IT Control Objectives for Implementing the Public Finance Management Act in South Africa

R. Luyinda and M.E. Herselman
Tshwane University of Technology, South Africa

G.H.K Botha, Independent Consultant, South Africa

rluyinda@gmail.com
herselmanme@tut.ac.za

Ayeye.solutions@gmail.com

Abstract

This paper presents the proposed IT Control objectives for implementing the Public Finance Management Act of 1999 (**PFMA**) for the Republic of South Africa. The aspects covered in this paper show the main concerns of accounting officers in implementing the PFMA.

The ability of IT Control Objectives for Information and related Technology (**COBIT**) to enable the participation of IT in the design and implementation of internal control over financial reporting for the PFMA is a major finding presented in this paper. However, this area of research is new and further studies to inform the responsibility of IT in facilitating the implementation of the PFMA need to be undertaken. This paper is a maiden effort in that direction.

Keywords: PFMA, Internal control; COBIT; Control objectives; implementation.

Introduction

The interests of organisations in the public sector differ from those of the private sector. While the private sector is driven by business survival, the public sector is driven by political survival. However the mechanisms that are used to enhance business goals in both sectors do not significantly differ. While an issue like profit is not a main stream government concern, another issue like governance and its attendant appendages like accountability, efficiency, effectiveness and value for money are cross-sector concerns, catching the attention of both the private and the public sector. While the private sector is concerned about the newly proposed Companies Bill that will implement more stringent Corporate Governance in South Africa, the public sector is concerned with the Public Finance Management Act (PFMA). The requirements of these two are not that different. The issues that arise in both regulations are governance based referring to efficiency, effectiveness, transparency, financial reporting and high standards of corporate governance. Both legislations necessitate the design and implementation of IT mechanisms for internal control. The concern of this paper is the design and implementation of IT mechanisms for internal control to enhance South African government departments' compliance with the provisions of the PFMA.

The propositions of this paper resulted from a research study that used a two pronged approach. The first part included a literature study to establish whether COBIT could be used to guide

the implementation of the PFMA. The second phase included in-depth interviews to identify those aspects of the PFMA that are considered important for IT's intervention as an enabler of the design and implementation of internal control over financial reporting for the PFMA.

This paper will present a brief background of the PFMA. Then a similar regulation, the Sarbanes-Oxley, will be presented to set a background for illustrating how COBIT has met the IT control needs in another regulated environment. Internal control and IT governance are discussed as a prelude to the exploration of COBIT's potential for implementing the PFMA. After the exploration of this potential, then the IT controls for PFMA will be presented. Compliance oriented architecture as a result of optimised PFMA implementation using COBIT will be presented before concluding.

Background

The PFMA is a legislation that was passed by the first democratic government in South Africa. The Act aims at proper financial management in order to ensure effective service delivery through the effective and efficient use of available national resources (Department of Public Enterprises, 2002, p. 21). The PFMA consists of the following components:

- Risk management.
- Asset management.
- Financial management and Budgeting.
- Performance management.
- Procurement, provisioning and Third Party Services.
- Legal compliance.
- Financial Reporting and Record Management.
- Medium Term Expenditure Framework.
- Strategic & business planning.

The main objective of the PFMA is to secure transparency, accountability, and sound management of the revenue, expenditure, assets and liabilities of the institutions to which this Act applies (PFMA, 1999, section 2).

Dickovick (2004, p. 33) explains this object clearly that the South African government aimed at curbing the over-expenditure of the provinces and public entities, which includes the national departments. He asserts that central government efforts to limit overspending culminated in the PFMA of 1999, which was, *inter alia*, designed to improve expenditure management by requiring provincial governments to submit periodic reports to the central government.

The stages of expenditure leading to the PFMA have been analysed by Dickovick (2004, p. 134). These stages are presented in Table 1.

Dickovick (2004, p. 128) also points out that management systems in the national executive closely monitor Sub–national Government (SNG) spending. Provinces and public entities are mandated to meet specific service standards and fixed output targets. National government has also constantly increased its monitoring of SNG expenditure. The government has therefore consistently monitored the expenditure of the provinces and public entities. To ensure that the departments meet the objectives set for them by the government. This is regarded as the only way the public service goals of the government can be achieved within the available budgets.

Table 1: Stages of Expenditure

Year	Change in expenditure autonomy
1994 (increase)	Constitutional transition. South African provinces and public entities go from administrative mechanisms to independent levels of government, but receive expenditure mandates from central government.
1996 (increase)	Constitution establishes independence of provinces and public entities, but spending mandates remain in place.
1996 – 98 (decrease)	"Structural adjustment" plans stipulate multiple specific spending reductions for provinces and public entities on a case-by-case basis.
1997 (decrease)	Medium Term Expenditure Framework (MTEF) implemented; multi-year budget plan designed to hold provinces and public entities to spending targets.
1999 (decrease)	Public Finance Management Act (PFMA) ensures tighter monitoring of provincial and public entities' budgets.

Source: Adopted from Dickovick (2004, p. 134)

Against this background of trying to achieve public service goals with the available resources, the PFMA was formulated. It is worth mentioning that many of the goals of the PFMA are also in line with the 1998 Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa. While the PFMA is a 1999 regulation, it has similarities with the 2002 Sarbanes-Oxley. The next section will exemplify this view.

Sarbanes – Oxley Act of 2002

The Sarbanes-Oxley (SOX) Act is a United States law that was signed on July 30, 2002, as a response to corporate and accounting scandals in United States. These scandals included companies like Enron, Tyco International, Peregrine Systems and WorldCom. Dietrich (2004, p. 2) noted that "the scandals resulted in a loss of public trust in financial reporting and accounting practices and required attention from legislators who recognized that, if left unaddressed, the loss of trust could have deepened to a system wide malaise. The Act, therefore, was meant to prevent future accounting scandals and rebuild the trust of the investing public."

Though the PFMA may not seem that rigorous and certainly not for the private companies, it has similar concerns with the Sarbanes-Oxley, especially where financial crime is concerned. The major concern of this paper, however, is the role of IT in ensuring internal control over financial reporting. Dietrich (2004, p. 2) observed that the two sections of the Sarbanes-Oxley that should concern IT executives the most are 302 and 404(a) because they deal with the internal controls that a company has in place to ensure the accuracy of their data. It relates directly to the software systems that a company uses to control, transmit and calculate the data that is used in their financial reports. The PFMA similarly deals with internal control with elaborate detail in the Treasury Regulations of the PFMA in Part 2 Section 3.

The reporting requirements of the PFMA are no different from those of Sarbanes-Oxley. These requirements need a clear system of internal control for IT as well as other assets with in the organisation to ensure transparent reporting. This next section addresses this concern.

Internal Control

Internal control includes the policies, plans and procedures, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected (IT Governance Institute, 2007, p. 206).

According to the Committee of Sponsoring Organizations (COSO) of the Institute of Internal Auditors (IIA, 2005, p. 3) internal control is a process, effected by an organisation's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories of effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations.

The PFMA hands over the responsibility of internal control to the officials in the various departments who are not necessarily the accounting officials for reporting to the audit committee for external oversight. This is stipulated in Section 45 of the PFMA which deals with the responsibilities of other officials other than the accounting officers.

In the case of the PFMA, the following reference applies under the heading Treasury Regulations and Instructions (PFMA, 1999, p. 40) which states that the National Treasury may make regulations or issue instructions applicable to all institutions to which the Act applies concerning financial management and internal control. About the responsibilities of other officials, the PFMA (1999, p. 33) states that an official in a public entity must ensure that the system of financial management and internal control is established for that public entity and that it is carried out within the area of responsibility of that official.

It was noted by Finkelstein (2005, p. 1), which observation suits the South African government context, that internal controls vary from enterprise to enterprise, and in this context from department to department and are therefore determined by the different business processes and activities of the enterprise (departmental) financial controls. These controls are "closely related to the IT systems and databases used for financial and other reporting". The significance for the South African context is what has been suggested in this paper that the IT control objectives suggested in this work are broad so that departments can draw their specific objectives by answering specific questions again suggested by the Finkelstein (2005, p. 2) (from the Zachman Framework) which include: What? How? Where? Who? When? Why?

In the context of the PFMA if two issues, that is, data and processes, proposed by Finkelstein are considered, these questions would be:

- *For Data:* What does the data represent? How is the data processed? Where is it used? Who is responsible for the data? When is the data used? Why is the data needed? Does this data support the strategic and tactical business plans?

- *For Processes*: How do we execute them? What data do they use? Where are they processed? Who is responsible for the processes? When are these processes used? Why are the processes needed? Do they support strategic and tactical business plans?

The answers to the above questions would be a start to the customisation of both internal controls and the IT control objectives for the PFMA in the different government departments.

Having shown the need for internal control for the PFMA, the next section will justify the need for IT to be involved in implementing the PFMA.

The Need for IT in Internal Control over Financial Reporting

The institute of Chartered Accountants in England and Wales (ICAEW) and Delloite and Touche (2005, p. 4) concur that most regulations are concerned with information and the way it is handled, stored and protected, and therefore IT systems are inevitably the core focus of most compliance activity (ICAEW, 2005:17). This highlights the sensitivity of IT in financial reporting and control.

Worthen (2003) adds, while remarking about the Sarbanes-Oxley, that while Sarbanes-Oxley is financial legislation, at its heart it is about ensuring that internal controls or rules are in place to govern the creation and documentation of information in financial statements and this is similar to the PFMA. Therefore, since IT systems are used to generate, change, house and transport data, CIOs have to build the controls which ensure that information stands up to audit scrutiny.

KPMG (2005, p. 17) also encourages IT representation in agency processes. It notes that since a major portion of an agency's control activities is likely to be IT controls, and the integration of the IT function into the agency's business processes is important, the agency is encouraged to include team members from the chief information officer's organization in review teams. Their participation would go a long way towards ensuring that key technology risks and controls are fully considered during the assessment process.

The above is a good guideline for executives that have to face the rigorous processes of compliance to the PFMA. While the PFMA stipulates that the accounting officer is responsible for compliance to the PFMA, such work is enormous for only one individual. It would be made simpler and more effective results would be achieved if the IT departments formed part of the compliance committee. This would allow IT to provide inputs while the compliance plans are being made thus enabling alignment of available IT resources to offer a platform for complying with the PFMA. It is therefore pertinent that IT must itself be governed if it is to be part of the internal control processes for financial reporting.

IT Governance

According to the IT Governance Institute (2003, p. 10) IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives. This is illustrated by Figure 1 below as a circular process of Strategy, Processes and Results, with Stakeholder Values as input and Results as output from the circular Governance effort.

For Weill & Woodham, (2002, p. 1) IT governance is specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT. The authors further assert, in clarification of their definition, that IT governance applies principles similar to those for financial governance to IT management. To achieve their goals, firms encourage particular desirable behaviours that exploit and reinforce the human, systems and intangible assets that comprise their core competency, (Weill & Woodham, 2002, pp. 1-2).

The above two definitions are no different from each other because Weill and Woodham's decision rights and accountability are equal to organisational sustainability as mentioned by the IT Governance Institute.
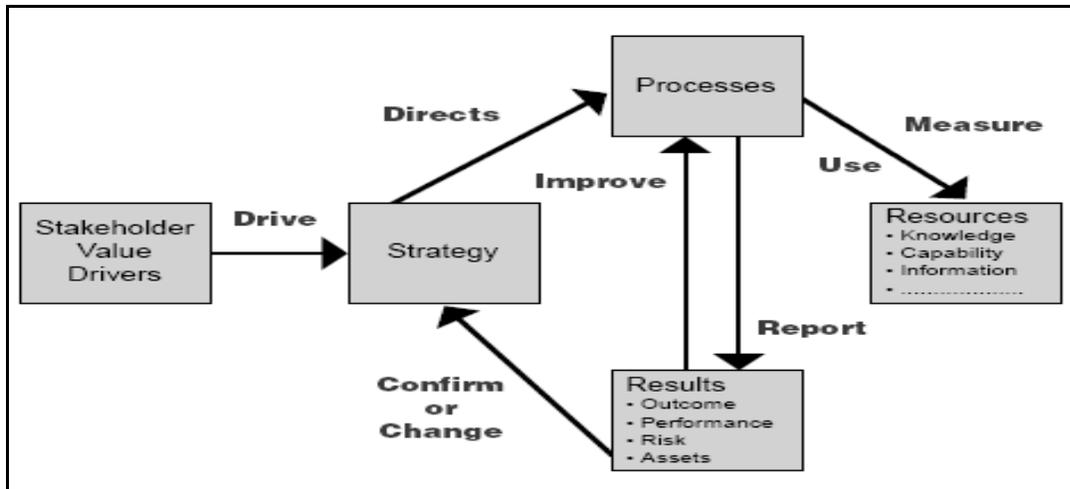
Figure 1: The IT Governance Process
Source: Adapted from IT Governance Institute (2003, p. 21)

This similarity shows that there is no need for executives looking at IT governance as a new concept, but one to be embraced as applying similar principles to another department of the enterprise. That is why the similar principles of the PFMA can and should be adapted to suit the governance requirements of IT.

To De Haes and Van Grembergen, (2004, par 5) IT Governance is the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.

Previously, Van Grembergen and De Haes, (2003, p. 6), reported that IT is situated at all levels of organisational management. This is exemplified in the figure below that shows the three levels of IT governance responsibility. IT is present at the board, the executive and operational level. This indicates that IT should thus be part of the process of designing and implementing control over financial reporting. IT's participation at all management levels (operational, executive and strategic) and the fact that IT has to do with information in an organisation necessitates its proper governance. Figure 2 shows the three layers of IT governance and levels of responsibility for IT in an organisation (Van Grembergen, De Haes 2003, p. 6).
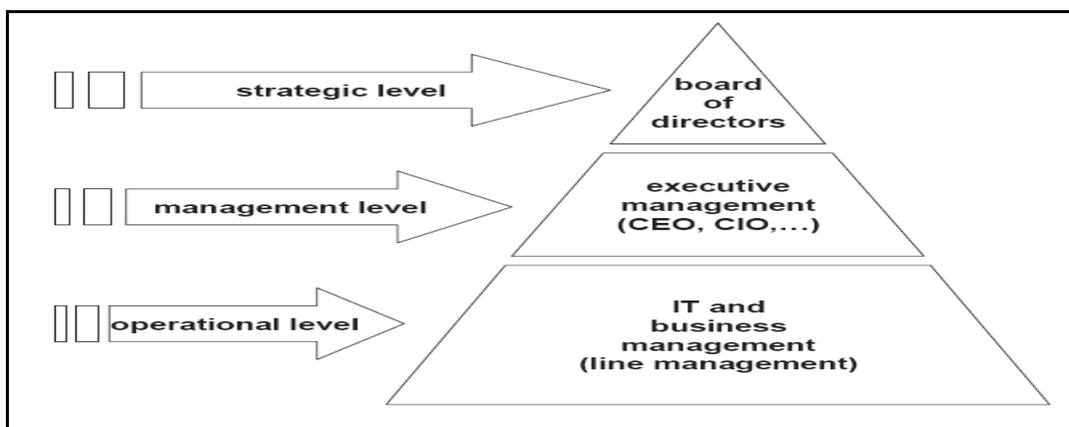

Figure 2: IT Governance Layers
Source: Adapted from Van Grembergen, De Haes (2003, p. 6)

Governance of both IT and the larger and broad corporate body are not different as shown in the next section.

IT Governance versus Corporate Governance

Since governance as a whole is generically considered as corporate governance, corporate governance then should drive and set objectives for IT governance. IT can facilitate the drive towards strategic opportunities as required by the enterprise and can be critical to strategic plan formulation. Hence as Van Grembergen and De Haes argue, IT governance and corporate governance can therefore not be considered as pure distinct disciplines and IT governance needs to be integrated into the overall governance structure, (2003, p. 8).

The relationship between corporate and IT Governance can be shown by the similarity of concerns by the stakeholders of both IT and the organisation. The questions asked of the organisation at corporate governance level or strategic level, are not much different from those asked of IT at the same level. Examples from Van Grembergen & De Haes (2003, p. 9) show this in Figure 3.

Corporate governance questions	⇒	IT governance questions
How do suppliers of finance get managers to return some of the profits to them?	⇒	How do the board and executive management get their CIO and IT organisation to return some business value to them?
How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects?	⇒	How do the board and executive management make sure that their CIO and IT organisations do not steal the capital they supply or invest it in bad projects?
How do suppliers of finance control managers?	⇒	How do the board and executive management control their CIO and IT organisation?

Figure 3: IT and Corporate Governance
Source: Adapted from Van Grembergen & De Haes (2003, p. 9)

After asking similar questions, it is also notable that IT governance and corporate governance are interlinked at a hierarchical level as Figure 4 below illustrates.

To show that there is a clear linkage between IT governance and corporate governance, the figure below illustrates a framework proposed by Weill and Ross (2004, p. 5) for linking corporate governance and governance of IT.

They argue that the top of the framework represents the board of directors with all their relationships to stakeholders and their disclosure and monitoring responsibilities. Then they articulate strategy and desirable behaviour required for the enterprise to realise its strategic objectives. Among the key assets are information and also the related technological assets that must be governed. They (Weill & Ross 2004, p. 7) argue that governance of the key assets occurs through a large number of organizational mechanisms (for example, structures, processes, committee, procedures, and audits). Some mechanisms are unique to a particular asset, and in particular point out the IT architecture committee as being specific to IT (Weill & Ross 2004, p. 5).
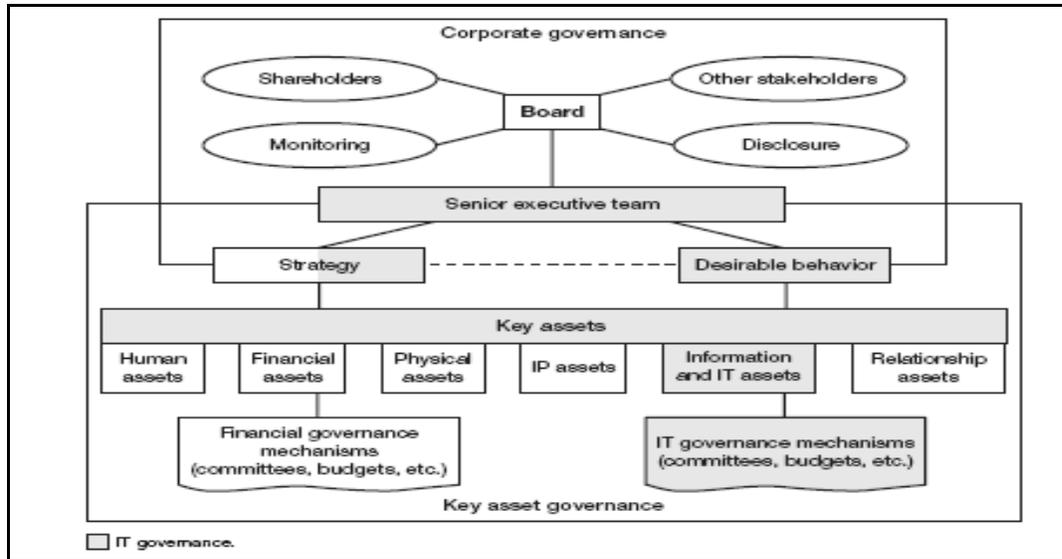
Figure 4: Corporate and Key Asset Governance
Source: Adapted from Weill & Ross (2004, p. 5)

If IT governance and corporate governance are similar in many regards, then there is reason to question why there should not be one governance structure. The next section addresses this question.

Strategic Alignment as the Aim of IT Governance

The general aim of IT governance is to align business goals with IT resources to achieve those business objectives. Two aspects are prevalent. Firstly, strategic fit caters for the external influence exerted upon IT strategy, which includes issues like how the firm is positioned in the IT marketplace. Secondly, the internal domain is concerned with the way IT infrastructure should be configured and managed. This requires integration in two domains, as suggested by Henderson & Venkatraman, (1993, p. 476). The two types of integration that exist are strategic business and operational integration. Strategic business integration aligns business strategy and IT strategy to the external IT environment, which are important for many companies if IT is to provide a source of strategic advantage. The other type is operational integration which ensures that the internal business processes are aligned with the IT processes to enable IT support organisational requirements and also ensure that IT develops the capability to support such requirements. From the above it can be concluded that the aim of IT governance is strategic alignment.

This section provided a general background to the PFMA and the relevance of COBIT and IT governance. The next section explores COBIT's potential to support the PFMA.

Exploring COBIT's Potential for Implementing the PFMA

COBIT is a well known and often used framework issued by the IT Institute of Governance (ITGI). Its purpose is to help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong, (ITGI 2007, p. 5). It is available from the IT Institute of Governance.

It is pertinent to explore COBIT's potential before considering it as the recommended framework for implementing the PFMA in South Africa. The starting point is to look at COBIT's success in regulated another business environment.

IT Control Objectives for Sarbanes-Oxley

According to the IT Governance Institute (2006, p. 9) this is a publication first issued in 2004 by the IT Governance Institute to help companies assess and enhance their internal control systems.

This publication motivates the need for compliance not from the view of regulation but from the benefits accruing to compliance with the Sarbanes-Oxley Act. Thus the work required to meet the requirements of the Sarbanes-Oxley Act should not be regarded as a compliance process, but rather as an opportunity to establish strong governance models designed to result in accountability and responsiveness to business requirements (IT Governance Institute 2006, p. 9). Similarly, instead of the stick or scare approach, the same could be done in the South African context by showing accounting officers how their work will be simplified if they comply with the PFMA.

Some, but not all, of the benefits (IT Governance Institute 2006, p. 9) that are forwarded for compliance with the Sarbanes-Oxley Act include,

- • gaining competitive advantage through more efficient and effective operations:
- • enhancing risk management competencies and prioritization of initiatives:
  - ➢ enhancing overall IT governance:
  - ➢ enhancing the understanding of IT among executives:
- • optimizing operations with an integrated approach to security, availability and processing integrity:
- • contributing to the compliance of other regulatory requirements, such as privacy: and
- • aligning project initiatives with business requirements.

These same benefits will be realized when IT control objectives are identified to enhance the design and implementation of internal control over financial reporting for the PFMA.

Figure 5 shows the control objectives for the Sarbanes-Oxley and the related COBIT processes that satisfy the Sarbanes-Oxley requirements.

	CoBiT	PCAOB IT General Controls			
IT Control Objectives for Sarbanes-Oxley	Mapping to CobiT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and maintain application software.	AI2	●	●	●	●
2. Acquire and maintain technology infrastructure.	AI3	●	●	●	
3. Enable operations.	AI4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●
10. Manage problems and incidents.	DS8, DS10			●	
11. Manage data.	DS11			●	●
12. Manage the physical environment and operations.	DS12, DS13			●	●

Figure 5. Mapping Sarbanes-Oxley to PCAOB and COBIT
Source: Adapted from IT Governance Institute (2006, p. 11)

The above control objectives align Sarbanes-Oxley with the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 and COBIT. The reason for aligning to the PCAOB is because this board is was created by the Sarbanes-Oxley Act of 2002 to oversee the auditing of public companies to protect the interests of investors. Therefore auditing according to the Sarbanes-Oxley must meet the requirements of this board. The alignment to COBIT adds an

IT role to the auditing of the IT components and the utilisation of IT to audit the other aspects of Sarbanes-Oxley. Similarly the auditing of the PFMA is overseen by the National Treasury and enacted by the Auditor General. The contribution of IT to auditing is the subject of this paper.

This mapping also enables the realisation of the above named benefits. Such a mapping was done for the PFMA. The next section introduces the mapping.

COBIT Addresses Internal Control Needs

According to the Committee of Sponsoring Organizations (**COSO**) (IIA 2005, p. 3) internal controls should be regarded as a process, designed to provide reasonable assurance regarding the achievement of objectives in the following categories of effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations. IT must be noted that this process and related controls are affected by an organisation's board of directors, management, and other personnel.

The IIA (2006, p. 13) explains the above categories by indicating that the first category (*effectiveness & efficiency of operations*) addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second (*Reliability of financial reporting*) relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third, (*Compliance with applicable laws and regulations*), deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

The IT Governance Institute (2007, p. 8) confirms COBIT's high consideration of internal control by asserting that for IT to be successful in delivering against business requirements management should put an internal control system or framework in place. The COBIT control framework contributes to these needs by:

- Making a link to the business requirements
- Organising IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered

Such contributions of COBIT can also be applied to the PFMA to ensure realisation of internal control.

COBIT Addresses IT Controls

To the IT Governance Institute (2007, p. 15) general controls are controls embedded in IT processes and services. Examples include systems development, change management, security, and computer operations. Controls embedded in business process applications are commonly referred to as application controls (2007, p. 15). Examples include completeness, accuracy, validity, authorisation and segregation of duties.

According to IIA (2005, p. 3) general controls (also known as infrastructure controls) apply to all systems components, processes, and data for a given organization or systems environment. General controls include, but are not limited to: information security policy, administration, access, and authentication; separation of key IT functions; management of systems acquisition and implementation; change management; backup; recovery; and business continuity.

The IT Governance Institute (2007, p. 16) shows that IT General controls cross various boundaries of the business enterprise. In terms of IT and the business, they are both the responsibility of business and IT. Business presents the control requirements and IT covers the IT general controls. These boundaries are illustrated in the figure below:

These boundaries do not differ from those found in government institutions and are therefore applicable for the PFMA implementation in the South African government.
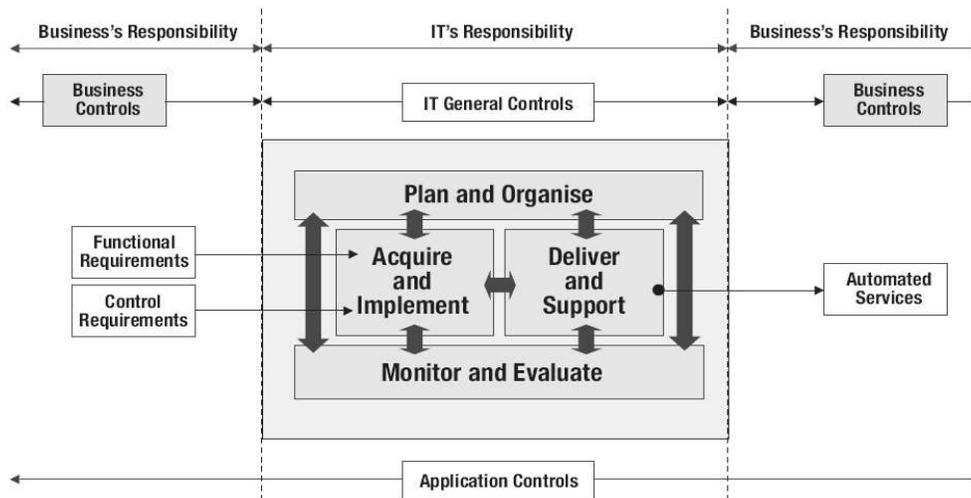

Figure 6: Boundaries of General and Application Controls
Source: Adapted from IT Governance Institute (2007, p. 16)

The identification of IT General controls can be done with any model and the same general controls may be arrived at. This is because the guidelines available emphasise the same aspects that must be considered to establish these IT general controls.

The IIA (2007, p. 6), further, sets down principles under which general controls can be scoped. These principles are outlined in the Guide to the Assessment of IT (GAIT) General Controls Scope based on Risk.

The four GAIT Principles which were adhered to when mapping COBIT to the PFMA are:

Principle 1

The identification of risks and related controls in IT general control processes (for example, in change management, deployment, access security, operations) should be a continuation of the top-down and risk-based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.

Principle 2

The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.

Principle 3

The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, databases, operating systems, and network.

Principle 4

Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

Table 2 shows the mapping of COBIT to PFMA components using the above principles.

The table also shows:

- Entity (company) level
- Activity level
- COBIT IT Processes (Each process is composed of several IT Control Objectives. We mapped at Process level to allow South African government departments and Institutions to review the process and select appropriate control objectives.)

Table 2: COBIT Mapping to PFMA

Entity (company) level	Activity level	COBIT IT Processes	PFMA Component									
			Risk management	Asset management	Financial management & Budgeting	Performance management	Procurement & provisioning & Third Party Services	Legal compliance	Financial Reporting & Record Management	MTEF	Strategic & business planning
Plan & Organise (IT Environment)												
●		Define IT strategic planning	●		●			●		●	●
●		Define the information architecture							●		
		Define technology direction									
●		Define the IT processes, organization and relationships	●			●					●
●		Manage the IT investment			●		●		●		
●		Communicate management aims and direction				●		●		●	●
		Manage IT human resources									
●		Manage quality			●	●	●	●	●		
●		Assess and manage IT risks	●				●	●	●		
●		Manage projects	●			●		●			●

Entity (company) level	Activity level	COBIT IT Processes	PFMA Component								
			Risk management	Asset management	Financial management & Budgeting	Performance management	Procurement & provisioning & Third Party Services	Legal compliance	Financial Reporting & Record Management	MTEF	Strategic & business planning
Acquire and implement (Program Development and Program Change)												
	•	Identify automated solutions									
	•	Acquire and maintain application software	•	•					•		
	•	Acquire and maintain technology infrastructure	•	•							
	•	Enable operation and use				•					
		Procure IT resources									
	•	Manage changes	•		•			•	•	•	
	•	Install and accredit solution and changes	•	•		•					
Deliver and Support (Computer Operations and Access to Programs and Data)												
	•	Define and manage service levels	•			•	•				
	•	Manage third- party services	•			•	•				
•		Manage performance and capacity				•				•	•
	•	Ensure continuous service									
	•	Ensure systems security	•		•				•		
		Identify and allocate costs									
•		Educate and train users				•				•	
		Manage service desk and incidents									
	•	Manage the configuration	•								
		Manage problems									
	•	Manage data	•					•	•		
		Manage the physical environment									

Entity (company) level	Activity level	COBIT IT Processes	PFMA Component								
			Risk management	Asset management	Financial management & Budgeting	Performance management	Procurement & provisioning & Third Party Services	Legal compliance	Financial Reporting & Record Management	MTEF	Strategic & business planning
	●	Manage operations									
Monitor and Evaluate (IT Environment)											
●		Monitor and evaluate IT performance	●			●					
●		Monitor and evaluate internal control			●	●			●		
●		Ensure regulatory compliance					●	●	●		
●		Provide IT governance	●					●			●

Identifying Specific IT control Objectives for the PFMA

The South African Public Finance Management Act No. 1 of 1999 as amended by Public Finance Management Amendment Act, No. 29 of 1999 addresses certain concerns. These concerns include financial management, financial reporting, standardised accounting procedures, effectiveness, efficiency, transparency and economy in the management of public funds. The Act allocates responsibilities to different individuals and bodies to ensure that State resources are not misused.

In terms of IT these concerns are translated to mean;

- secure and authorised access to financial data;

- segregation of duties and granting of access to data depending on the needs and hierarchy and responsibility in the government institutions;

- communication of changes in employee status to guard against unauthorised access to systems and sensitive financial data;

- mitigation of risk through change and configuration management as an addition to risk assessment;

- appropriately outlined phases of the SDLC to ensure that systems are monitored from inception to disposal; and

- performance management to ensure effectiveness, efficiency, economy and transparency in management of public funds.

Financial data is the most important item to secure in this process. It has to be guarded against among other things; unauthorised access, improper reporting, inaccurate processing and inaccurate data being processed, misstatements due to wrong data, unauthorised transactions and improper changes to systems that can directly affect financial information.

When identifying key IT controls (IIA 2006, p. 34), it is important to recognize, in addition to the four GAIT principles, that:

- Some key business controls are fully automated, for example the calculation of interest for banks or updating the correct general ledger account.

- Some controls are partly automated. For most companies, a large number of controls are of this type, where the individual performing the control relies on a computer report or information on a computer screen.

- Other controls are fully manual, for example the inspection of incoming materials for quality.

The above considerations were used to map COBIT to the PFMA. The successful mapping of COBIT to the PFMA would lead to identification of the IT control objectives for implementing the PFMA.

The result of the mapping was the identification of IT controls objectives that addresses PFMA concerns. These objectives are not directly stated but categories were created into which these objectives can be identified to allow each department and government institution to adapt them to their unique needs and resources. The control objective categories are shown in Figure 3.

Table 3: Aligning PFMA Concerns with IT Objectives' Categories

PFMA Concern	IT Control Objective Category (cf COBIT 2007)	Rationale
Internal control and internal audit: this is very important because if there are internal control and audit mechanisms over financial reporting, it would mean that the funds are used for their allocated functions and not for any other entertainments that are not in line with the objectives of the departments and institutions, and therefore the objectives of government as a whole.	Security management, change management, data management	There is a need for security when executing internal control and internal audit because if financial data is not taken care of, it can easily be modified. This goes hand in hand with data management to ensure that data is not easily lost, and in case it is lost, it can be recovered, and if changed, different versions of the data can be used to justify its authenticity. Therefore change management is important because such changes to data can be tracked and the changing party can be identified and checked against authorizations to effect such changes.

PFMA Concern	IT Control Objective Category (cf COBIT 2007)	Rationale
Proper accounting and reporting capabilities that can be derived from a proper service from IT. Since most of the data is available in soft copies, it would be of benefit if IT enabled accounting and reporting practices in line with the requirements of the PFMA.	Data management, Computer Operations	Since financial data is sensitive, it is important that it is backed up in case of eventual loss. Operations need to be effective to avoid incidents that could lead to misstatements of financial data.
Performance management which included efficiency, effectiveness, and value for money: this includes the need for doing work in a proper and cost-effective way.	Computer Operations, Data Management	Since Computer operations includes incident, and problem management, and production monitoring, it should be part of performance management to ensure that the down time of the networks are minimised and when it do happen data is backed up and can be recovered from a secure storage.
Data integrity and safety in the form of information security: data is not tampered with in any way that could compromise the reporting of accurate financial information with respect to the laws requiring information access.	Security Management, Change Management	This concern is addressed by Security Management because it involves processes like security administration, security configuration, and security management at application, database, platform, and network level. This keeps the data secure. In case some one changes anything, Change management which includes processes like application development lifecycle management, quality assurance and testing, change management at application, database, platform and network level would be the appropriate measure to curb this. It would include audit trails as well to ensure that the source of change is identified.

PFMA Concern	IT Control Objective Category (cf COBIT 2007)	Rationale
Risk management to ensure that uncalled for expenditures are avoided which may lead to wasteful expenditure according to the PFMA.	Change Management, Data Management Security Management	Managing risk requires that change is well managed and tracked to know where risks of financial misappropriation may come from. It also includes data management to ensure that if the financial databases are attacked, there are current backups to the data. Therefore security is important to ensure that the data is only available to those accountable for the financial reporting.
Proper asset management	Security Management, Change Management	Asset management requires approvals and keeping up to date information about the assets. Only those on charge of data related to assets may be able to access it and also make modifications to this data. In case assets are wrongfully moved or stolen, it should not be easy for the responsible individuals to change the data on the systems, and if the data is changed, then the responsible officers must be the only ones with the ability to do the changes and are therefore answerable.
Proper procurement and Supply chain management	Data Management, Security Management	Proper procurement requires security because financial values may be over inflated beyond market value and that means it is possible to account for mismanaged funds. There is also a need to ensure that the data is not corrupted to lead to wrong calculations when dealing with issues of government procurement.

With increasing levels of efficiency in implementation and as the learning curve yields better outcomes, compliance oriented architecture can be explored to allow higher optimisation of the resources and knowledge base available. The next section briefly looks at the possibility of such architecture.

Exploring a Compliance Oriented Architecture

According to the IEEE (2000, p. 3), architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.

Taking the IEEE as the standard description of architecture, one can accept that the definition of architecture does not leave room for doubt that an architectural approach would be suitable for compliance. This is because even compliance works in an environment that is guided by principles, regulatory or otherwise, and these principles affect the design and evolution of compliance. Taking a look at the PFMA compliance, indeed there has been evolution because the level of compliance that first saw the birth of the PFMA is different from the level now.

However it all comes back to the maturity level of compliance that will determine the level of enterprise architectural complexity that will take place in an organisation. An architectural approach would fit at a high end of maturity because then the requirements from IT would be well refined over several compliance iterations.

O'Grady, (2004, p. 1), indicates that given the breadth and depth of compliance requirements plus the fact that the regulatory landscape is highly dynamic, it is clear that businesses now require a flexible compliance oriented architecture to keep pace. The author qualified this view with the fact that compliance requirements are increasingly driving business agendas, to the point of dominating many information technology budgets.

The architecture would be described in the format of accepted standards to ensure compliance with standards and then it would be in line with the uniqueness of each entity. Pahos and Rao (2007) suggest the recognition of ""enterprise patterns" that are exhibited by Federal Agencies that are established by common charter, and perform business functions that are governed by similar constraints, and are structured organizationally in a similar manner."

In the case of the South African government, those would be patterns in departmental structures established by laws like the Public Service Regulations, 2001. In case such legally stipulated patterns exist, Pahos and Rao (2007) assert that it would be a source of benefits like a "source of architectural information for building a Common Regulatory Enterprise Architecture Model (CREAM)". Other benefits that they outlined were; efficient and effective compliance with mandates (which is the main objective of the PFMA), promotion of best practices and provision of a ready made reference model for architecture patterns and a methodology for developing a compliance or common architecture (which is one of the proposals of this paper for achieving the above objective of the PFMA).

Conclusion

The purpose of this paper is to present the results of a study that aimed at identifying IT control objectives for the PFMA. This has been achieved by setting a background to the PFMA and building on the need for these controls. It has also outlined how these objectives can be identified and which aspects of the PFMA they address.

It is therefore possible to use COBIT as an enabling framework to employ IT as an enabler of the design and implementation of internal control over financial reporting for the PFMA. It is, however, important to point out that IT works not as the sole enabler but in liaison with all other assets in the government entities.

References

De Haes S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal, 1.* Retrieved July 7, 2007, from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=1677 1,

Delloite & Touche. (2005). *Under control sustaining compliance with Sarbanes-Oxley in year two and beyond*. Retrieved August 10, 2007, from http://www.deloitte.com/dtt/article/0,1002,sid%253D36513%2526cid%253D70194,00.html

Dickovick, J. T. (2004). Municipalization as central government strategy: Central-regional–local politics in Peru, Brazil, and South Africa. *Publius: The Journal of Federalism 2007, 37*(1),1-25; doi:10.1093/publius/pjl012. Retrieved July 7, 2007, from: http://publius.oxfordjournals.org/cgi/content/full/37/1/1

Dietrich, R. (2004). *Sarbanes-Oxley and the need to audit your IT processes*. Retrieved July 7, 2007, from: www.cgservices.com/compliance/library/**MKS**-Sarbanes-Oxley_062504.pdf

Department Of Public Enterprises. (2002). *Protocol on corporate governance in state owned enterprises*. Retrieved August 31, 2007, from: www.dpe.gov.za/res/ProtocolonCorporateGovernanceinthePublicSector.pdf

Finkelstein, C. (2005). *Governance analysis using enterprise architecture*. Retrieved February 22, 2008, from http://www.ies.aust.com/pdf-outlines/governance.pdf

Henderson J. C., & Venkatraman N. (1993). Strategic alignment: Leveraging information technology for transforming organisations. *IBM Systems Journal, 32*(1). [Reprinted in *IBM Systems Journal, 38,* 2&3, 1999]. Retrieved August 13, 2007, from http://www.research.ibm.com/journal/sj/382/henderson.pdf

IEEE STD 1471-2000. (2000). *IEEE recommended practice for architectural description of software-intensive systems*. New York: The Institute of Electrical and Electronics Engineers.

Institute Of Chartered Accountants in England and Wales. (2005). *Planning for compliance – The role of IT* .London: Faculty of Information Technology of the Institute of Chartered Accountants in England and Wales

Institute of Internal Auditors. (2005). *Global technology audit guide: information technology controls*. Florida: Institute of Internal Auditors.

Institute of Internal Auditors. (2007). *The gait methodology: A risk-based approach to assessing the scope of IT general control*s. Florida: The Institute of Internal Auditors.

IT Governance Institute. (2003). *Board briefing on IT governance* (2nd ed.). Illinois: IT Governance Institute.

IT Governance Institute. (2006). *IT control objectives for Sarbanes-Oxley* (2nd ed.). Illinois: IT Governance Institute.

IT Governance Institute. (2007). *Control objectives for information and related technologies 4.1 (COBIT 4.1)*. Illinois: IT Governance Institute.

KPMG LLP. (2005). *Assessing internal control over financial reporting*. Retrieved September 20, 2007 from http://us.kpmg.com/microsite/attachments/10505DCGR-A-123_forweb.pdf

O'Grady S. (2004). *SOA meets compliance: Compliance oriented architecture*. Retrieved August 13, 2007, from http://soa.omg.org/Uploaded%20Docs/COA/COA_Final.pdf

Pahos P. E, & Rao P. C. (2007). Common Regulatory Enterprise Architecture Model (CREAM). Retrieved February 22, 2008 from https://www.feacinstitute.org/za/FEAC?PAGE=EA_ZONE_ABSTRACTS&MENU=EA_ZONE

PRICEWATERHOUSECOOPERS. (2006). *IT governance in practice insight from leading CIOs*. Retrieved September 21, 2007 from http://www.pwc.com/extweb/pwcpublications.nsf/docid/790D48A25A3505008525726D00567783/$File/pwc_itgovernance.pdf

Presidential Review Commission. (1998). *Report of the Presidential Review Commission on the reform and transformation of the public service in South Africa*. Retrieved July 18, 2007, from www.info.gov.za/otherdocs/1998/prc98/index.html - 50k

The Republic of South Africa. (2005). Treasury Regulations For Departments, Trading Entities, Constitutional Institutions and Public Entities Issued in Terms of The Public Finance Management Act, 1999.

The Republic of South Africa. (1999). The Public Finance Management Act No. 1 of 1999 as amended by Public Finance Management Amendment Act, No. 29 of 1999.

United States. (2002). *The Sarbanes- Oxley Act*, [Online]. Retrieved June 7, 2007, from www.findlaw.com

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Boston, Massachusetts: Harvard Business School Press.

Weill, P., & Woodham, R. (2002). Don't just lead, govern: Implementing effective IT governance. Retrieved August 21, 2007, from http://web.mit.edu/cisr/working%20papers/cisrwp326.pdf

Worthen, B. (2003). Data privacy: What to do when Uncle Sam wants your data. *CIO Magazine*. Retrieved August 13, 2007, from:
http://www.cio.com/article/31836/Data_Privacy_What_to_Do_When_Uncle_Sam_Wants_Your_Data_/8

Van Grembergen, De Haes. (2003). Strategies and models for IT governance. Retrieved August 13, 2007 from: http://www.igi-pub.com/downloads/excerpts/9781599049267ch1.pdf

Biographies

Richard Luyinda is a postgraduate student at Tshwane university of Technology. His research and professional interest focuses on IT/Business alignment and Enterprise Architecture.

Prof **Marlien Herselman** is a Research and innovation Professor in the Faculty of Information and Communication Technology. She assists lecturers and postgraduate students with research projects, NRF projects, writing research articles, and with other research-related activities. In 1999 she obtained a PhD at the University of Pretoria. Her PhD studies focused on the use of computer games. In 2000, she became Head of the Department of End-User Computing at Port Elizabeth Technikon and, in 2002, she joined the team at the former Technikon Pretoria (now part of TUT). In 2004, a Master's degree in Business Information Systems was conferred on her. She is currently busy with a funded research project on Technology assessment models in rural communities in South Africa, funded by the National Research Foundation. She is also on a joint appointment at the CSIR for two days a week assisting the Meraka Institute with research capacity building.

In 2000, Prof Herselman was awarded a scholarship of the Deutsche Akademischer Austauschdienst (DAAD) of the International Women's University (IFU) to attend a summer semester at the University of Hamburg, in the project field of information. In 2005, she was named *Women Researcher of the Year* at TUT. In 2006 she obtained NRF rating at level C3 in South Africa. She written 24 articles and has fifteen conference contributions at international conferences. Her re-

search focus on ICT for business enhancement, rural community and informatics and e-health projects. Contact information: Tel: +27 12 382 5758 Fax: +27 12 328 4839 Cell: + 2782809 4319 E-mail: herselmanme@tut.ac.za

Gerrit Botha is an independent consultant practicing the art and science of enterprise and IT strategy and architecture. He promotes the concept of business capabilities and has successfully developed and implemented several strategies in the public and private sectors, using such an approach.

He lectures on the masters program of the Tshwane University of Technology and has published several articles and conference proceedings on the subject of "value innovation" which is also referenced internationally.