

Module 2 – Overview of Internal Control over Financial Reporting

Handout 2 – COBIT 4.1 Framework

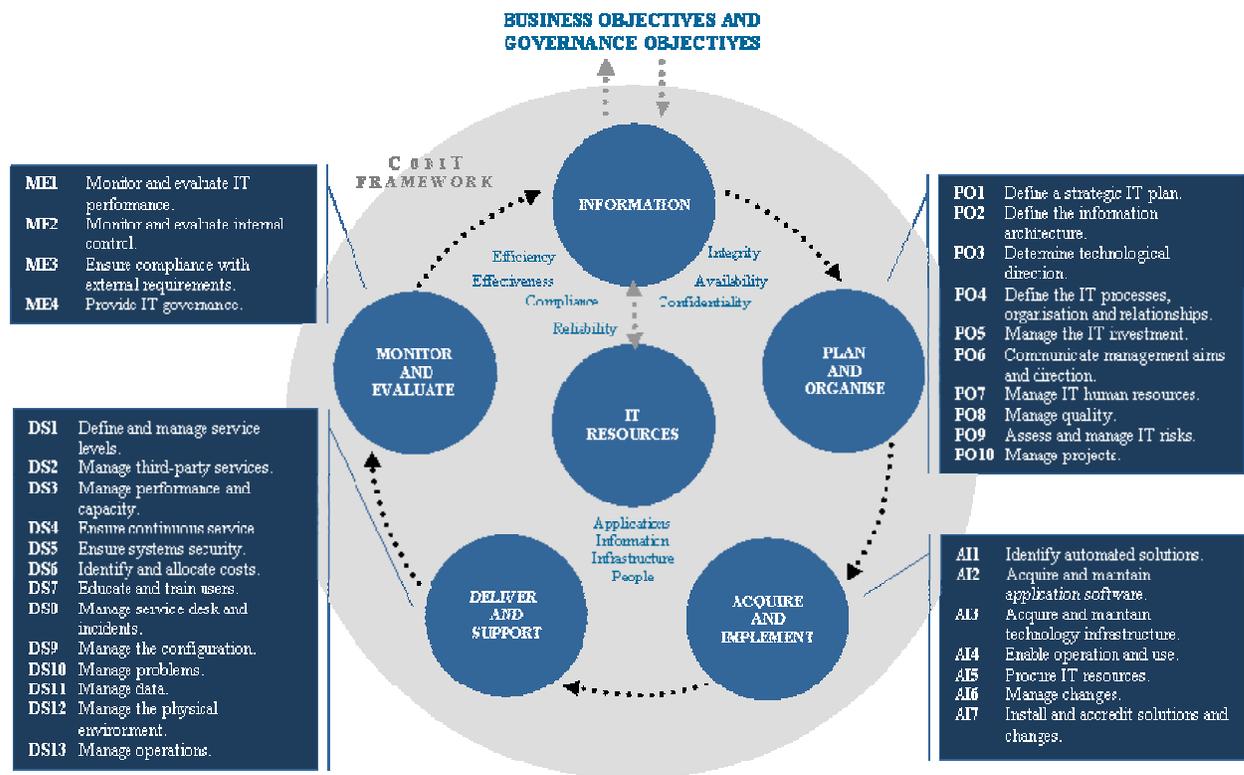
While the COSO framework is generally accepted as the internal control model for enterprises, *Control Objectives for Information and related Technology* (COBIT) is the generally accepted internal control framework for IT. COBIT was first released by the Information Systems Audit and Control Association (ISACA) in 1996 and has been updated to include current IT governance principles and emerging international technical, professional, regulatory and industry specific standards. The resulting control objectives have been developed for application to organization-wide information systems. Now in edition 4.1, COBIT is intended to meet the multiple needs of management by bridging gaps between business risks, control needs and technical issues.

The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help to identify the resources essential for process success, i.e., applications, information, infrastructure and people. The image depicted on the following page was released/published by the IT Governance Institute (ITGI) as reflective of the new COBIT 4.1 Framework that was introduced on May 8, 2007.

Module 2 – Overview of Internal Control over Financial Reporting

Handout 2 – COBIT 4.1 Framework

COBIT Framework



Although there are 34 processes identified within the COBIT framework for assessing IT risk, the EAGLE Program requires compliance with the 10 bolded processes related to financial reporting.

- **PLAN AND ORGANIZE (PO)**

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realization of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organization, as well as technological infrastructure, should be put in place. This domain addresses the following processes:

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships

Module 2 – Overview of Internal Control over Financial Reporting

Handout 2 – COBIT 4.1 Framework

- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- **PO8 Manage Quality**
- **PO9 Assess and Manage IT Risks**
- PO10 Manage Projects

- **ACQUIRE AND IMPLEMENT (AI)**

To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain addresses the following processes:

 - AI1 Identify Automated Solutions
 - AI2 Acquire and Maintain Application Software
 - AI3 Acquire and Maintain Technology Infrastructure
 - AI4 Enable Operation and Use
 - AI5 Procure IT Resources
 - **AI6 Manage Changes**
 - AI7 Install and Accredite Solutions and Changes

- **DELIVER AND SUPPORT (DS)**

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It addresses the following processes:

 - DS1 Define and Manage Service Levels
 - DS2 Manage Third-party Services
 - DS3 Manage Performance and Capacity
 - **DS4 Ensure Continuous Service**
 - **DS5 Ensure Systems Security**
 - **DS6 Identify and Allocate Costs**
 - DS7 Educate and Train Users
 - DS8 Manage Service Desk and Incidents
 - DS9 Manage the Configuration
 - DS10 Manage Problems
 - **DS11 Manage Data**
 - **DS12 Manage the Physical Environment**
 - DS13 Manage Operations

Module 2 – Overview of Internal Control over Financial Reporting

Handout 2 – COBIT 4.1 Framework

- **MONITOR AND EVALUATE (ME)**
All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It addresses the following processes:
 - ME1 Monitor and Evaluate IT Performance
 - **ME2 Monitor and Evaluate Internal Control**
 - **ME3 Ensure Compliance With External Requirements**
 - ME4 Provide IT Governance