COBIT

BA 559: IT Governance

Ben Tsao

12/15/2008

General Overview of COBIT

With information technology now a driving force in today's high tech enterprises, there is a greater need for a more widespread understanding for how IT works. These companies need to practice good IT governance to ensure that the enterprise's IT sustains and extends the organizations strategies and objectives. COBIT or Control Objectives for Information and Related Technology can be summarized as an open standard control framework for IT. Basically, COBIT builds upon the COSO framework for financial processes as a set of best practices used for IT. COBIT's mission is to provide business managers and auditors with a set of generally accepted measures and processes to assist them in maximizing the benefits derived through the use of information technology in day to day use. This will better help them understand their IT systems and will make them develop appropriate IT governance and control within the company such as the right amount of security necessary in order to protect the company's assets.

COBIT concentrates on what should be achieved rather how it should be achieved, therefore COBIT appeals to everyone, not just used by the tech savvy IT personnel. Managers also need to use COBIT because it helps bridge the gap among business requirements, control needs, and technical issues. Therefore, it aids them in developing a strategic IT plan to execute an IT strategy and to continue monitoring the performance of the IT system. IT users mostly use COBIT for the assurance of COBIT's controls and governance while auditors benefit from COBIT because it helps them identify control issues within a company's IT infrastructure.

History of COBIT

Currently, the most recent version of COBIT is version 4.1, which was released in May 2007. Although COBIT was created in 1992 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI), it did not get its first version release until 1996. The IT Governance institute has a COBIT Steering committee branch that continuously researches and helps evolve the COBIT body of knowledge as businesses change and focus on more IT aspects. There have been four major releases of COBIT as the following list shows the version releases as well as the dates on which they were first released:

COBIT First Edition – Released in 1996. COBIT framework was first defined in this edition. The application and of international standards, guidelines, and research into best practices led to the development of control objectives.

COBIT Second Edition – Released in 1998. "Management Guidelines" were added to this edition as well as research of a compilation, review, assessment, and appropriate incorporation of international technical standards, codes of conduct, quality standards, and professional standards in auditing as they relate to the framework and individual control objectives. After the review of the research of each domain, new or modified control objectives were suggested to the COBIT steering committee.

COBIT 3rd Edition – Released in 2000. The management guidelines were further developed as well as other updates of the second edition based on new and revised international references. The COBIT framework was also revised and enhanced to

support increased management control and to introduce performance management and to further develop IT governance. An online version also became available in 2003.

COBIT 4.0 – Released in December 2005. Improves upon version 3 by consolidating most of the separate books into a single volume for ease of use. The main areas of change in COBIT 4.0 are in IT governance, business requirements, harmonization, value creation, enterprise architecture, process definition and flows, language and presentation, and feedback.

COBIT 4.1 – Released in May 2007. Most current version.

COBIT Product [2]

COBIT is a set of written best practices created by the ISACA. It can be purchased or downloaded directly from the ISACA website at http://www.isaca.org. The complete COBIT package consists of:

- Executive Summary
- Governance and Control Framework
- Control Objectives
- Management Guidelines
- Implementation Guide
- IT Assurance Guide

Executive Summary – This section consists of an executive overview of COBIT's key concepts and principles that is designed for senior executives and managers. A synopsis of the framework is also included.

Framework – The framework is the foundation of the COBIT package and keeps it all together. It explains how IT processes deliver information to a business to help achieve its objectives. This delivery is controlled by the 34 IT processes within COBIT contained in each of the four domains (planning and organization, acquisition and implementation, delivery and support, monitor and evaluation). It also identifies which IT resources are important for the IT processes to fully support the business.

Control Objectives – The control objectives are the main thought processes that are within COBIT. The insight for good practice in IT controls is included here. The statements of desired results of the control objectives and IT processes can be found here.

Management Guidelines – Added in COBIT version 3, it is composed of maturity models, to help determine the stages and expectation levels of control and compare them against industry norms. These include critical success factors, key goal indicators, and key performance indicators.

IT Assurance Guide – The assurance guide provides the tools to make sure that IT control objectives can be achieved. It also allows for assurance initiative planning and scoping in a standardized repeatable way so that business and IT can be assessed under a single framework.

COBIT Framework [4]

As it was mentioned earlier, COBIT is mainly used to help support IT governance. In general COBIT provides a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

The focus areas of IT Governance as described by COBIT include:

- **Strategic Alignment** focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs, and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of critical IT resources: applications, information, infrastructure, and people. Key issues relate to the optimization of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance

requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measureable beyond conventional accounting.

The COBIT framework was created with the main characteristics of being business-focused, process-oriented, controls-based, and measurement-driven. Business orientation is the main theme of COBIT. It is designed to provide comprehensive guidance for management and business process owners. Managing and controlling information is the heart of the COBIT framework. Business goals and IT goals need to be aligned to make sure that the enterprise's goals can be achieved.

COBIT Structure [2]

Along with the focus areas of COBIT in IT Governance, the main structure of COBIT covers four domains with 34 total IT processes divided among the domains. These domains include:

- **Plan and Organize (PO)** which covers the strategy and tactics and concerns the identification of the way IT can best contribute to the achievement of business objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and generate the most benefit from the use of IT. The following table lists the IT process in the planning and organizational domain:

IT PROCESSES
Plan and Organize

PO1	**Define a Strategic IT Plan and direction**
PO2	**Define the Information Architecture**
PO3	**Determine Technological Direction**
PO4	**Define the IT Processes, Organization and Relationships**
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)** makes sure that IT strategies and solutions need to be identified, developed, or acquired, as well as implemented and integrated into the business process. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components. The following table lists the IT processes in the acquire and implement domain:

IT PROCESSES
Acquire and Implement

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 Accredit Solutions and Changes**

- **Deliver and Support (DS)** 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. The support processes that are addressed include security issues and training. The following table is the list of IT processes in this domain:

IT PROCESSES
Deliver and Support

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**

- **Monitor and Evaluate (ME)** makes sure that all IT processes are regularly assessed over time for quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance, and governance. Monitoring also covers the issue of an independent assessment of the effectiveness of IT systems in its ability to meet business objectives and the company's

control processes by internal and external auditors. The following table lists the IT processes of this domain:

IT PROCESSES Monitor and Evaluate	
ME1	**Monitor and Evaluate IT Processes**
ME2	**Monitor and Evaluate Internal Control**
ME3	**Ensure Regulatory Compliance**
ME4	**Provide IT Governance**

COBIT and Sarbanes Oxley

The Sarbanes Oxley act (SOX) was enacted on July 30th, 2002 as a response to many corporate and accounting scandals. This legislation established new or enhanced standards for all US public company boards, management, and public accounting firms. These public companies that were subject to SOX were encouraged to adopt either the COBIT framework model or COSO.

COBIT Case Studies [1]

COBIT is used by organizations of all types around the world to ensure that their business plans are aligned with IT Governance and control. The following are a few case studies of different organizations in different fields that have adopted COBIT.

- **SUN Microsystems (Consulting/IT)** – Sun Microsystems is a leading provider of industrial strength hardware, software, and services. 30,000+ employees are employed in over 100 countries throughout the world. Due to increased board attention of optimizing the value of IT and the Sarbanes Oxley act, SUN's IT department sought for a

use of a common framework to view and measure IT alignment for its business strategy. COBIT support and adoption was met with a lot of hesitation at first due to much of the company going under an organizational overhaul. However, the IT department saw the value of having a common framework and this resulted in the SUN IT/COBIT Activities listing, which maps SUN IT processes and activities to COBIT. Although SUN has adopted many elements of COBIT, it has still not been formally adopted into their control frameworks, but the result is looking positive.

- **Curtin University of Technology (Education)** – With over 31,000 students, Curtain University of Technology is Western Australia's largest university. The university was introduced to COBIT while searching for a comprehensive IT governance methodology. The University's IS department realized that COBIT would increase acceptance and reduce time to implement the IT governance program. The implementation process began with university auditors using COBIT as a guide for formal audits of the central ICT organization. Within a year, the internal audit department of the university reported improvements in maturity levels across the board. Because of this success, the university is currently trying to implement COBIT on an operational level instead of using it just for audits.

- **Adnoc Distributions (Energy)** – Adnoc is an energy company of about 5,500 employees located in the United Arab Emirates. Adnoc Distribution did not have established processes and procedures to provide IT services in a effective and efficient manner. IT was also not aligned to the business to support organizational goals. Therefore the

leaders decided to implement COBIT to add discipline, improve service levels, increase IT user's satisfaction, and improve IT governance practices. COBIT was chosen as the best framework to use because it addressed all elements of the processes including key performance indicators and key goal indicators. After the implementation, all four IT departments at Adnoc Distribution are using COBIT including data center operations, retail automation, network and help desk, and application systems. The main goal of implementing COBIT was to improve the efficiency and delivery of the information system services and improve existing process and that has been accomplished.

- **Prudential (Financial Services/Insurance)** – The Prudential branch in Asia employs over 9000 personnel in 12 countries across the Asia Pacific region. By providing financial services worldwide, they recognized the need to adopt an IT governance framework to provide its operations in Asia with a uniformed platform to sustain growth and eliminate risks. COBIT helps Prudential in Asia with the process that better IT control is the key to sustain corporate growth in Asia. COBIT also provides essential foundation for management support and helps protect corporate integrity and reputation. For Prudential Asia, COBIT is also a value creator and helps create long lasting results for the corporation. Although the COBIT implementation is still in process, there have already been results in enhanced communications between IT and business operations and better responsiveness in project management.

- **US House of Representatives (Government)** – There have been a large number of audit reports addressed by the Office of the Inspector General (OIG) that there were

weaknesses in various IT operations of the House including lack of policies and procedures, and poor systems design. Management needed to take control of the situation and establish clear roles and responsibilities and to adopt an IT governance framework which was COBIT. The Chief Administrative Officer (CAO) was in charge of implementing COBIT and recognized that it would benefit the House Information Resources and Finance organizations. Soon, the CAO implemented COBIT and it became an integral governance component of all House activities. The OIG incorporated COBIT into its policies and procedures manual and used it as an integral resource for all OIG IT audit activities. COBIT turned out to be a key element for the audit planning process and training the needs assessments of all staff and audit reporting processes. The House found that COBIT was a great tool for running the operations and audits of the house and greatly improved the entire operation.

- **Harley Davidson (Manufacturing/Transportation)** – Known throughout the nation as a leading cult motorcycle manufacturer, Harley Davidson faced the challenge of getting management, IT, and auditing all aligned together to work towards increased control in their business model. After the SOX act, Harley Davidson created an IS compliance department and began implementing a vendor's general computer controls model. The risk specialist at Harley Davidson recommended converting the control framework to COBIT. After implementing COBIT, Harley Davidson is able to choose the areas selected for auditing business values and control needs instead of at random.

Conclusion

Since its first inception and its many revisions, COBIT has shown us why it is still the one of the best frameworks to use for control in IT Governance. Its ease of use along with its general acceptability allows for a widespread of companies and their managers to implement this set of best practices. With so many top companies around the world adopting the COBIT framework, this set of controls should be lasting for a long time.

References

1. ISACA – Serving IT Governance professionals, http://www.isaca.org
2. COBIT – Wikipedia, http://en.wikipedia.org/wiki/COBIT
3. COBIT – Forums and information, http://www.controlit.org/
4. IT Governance Institute, COBIT 4.1 Executive Summary http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172