

## **Alignment of COBIT to Botswana IT audit methodology and its value in improving IT Policies**

Control Objective for Information and Related Technology (CoBiT) is a framework that provides guidance on security and control in Information Technology (IT). It covers IT processes from planning to monitoring of activities within the IT environment. Its emphasis on controls provides a structured way in which investments in IT resources (application, systems and associated infrastructures) can be evaluated and coordinated to add value in achievement of organisational objectives. The office of Auditor General Botswana has adopted this framework as a base to substantiate judgements on auditees' internal controls.

The paper will discuss how the alignment of our audit methodology to CoBiT has improved our auditing process and provided guidance on the structures that are to be expected at our auditees. Among other issues to be discussed in the paper will be how COBIT has been instrumental in ensuring that we give relevant recommendations which have in turn assisted auditees to improve their IT policies, structures and the overall quality of services extended to customers. The paper will examine an audit that was carried out for Department of Tertiary Education on the Student Loan Management System. It will highlight key areas tested and the CoBiT areas which served as guidelines. Furthermore the paper will analyse the recommendations made detailing those that were implemented and those not attained by the auditee with reasons thereof. In assessing the recommendations, the paper will highlight areas to be considered when making a recommendation for example, involvement of the auditees, and cost of proposed controls and / or improvement of current mitigating controls.

Below is the list of proposed sub topics;

- Brief introduction on CoBiT
  - reasons for Botswana to align its methodology to it
- Mapping CoBiT 4.1 to audit programs
  - Types of IT Audits undertaken and which COBIT areas are mapped to the working papers.
- The value derived from alignment to CoBiT
  - Structured audit methodology
  - Understanding of IT services
  - Improved recommendation
- Review of the Department of Tertiary Education project
  - Objective of the audit
  - CoBiT areas selected and mapped to the working papers
  - Analysis of recommendation, Value added
- Brief discussion on New CoBiT 5, its focus and what effects it will have on our audits

## **Brief introduction on COBIT**

### **Reasons for Botswana office to adopt COBIT Framework**

The office of Auditor General Botswana adopted COBIT in 2000. COBIT framework and COBIT Audit Objectives 3<sup>rd</sup> edition (referred to now as the IT Assurance guide with COBIT 4.1) documents were utilised to develop the IT audit manual for the office of Auditor General Botswana. The COBIT framework outlines IT processes and key activities that are to be carried out in an IT environment to support IT delivery against business requirements.

One of the reasons that the office of Auditor General Botswana adopted COBIT was that COBIT gives a holistically view of the IT computing environment, starting with management issues to operational issues. What controls does management need to implement which cascade to operational goals? COBIT is well known for its focus on IT Governance. What is management responsibility in establishing policies and procedures that ensure IT department meet business requirements.

Another reason that the office adopted this framework is because of its practicality. The processes identified in the COBIT framework are easily relatable to IT professionals. The issues addressed by the framework include day to day IT operations. For example managing of the IT help desk; each IT department regardless of its size, will receive calls from the users requesting for assistance. The department needs to keep track who called and whether they are being assisted. Deliver and Support 8 (DS8) **Manage service desk and incidents** provides elaborate description of the service function, control objectives, such as establish a service desk, registering calls, incident escalation, and incident closure and report and trend analysis.

Last but certainly not the least of reasons by far is that the COBIT IT assurance guide provides a clear road map from planning of the audit up to field work execution. The COBIT IT Assurance guide is specifically targeted at IT assurance professionals. "The guide is designed to enable efficient and effective development of IT assurance initiatives, providing guidance on planning, scoping and executing assurance reviews using a road map based on well-accepted assurance approaches." *COBIT, IT Assurance Guide, 2007*. The guide is linked to COBIT processes outlining the control objectives, value drivers for the process, risk drivers and tests of controls to be performed by an assurance professional. The guide has assisted the office in developing relevant audit programs that are aligned with the COBIT framework.

## **Types of IT Audits Carried Out**

IT audits carried out include;

IT performance audits which focuses on ensuring that IT systems are procured and implemented effectively, efficiently and economically. These audits were carried out in the years 2008 to 2010. Three projects have been successfully complemented namely;

- Student Loan Management System
- State Land Integrated Management System
- Government Payroll Pensions and Passages

The State Land Integrated Management System was presented to Public Accounts Committee (PAC) on the 03 and 04<sup>th</sup> October 2012. Remarks from PAC showed that members of PAC had interest in knowing whether reasons for procuring the new system were valid that is return on investment. What were the actual cost of the project and if there any overruns. This is an area that the team is currently developing to see whether IT procurements indeed add value to organisation and if there are aligned to departments and ministries strategies or meet the expected objectives.

Another area of IT audit that the office carries out is IT audit in support of financial audits. The audits are carried out to ascertain that there are sufficient controls within the systems and applications so that financial auditors can place reliance on information processed through the applications. Report of these audits are sent to management and where the Auditor General deems the audit finding to be crucial, there are included in the Report of the Auditor General which is discussed at by the Public Accounts Committee. Findings of the review of the motor vehicle registration and licensing application were included in the report of the Auditor general of 2007.

It is thus imperative for the IT audit section to carry out its wok in accordance with best standards and or best practices. COBIT was selected as one of the framework on which to benchmark our audits against. In addition the Department of Information Technology use COBIT framework. The Department of Information Technology is responsible for providing strategic IT advice and support to all government departments, ministries and local authorities.

## Review of the Department of Tertiary Education project

### General Objectives

- To assess whether Student Loans Management System assists the DSPW to achieve its mandate.

### Specific Objectives

- To assess if the system assists the users in performing their tasks effectively.
- To assess whether the project scope included all aspects of the department, including identification of stakeholders and key players.
- To assess how data integrity is maintained and identify business continuity measures in place.
- To identify how the system's performance is managed and measured.
- To assess whether training was carried out to assist users to use the system efficiently.

### COBIT areas selected and mapped to the audit questions

The following are COBIT areas aligned to the questions that the project was addressing.

Audit Question	COBIT Areas
Is the system assisting the department perform its activities more effectively?	PO1.1 IT Value Management PO1.2 Business-IT Alignment PO1.3 Assessment of Current Capability and Performance PO10 Manage Projects
Was the project scope comprehensive enough with regards to stakeholder's identification?	A11 Identify Automated Solutions A11.1 Definition and Maintenance of Business Functional and Technical Requirements. A12 Acquire and Maintain Application Software
How is data integrity and disaster recovery addressed?	DS5 Ensure Systems Security DS11 Manage Data DS11.5 Backup and Restoration
How is the performance of the system monitored and managed?	DS3 Manage Performance and Capacity DS3.1 Performance and Capacity Planning

	DS3.2 Current Performance and Capacity DS3.3 Future Performance and Capacity DS3.4 IT Resources Availability DS3.4 IT Resources Availability DS3.5 Monitoring and Reporting
Has the training equipped the users to efficiently use the system?	DS7 Educate and Train Users DS7.1 Identification of Education and Training Needs DS7.2 Delivery of Training and Education DS7.3 Evaluation of Training Received

### **Analysis of recommendation, Value added**

Some of the recommendations issued on the Student Management Loan System report include;

Management was advised that reports produced by system should be appropriate and relevant to strategic decision making process. The recommendation emphasised that the use of the system should not only be focusing on processing loans but management should be in a position to gather enough information from the system to make strategic decisions. COBIT P0.1.1 IT value management and IT business alignment emphasise on the need for IT resources to be aligned to business strategies.

Management was further advised to conform to Government IT Projects Guidelines and requirements. The government of Botswana has established IT project guidelines which guides IT officers on how to manage a project including documentation of user requirements, project initiation report, project memorandum and project end reports. The IT Projects guidelines are aligned to COBIT.

In addition management was advised to develop SLMS performance measures to enable them evaluate the system's performance and take corrective steps if necessary.

The use of and understanding of COBIT has significantly improved our audit methodology. Recommendation provided to clients are based on best standard and therefore if implemented will greatly improve on IT processes. Benchmarking on a recognized framework also gives assurance to the client that the criterion being used is fair. What is important in providing recommendation to the client is having an understanding the environment in which they work within and its limitations. This can be

achieved through discussion of finding with the clients, identification of mitigating controls and finding a cost effective recommendation.

## **COBIT 5**

- COBIT 5 which was released early in 2012 aim is to align COBIT to other frameworks such as Val IT, ITIL, ISO270002 and Prince 2.
- COBIT 5 clearly defines governance and management and separates the duties of two roles.
- COBIT 5 introduces 5 principles and 7 enablers
- The concept of goal cascade from stakeholder needs to operation duties is emphasized. (Considering IT related interests of internal and external shareholders)
- The control objectives are no longer explicitly defined.
- The framework processes have increased from 34 to 37. The new processes included are
  - a) APO 04Manage Innovation
  - b) APO 10Manage Supplies
  - c) BAI 06Manage Knowledge