IT Governance and Control:
An Analysis of CobIT 4.1

Prepared by: Mark Longo

December 15, 2008

Table of Contents

Introduction

The ever-increasing competitiveness of modern business creates the need to utilize information technology to create efficiencies within the company. Information systems and related business processes require effective risk management, which can be achieved through appropriate use of control within the organization. CobIT 4.1 is a widely used IT Governance framework that takes a broad based best practices approach to linking IT to business goals, recognizing key IT process risks, and introducing more accountability into business and IT processes.

Project Scope

This project will attempt to take a creative approach to learning about CobIT and its role inside an organization. I will use an *imaginary* retail store, known as Store XYZ, as a case study to create an original IT Framework based on CobIT 4.1. We will assume this *imaginary* Store XYZ is operated like a small business. This assumption will make the business model of the business much simpler, therefore, allowing me simplify the process of planning, implementing, and monitoring an IT Governance system. As I enter the public accounting profession in an Advisory role, I hope this project will provide me with a base to understanding larger/more complex clients. CobIT 4.1, provided by the IT Governance Institute website, is the only source used during the report.

IT Governance

According to CobIT 4.1, the purpose of IT governance is to ensure that an organization's Enterprise IT helps achieve organizational objectives. The figure below represents the key components of IT Governance: strategic alignment, value delivery, risk management, resource

management, and performance measurement. Ideally, an organization's IT Governance should create value and even improve financial performance. IT systems must be integrated with organizational objectives to effectively measure performance and provide value. All the while, IT provides appropriate levels of risk management and reliability. More specifically, Store XYZ can accomplish effective IT governance by creating control objectives to address the various risks that occur within business and IT processes. Controls must be created to mitigate the risks that threaten the organization's objective.

Source: CobIT 4.1

CobIT 4.1 Framework

The CobIT acronym stands for *Control Objectives for Information and related Technology.* CobIT is a framework whose goal is to achieve superior management and control of IT and provide a roadmap to ideal IT Governance. An organization should recognize business processes and associated IT processes, likely and material risks, and design mitigating controls using the guidance provided by CobIT. This report will analyze 6 General control objectives, 6 IT Application control objectives, and several other control objectives across the 4 CobIT-defined

domains of IT management: Plan and Organize, Acquire and Implement, Deliver and Support Monitor and Evaluate.

General Control Objectives

The CobIT 4.1 process has so-called "generic control requirements" that apply generally to all businesses. Listed below is a summary of the 6 control objectives (PC 1-6) from CobIT 4.1:

PC1 Process Goals and Objectives

PC1 involves designing "SMARRT" IT process objectives that are specific, measurable, actionable, realistic, results-oriented, and timely. Each business and IT process should be linked to the business strategy and monitored with metrics.

PC2 Process Ownership

PC2 suggests assigning "owners" to IT processes to clarify responsibilities and create accountability within the process, thus allowing employee performance to be more easily evaluated. In addition, PC2 emphasizes assigning clear expectations and responsibilities to process owners to avoid an expectation gap.

PC3 Process Repeatability

Process Repeatability refers to the reliability and consistency, yet flexibility needed in the design of IT processes. A reliable and flexible system will produce accurate results in times of stability and dynamism.

PC4 Roles and Responsibilities

PC4 seeks to thoroughly define key business processes and associated activities. The responsibilities of process owners must be clear.

PC5 Policy, Plans and Procedures

PC5 “defines and communicates how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training.”

PC6 Process Performance Improvement

In order to measure performance, a detailed set of metrics must be established. Targets should be set, and performance measured in this on-going task of improving processes.

Application Control Objectives

The purpose of Application Control Objectives is to provide guidance into managing data inputted into the system, the reliability of system reporting, and assuring the data provided is accurate. Data security, integrity, and validity are recurring themes. The following section provides 6 suggested Application Control Objectives and brief explanations as they may relate to Store XYZ.

AC1 Source Data Preparation and Authorization

The first step is controlling the quality of data and information that flows into the IT system. This includes ensuring that Store XYZ’s source documents such as PO’s, invoices, customer information, etc. is originated and validated by the appropriate employees, through an

established process, and with accurate information. A risk in this process is that source forms are improperly validated and authorized. A control that can help mitigate this would be adopting segregation of duties so that a system of checks and balances is put in place where employees are held accountable for monitoring each other. For example, every payment made to a vendor should have the signature of the process owner and another *independent* employee to verify the payment accuracy and other pertinent information. Duty segregation should help to reduce careless errors by standardizing the validation and entry process, and it helps to deter fraud or other misuses of power. It is worth noting that segregation of duties within a small organization, such as Store XYZ, is often difficult to achieve because of the small number of managers and employees.

AC2 Source Data Collection and Entry

AC2 builds off of AC1 but focuses more on timely data input by appropriate staff. The risk inherent in this process is that too many employees may have access to the system, in other words, Store XYZ's IT system lacks restricted access. For example, only a select group of employees should have the ability to enter in a PO or pay an invoice. The system should have a unique username and password for each employee, so that the actions of all employees can be monitored and accountability given. All transaction approvals, authorizations, and data changes should be restricted to management, and no employee should be granted access to information not related to their job function.

AC3 Accuracy, Completeness and Authenticity Checks

AC3 maintains the goal of ensuring that transactions are accurate, complete and valid. In modern companies, most transactions occur digitally, and Store XYZ would make use of IT to facilitate transactions and financial statement preparation for public companies.

AC4 Processing Integrity and Validity

AC4 seeks to maintain the integrity of the data throughout the entire data processing cycle. This includes having adequate security and control in place to restrict system access and detect suspicious transactions. In order to ensure that order data is processed accurately, Store XYZ can sample a batch of transactions and follow each through the system to the ledger. The users should be able to identify the person who authorized the transaction, entered it, and if any changes were made to the entry. Another unique control is to program a product flow analysis into the procurement system, so that order amounts significantly different from a benchmark period can be red flagged.

AC5 Output Review, Reconciliation and Error Handling

This control objective establishes the importance of "ensuring that output is handled in an authorized manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used." On a sample basis, the output data should be cross-checked with source documents to ensure that system output is restricted to key employees and that no un authorized changes to the information occur.

AC6 Transaction Authentication and Integrity

AC6 protects data during transmission. It states that control objectives should help ensure that data transmitted within the company is sent to appropriate locations, and the end users can verify its validity via a "stamp of approval." AC6 differs from AC5 because AC6 focuses on the transmission of data from internal applications to business and operations.

IT Domains and Control

An important first step in implementing adequate IT control is creating control objectives whose design ensures that business objectives are achieved and risks are mitigated within business and IT processes. This analysis is divided into four CobIT-defined domains: *Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.*

Plan and Organize

Within the Plan and Organize (PO) domain, there are 10 IT processes that relate to designing, implementing, maintaining, and monitoring IT projects. Within each of the 10 Plan and Organize processes are several control objectives. The list below summarizes the 10 IT processes:

Plan and Organize Process Summary	
PO1 Define a Strategic IT Plan	PO6 Communicate Management Aims and Direction
PO2 Define the Information Architecture	PO7 Manage IT Human Resources
PO3 Determine Technological Direction	PO8 Manage Quality
PO4 Define the IT Processes, Organization and Relationships	PO9 Assess and Manage IT Risks
PO5 Manage the IT Investment	PO10 Manage Projects

Of these 10 processes, I will discuss *PO1: Defining a Strategic IT Plan* in more detail in terms of Store XYZ. I will address specific control objectives, risks, and controls that process stakeholders can utilize.

In order to solidify the linkage between IT resources and business objectives, Store XYZ must *define a strategic plan* and develop control objectives. Control objectives should focus on delivering value, aligning IT with the business, measuring and evaluating system design, and achieving efficient portfolio management. For example, Control Objective *PO1.2 Business-IT Alignment* provides guidelines by which a company can utilize control to align its IT and business objectives.

For example, lets say that Store XYZ actively sought to achieve a certain inventory turnover rate as part of its core strategy. When determining if a solid link between this goal and IT exists, we must determine if the IT system provides employees the tools needed to meet the business objectives. For example, to align this business objective with IT, the system needs certain capabilities. Most importantly, a reliable method of tracking inventory shipments needs to be present and fully integrated with IT. From the warehouse to the checkout line, the barcode inventory accounting system must be reliable across all areas. Once Store XYZ has a reliable inventory accounting process, the inventory manager can monitor system metrics such as inventory turnover and obsolescence rates at the click of a button. However, whether PO's and invoices are sent/received from suppliers electronically or manually, the data needs to eventually be accessible in electronic format to efficiently analyze the data. By taking a systematic

approach to understanding how risk within the inventory process affects its goals, Store XYZ successfully aligned its IT capabilities and business strategy.

Acquire and Implement

Within the Acquire and Implement (AI) domain, there are 7 IT 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 Accredit Solutions and Changes

Of these 7 processes, I will discuss *AI4: Enable Operation and Use,* which is concerned with the process of training employees to use system applications and software. According to CobIT 4.1, an important control objective is ensuring *knowledge transfer to end-users.* Employees must have the appropriate knowledge and skills required to use the IT system to create value and utilize metrics to evaluate performance to achieve organizational objectives. The risks inherent in this process include: inadequate employee training, system complexity, employee skill, and performance measurement. To mitigate these risks, Store XYZ, for example, should provide one-on-one training. A larger company may decide to adopt a training program up to several days long and provide online courses and certification. The company should also create a detailed operators manual. The manual can discuss the core business and IT processes,

responsibilities of process owners, important metrics, and provide other detailed instructions on using the IT applications. To ensure employees understand the system, the company can administer an annual examination that is tailored to testing the knowledge of specific process owners. Perhaps most importantly is that the design of the software and applications needs to be user-friendly.

Deliver and Support

Within the Deliver and Support (DS) domain, there are 13 IT processes:

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

Managing Third-Party Services (DS2) is an important IT process that requires control planning. There are 4 CobIT-defined control objectives areas, of which I will discuss Supplier Risk Management. Supplier risk management is a broad concept that can be simplified into more specific control objectives. The chart below lists possible control objectives that can be achieved through IT within Store XYZ. For each control objective, I identified risks inherent in the process and mitigating controls that provide detective or preventive control.

Store XYZ Control Matrix – Supplier Risk Management

Control Objectives	Risks	Controls
Supplier shipments are on time, accurate, and efficient	(1) Incorrect shipments or late orders	(1) Note ALL supplier "Incidences" in the system. Review supplier "Incidences" regularly and discuss issues with supplier
Suppliers offer competitive prices on quality products	(1) Current supplier prices are higher than other suppliers	(1) Utilize historical system data to monitor changes in inventory costs and supplier fees.
	(2) Product quality is poor	(2) Create a "product return" reporting process, whereby customer service enters product returns and defects into a database. Monitor quality alerts and involve supplier
Supplier contracts conform to legal and contract requirements	(1) Product safety recalls	(1) Working with suppliers, create a formal method of reporting and communicating product recalls, and automatic/conditional shipment cancellation.
	(2) Supplier shipment/payment terms are in accordance with a legal contract	(2) Analyze credit terms of supplier contracts. Review new supplier contracts align to financial reporting

Monitor and Evaluate

Within the Monitor and Evaluate (ME) domain, there are 4 IT processes CobIT 4.1 defines:

- ME1 Monitor and Evaluate IT Performance
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Compliance With External Requirements
- ME4 Provide IT Governance

I will discuss *ME2: Monitor and Evaluate Internal Control* in more detail. In order to effectively monitor and evaluate internal IT controls, a substantial amount of control testing may be required. The purpose of control testing is to provide assurance that a company's internal control structure is reliable, secure, and well designed. For example, suppose Store XYZ creates the following control objectives to monitor and evaluate internal control quality:

Store XYZ Control Matrix – Evaluating Internal Control Quality

Control Objective	Risk	Controls
Security Changes to restricted access applications are approved by the appropriate personnel	Unauthorized individuals obtain access to proprietary information	Additions and changes to user access are approved by IT security personnel and upper management.
Control system design The design of internal controls are adequate and consistent with the company's objectives	Internal controls lack coherence and do not facilitate objective achievement	An annual review of internal controls and adherence to CobIT and COSO principles
Financial Reporting Payment to suppliers are initiated and approved by appropriate personnel in accordance with segregation of duties principles	An employee is able to initiate, approve, and record transactions	Transaction source documents are reviewed for appropriate approval. IT system recognizes inappropriate user power and creates and formal "Incident" inquiry

Conclusion

In conclusion, this report analyzes CobIT 4.1 and how its guidance helps create an ideal control structure within a business. I analyzed control objectives, risks, and mitigating controls across 4 IT domains: *Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.* I felt that this project was worthwhile and provided valuable insight into IT systems and control.