIC LIFE

Selflessness	**Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.**
Integrity	**Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.**
Objectivity	**In carrying out public business, including making public appointments, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.**
Accountability	**Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.**
Openness	**Holders of public office should be as open as possible about all the decisions and action that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands it.**
Honesty	**Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in away that protects the public interest.**
Leadership	**Holders of public office should promote and support these principles by leadership and example.**