# A Survey of IT Governance through COBIT, ITIL, and ISO 17799

**Samantha Schreiner**

**University of Illinois at Urbana-Champaign**
**BA 559 – Professor Michael Shaw**

**December 15th, 2008**

## INTRODUCTION

The use of IT is critical to an enterprise's success in today's world. In many organizations it is fundamental to support, sustain and grow the business ("About IT Governance', 1). IT provides opportunities for competitive advantage and increases in productivity. It is fundamental for managing resources, suppliers, customers, and the transitioning of today's market value from the tangible to intangible ("Board Briefing on IT Governance", 13). An enterprise's ability to leverage IT has become a universal business competency ("Board Briefing on IT Governance", 13). Since IT is critical for the execution of business strategy, governance needs to pay particular attention to managing IT. In this paper, I will explain what IT Governance is, its objectives and how it is accomplished. Then I will go over the three major IT Governance frameworks, COBIT, ITIL, and the ISO 17799 standard, and survey how the frameworks work to help achieve management's goals on managing IT.

## IT GOVERNANCE

The Institute on IT Governance defines IT governance as "the integral part of enterprise governance that consists of the leadership and organizational structures and processes that ensure that an organization's IT sustains and extends the organization's strategies and objectives" ("Board Briefing on IT Governance", 10). The purpose of IT governance is to direct IT applications and to make sure that IT's performance meets the following four objectives: alignment of IT with the enterprise, use of IT enables the enterprise to take advantage of all opportunities and maximize benefits, IT resources are used responsibly, and IT-related risks are appropriately managed ("Board Briefing on IT

Governance", 11). The overall objective of IT governance in the listed activities are to make sure that the enterprise is able to sustain its operations and implement the strategies it requires necessary to extend its activities into the future ("Objectives of IT Governance", 1).

The process of IT Governance starts with setting the objectives for the enterprise's IT. As shown in Exhibit 1, IT governance provides the beginning direction and from then on a loop is established where performance is measured and then compared to objectives ("Process of IT Governance", 1). From there a redirection of activities and a change of objectives can be done when seen as necessary.

**FRAMEWORKS**

IT governance is the responsibility of executives and board members, but the actual governance activities must go through many levels of the enterprise ("Board Briefing on IT Governance", 14). Exhibit 2 shows the typical IT governance activities decided on by top management at the board and executive level ("Board Briefing on IT Governance, 57). The board and executives on the whole set the direction of IT governance for the firm, while relying on the rest of enterprise to give the information required for decision-making and evaluation ("Board Briefing on IT Governance, 14). In order for this to work throughout the different management levels of the enterprise, top management's strategy and goals must be effectively stated and brought to each different level. An IT Governance framework is a key element in ensuring proper control and governance over information technology and the systems that create, store, manipulate and retrieve information by making sure management's strategy is brought out at each

level of the enterprise ("About IT Governance", 1). In a recent survey of security professionals by Enterprise Strategy Group, it was found that 72% of North American enterprise-class organizations (organizations with over 1,000 employees) state they are using one or more formal IT control and process model, with the most widely used being COBIT, ITIL, and ISO 17799 (Turner, 1).

## COBIT

COBIT was developed in 1996 by the Information Systems Audit and Control Association (Handler, 92). COBIT's stated mission is "to research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals" ("COBIT 4.1 Framework", 9). COBIT stands for "Control Objectives for Information and related Technology." COBIT s a framework and tool set that allows management to bridge together control requirements, technical issues and business processes ("COBIT 4.1", 2). It was created with the main characteristics of being business-focused, process-oriented, control based and measurement driven ("COBIT 4.1 Framework", 10). As shown in Exhibit 3, the framework is based on the principal that to provide the information the enterprise needs to achieve its objectives, the enterprise needs to invest in, manage, and control IT resources using a structured set of processes to provide the services that deliver the needed information ("COBIT 4.1 Framework", 10).

COBIT identifies that business goals can be fulfilled by having a clearly defined set of processes that use people skills and technology infrastructure to run business

applications while leveraging business information. The resources along with the processes give a structured architecture of IT. COBIT identified four major resources in order to fulfill business goals. These include applications of the automated user systems and manual procedures to process information, information of all forms of data used in the business, infrastructure the technology and facilities infrastructure to enable the processing of applications, and all personnel required to manage all aspects of the information systems and services ("COBIT 4.1 Framework", 12).

In addition to using resources to support business goals, COBIT also defines processes. COBIT is a process-oriented framework and defines IT activities in a generic process model within four domains ("COBIT 4.1 Framework", 12). As shown in Exhibit 4, the domains include Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate ("COBIT 4.1 Framework", 12). Each domain covers specific activities and risks that need to be managed. Within each domain, COBIT has 34 IT processes that are generally used with a link made to the business and IT goals that are being supported with information on how the goals can be measured, the main activities, and the person responsible for making sure the processes are completed ("COBIT 4.1 Framework", 13).

Plan and Organize covers identifying the best way IT can help achieve the company's business objectives. The domain covers the strategy and tactics in which the strategic vision is planned, communicated and managed for different perspectives ("COBIT 4.1 Framework", 13). It asks questions such as "are IT and the business

strategy aligned?", "does everyone in the organization understand the IT objectives?", and "are IT risks understood and being managed?" ("COBIT 4.1 Framework", 13).

Acquire and Implement covers IT solutions being identified, developed or acquired, and implemented into the core business processes ("COBIT 4.1 Framework", 13). It includes guidance on making sure that maintenance and system changes are performed to make sure that business objectives are continually achieved and up to date. The domain asks questions such as "are new products likely to deliver solutions that meet business needs?", "will the new systems work properly when implemented?", and "will changes be made without upsetting current business operations?" ("COBIT 4.1 Framework", 13).

Deliver and Support covers the actual delivery of required services. The domain also involves management of security and continuity, service support for users, and management of data and operational facilities ("COBIT 4.1 Framework", 13). It asks questions such as "are IT services being delivered in line with business priorities?", "are IT costs optimized?", and "are adequate confidentiality, integrity and availability in place for information security?" ("COBIT 4.1 Framework", 13).

Monitor and Evaluate covers reviewing all IT processes for quality and compliance with control requirements ("COBIT 4.1 Framework", 13). It addresses performance management, monitoring of internal control, regulatory compliance and governance ("COBIT 4.1 Framework", 13). It asks questions such as "is IT's performance measured to detect problems before it is too late?", "does management

ensure that internal controls are effective and efficient?" and "can IT performance be linked back to business goals?" ("COBIT 4.1 Framework", 13).

## COBIT IN PRACTICE

A company that uses the COBIT framework is Allstate. Allstate's internal audit implemented COBIT in 2000 and uses the framework to scope and plan all audits ("Allstate", 1). Allstate adopted COBIT after the Sarbanes-Oxley Act was passed to ensure compliance and evaluate its own IT governance and control ("Allstate", 1). COBIT was specifically chosen to "ensure alignment between business strategies and technology investments" after it was demonstrated that COBIT could "give a structured means to ensure consistent and appropriate IT controls throughout the company" ("Allstate", 1). COBIT fits well for Allstate because it provides guidance on assessing automated control in main business processes and also assessing control activities by its support team ("Allstate", 1). COBIT allowed Allstate to have a common language for communications between its processes and controls ("Allstate", 1). Allstate has commented that COBIT allows it to "achieve an effective balance of appropriate and consistent controls to improve the efficiency and effectiveness of the business" ("Allstate", 1).

## ITIL

ITIL stands for "Information Technology Infrastructure Library" and defines the organizational structure and requirements for an organization's IT ("ITIL", 1). It gives a standard set of operational management tasks to allow management to better control the company's IT ("ITIL", 1). ITIL provides recommendations for a large range of IT

operations and emphasizes information confidentiality, integrity and availability (Turner, 1). The framework was created under the British government and is a registered trademark of the UK Government's Office of Government Commerce ("ITIL", 1).

ITIL is composed of a serious of books that give guidance on the provision of quality IT services ("What is ITIL", 1). The latest version is ITIL v3. Version 3 came out in 2007, giving a broader scope than version 2 ("Version 3", 1). The five volumes include ITIL Service Strategy, ITIL Service Design, ITIL Service Transition, ITIL Service Operation and ITIL Continual Service Improvement ("ITIL", 1).

The Service Strategy volume applies to IT Service Management and gives guidance on leveraging service management capabilities to deliver value to customers ("ITIL Service Strategy", 1). It deals with service management in respect to strategic analysis, planning, positioning, and implementation of service models, strategies, and strategic objectives ("ITIL Service Strategy", 1). The volume gives guidance on the design, development, and implementation of service management, as well as on the principles necessary to develop service management policies, guidelines and processes ("ITIL Service Strategy", 1). It involves setting goals and performance expectations in order to prioritize and select opportunities ("ITIL Service Strategy", 1). Some topics include market developments, service assets, service catalog, and strategy implementation ("ITIL Service Strategy", 1).

Service design takes the strategic plans and objectives and turns them into reality. It gives guidance on putting together infrastructure, applications, systems, and process to feasible service offerings through different designs and specifications ("Service Design",

1). It includes design methods and principles for turning company objectives into services and assets ("Service Design", 1). The volume also includes changing and improving old services necessary to increase value ("Service Design", 1).

Service Transition gives guidance on making sure the services provided follow the intended strategy. The volume also makes sure that through the design and implementation the service can be maintained and operated ("Service Transition", 1). It gives advice on transitioning new and changed services and how requirements in the Service Strategy volume put into the Service Design volume are realized in the Service Operations volume ("Service Transition", 1). The volume basically accommodates the volume's before and after guidance for ITIL from planning to operations. This section also tries to prevent defects in the system while still allowing for improvements and innovation ("Service Transition", 1).

The Service Operation volume involves guidance on how to manage a service on a day-to-day basis ("Service Operation", 1). It gives advice on supporting operations as well as set practices in service operation management ("Service Operation", 1). The volume tries to help management achieve efficiency and effectiveness and make sure that service operations fulfill the strategic objectives ("Service Operation", 1). Techniques are focused to make sure operations are maintained while allowing for changes in different levels of design, scope, scale, and service ("Service Operation", 1). The most detail in this volume is provided on addressing control perspectives ("Service Operation", 1).

The last volume is Continual Service Improvement, which reflects on measuring service performance. It gives guidance on different principles, practices and methods from change management to capability improvement to allow improvements in service quality ("Continual Service Improvement", 1). The volume gives guidance on improving operational efficiency and business continuity is also looked at to be improved, as the volume focuses on linking efforts and outcomes to maximize the IT Service Management process ("Continual Service Improvement", 1).

## ITIL IN PRACTICE

A major company that uses the ITIL v3 framework today is Microsoft. Microsoft has adapted ITIL v3 to its service life cycle across the Microsoft Core Windows Platform because the company needed "task-level guidance aimed at their roles" that can be implemented into daily operations ("How Microsoft Moves ITIL V3 from Concept to Practice", 5). One of the leading authorities on IT Service Management and former CEO of itSMF International, Aiden Lawes, claims:

> "ITIL is and always has been generic good practice guidance which enterprises need to adopt and adapt for their individual circumstances. While it was implicitly acknowledged that complementary material would add value, v3 explicitly recognizes the need for complementary guidance that will assist enterprises to develop solutions in specific market sectors or for managing specific technologies. Such complementary material can, and in many cases should, come from those who best understand the specific environment. Hence, the Microsoft suite of offerings is seen as adding immense value to the marketplace. The comprehensive nature of the suite demonstrates how important Microsoft considers Service Management to be. The emphasis on business needs and value as the driving force for decision making fits perfectly with the core ITIL thrust and the various components in the suite can enable enterprises to accelerate the development of their own quality solutions. Addressing the key areas of people, process, and tools, the suite provides a comprehensive toolkit for those wrestling with the complex challenges inherent in Service Management." ("How Microsoft Moves ITIL V3 from Concept to Practice", 5).

ISO 17799

ISO 17799 was first published by the International Organization for Standardization in 2000, being derived from an earlier UK standard BS7799 (Gossels, 1). Although it is still commonly referred to as ISO 17799, it was renumbered and renamed ISO 27002 in July 2007. ISO 17799 is a standard that is used as a framework and assists companies in establishing risk assessment methods, policies, controls and counter measures (Myles, 44). The standard is not only used for information security but also to establish guidelines for certification, compliance and audits (Myles, 44). The framework is organized into 11 security control clauses, each with 39 main security categories (Myles, 44). Each category has a control objective with one or more controls to follow the objective. In addition to this, there are suggested steps shown in Exhibit 5 to starting and implementing an information security program.

The first step is to conduct risk assessments. This part should be completed before security procedures are designed. Risk analysis is defined as "a process of identifying the risks to an organization and often involving an evaluation of the probabilities of a particular event of an assessment of potential hazards" (Myles, 44). Risk assessments should be conducted to understand, analyze, determine, and evaluate the risks likely to occur in the company's environment (Myles, 44). These processes involve IT in relation to information processing facilities, facilities management, human resources, records management and risk management groups (Myles, 44). All company areas must work together to determine the controls to minimize the evaluated risks. The

is done to isolate events that could result in damaging business processes. The standard recommends this risk analysis to be done on a regular basis as risks are ever changing.

The second step is to establish a security policy. At this stage, an information security policy gets developed, authorized by management, published and communicated (Myles, 46). It must apply to all information assets, explain implications on work processes and responsibilities and show management's commitment to the policy (Myles, 46). The policy needs to be periodically evaluated and updated to reflect changing company goals (Myles, 46).

The third step is to compile an asset inventory. This is where the company's intellectual property and physical assets are identified and detailed to know what and where the company's resources are. The details reflect how the assets are to be used and distinguishes the types, formats and ownership control issues (Myles, 46). This allows for rules to be implemented on the asset's usage.

The fourth step is defining accountability. This needs to be done so that roles and responsibilities are understood so the information security program can be properly implemented (Myles, 46). The ideal situation is to outline roles and responsibilities in job descriptions and in terms of employment (Myles, 46). This stage highly involves Human Resources (HR) working with IT and risk management, as employees are often the best able to prevent risky incidents from occurring (Myles, 46). HR must highly pre-screen employees and perform background checks to make sure employees have a great deal of integrity (Myles, 48). Information security awareness, education and training must be routine to make sure employees know what is expected and are consistently

updated on their responsibilities (Myles, 48). A key part is standardizing processes for security breaches and making plans when employees leave or change jobs (Myles, 48).

The fifth step is addressing physical security. The company's facilities and equipment must be fail proof to prevent intrusions, unauthorized access and theft (Myles, 48). There should be guidelines for security perimeters, entry controls, threats and access patterns with supporting utilities, power, and telecommunication networks addressed (Myles, 48). The disposal of equipment also must be specifically addressed so information can be completely deleted or "wiped" clean (Myles, 48).

The sixth step is documenting operating procedures. This is done because a program is more established when its administration, policies, procedures and processes are formally documented (Myles, 48). Here operating procedures, details on executing instructions and the management of the audit trail and system log information are defined (Myles, 48). All parts of the information security program are involved. By formally documenting all activities, an organization will be able to keep track of the development, implementation and associated documentation for the program (Myles, 48).

The seventh step is determining access controls. This part of the standard gives guidelines for establishing policies and rules for information and system access (Myles, 49). The standard recommends access control measures including setting up user registration procedures, allocating privilege and passwords, and implementing a clear desk and screen policy. The standard also recommends managing: unattended equipment, virtual private network solutions, wireless networks and authentications, network service issues such as routing and connections, telecommuting virtual spaces and intellectual

property rights, cryptographic keys and procedures, software development, testing, and production environments, program source code and libraries, change control procedures and documentation, patches, updates, and service packs (Myles, 49).

The eight step is coordinating business activity. This part of the standards gives reporting requirements, response and escalation procedures, and business continuity management (Myles, 50). As company's can go through security breaches, all organizations must have a formalized manner or response to these events (Myles, 50). Business continuity management addresses these events that can interrupt critical business functions (Myles, 50). The formalized process should include: identifying risks and possible occurrences, conducting business impact analyses, prioritizing critical business functions, developing countermeasures to mitigate and minimize the impact of occurrences, compiling business continuity plans and setting up regular testing methods for plan evaluation and updates (Myles, 50). This part of the standard also recommends the formalized plan including emergency or crisis management, resumption plans, recovery and restoration procedures, and training programs (Myles, 50). The plan must be tested by simulating and rehearsing real-life situations in order to determine how well the plan actually works (Myles, 50).

The final step is demonstrating compliance. This part of the framework gives actual standards for intellectual property rights, risk management requirements, and compliance measures (Myles, 50). In today's business environment, all companies must show compliance to laws, regulations, and legislative requirements for all business transactions. Following these rules and regulations is a crucial part of information

security and will contribute to the company showing corporate accountability (Myles, 50). All policies and procedures must be followed up on and evaluated as well to evaluate compliance and determine implementation effectiveness (Myles, 50). Audit controls and tools must be specifically addressed in order to find areas that need improvement (Myles, 50). As specified before, it is especially crucial to document all this information for standard compliance for the audit.

## CONCLUSION

As IT governance is necessary for an entity's success in necessary IT endeavors and compliance; COBIT, ITIL, and ISO 17799 all provide adequate IT governance frameworks. IT experts even suggest that company's can use more than one framework in order to better meet external pressures (Turner, 1). With today's diverse regulatory requirements for large companies who run operations in many different industries or countries, it may be difficult for just one framework to fully apply. Complicated regulations such as Sarbanes-Oxley, Federal Information Security Act, Health Insurance Portability Accountability Act, and Payment Card Industry Data Security Standard may require an entity to implement more than one framework to better comply (Turner, 1). Some reasons more than one framework can be better include: the fact that different regulatory programs are likely to emphasize different aspects of physical, logical and virtual information and IT security management activities, requiring organizations to draw on best practices and reporting from multiple sources, the need to align policies and priorities across many different decision makers representing a broad mix of business, security and IT stakeholders, the need to better coordinate communications and workflow

across many diverse IT and security operations groups, and the need to validate the information security choices implemented with a broad range of end-users, national and local government agencies and, in some cases, national and global networks of partners (Turner, 1). The more standards the better communication and cooperation between a company's divisions so reporting capabilities as well as overall business processes are greatly enhanced (Turner, 1).

To conclude, COBIT, ITIL, and ISO 17799 can be used alone or in corroboration. A company must look at its size and what it needs to best help its business processes and follow regulations. Then from there it can decide what framework best fits to meet its IT governance needs.

# Appendix

## Exhibit 1

QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

## Exhibit 2


QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

**Exhibit 3**

QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

**Exhibit 4**

QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

**Exhibit 5**


QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

## Works Cited


"About IT Governance." 2008. IT Governance Institute. 19 November 2008. < http://www.itgi.org/template_ITGI.cfm?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657>

"Allstate." 2008. IT Governance Institute. 5 December 2008. http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=13502&TEMPLATE=/ContentManagement/ContentDisplay.cfm

"Board Briefing on IT Governance." 2003. IT Governance Institute. 19 November 2008. <http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=39649>

"Cobit 4.1." 2008. IT Governance Institute. 19 November 2008. http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf

"Cobit 4.1 Framework." 2008. IT Governance Institute. 19 November 2008. http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172

"Continual Service Improvement." 2007. ITIL & ITSM World. 5 December 2008. <http://www.itil-itsm-world.com/cserv.htm>

Gossels, Jonathan G. "ISO 17799: Pay Attention to this One." 2001. System Experts Corporation. 1 December 2008. <http://www.systemexperts.com/tutors/17799.pdf>

Handler, Robert and Bryan Maizlish. IT Portfolio Management Step-By-Step. New Jersey: META Group, 2005.

"How Microsoft Helps Overcome Obstacles to Service Management Success." 3 March 2008. Microsoft TechNet. 7 December 2008. <http://technet.microsoft.com/en-us/library/cc305134.aspx>

"ITIL." 2008. Open Guide. 5 December 2008. <http://www.itlibrary.org/>

Myler, Ellie. "Standard for Security." The Information Management Journal. November/December 2006. EBSCO. University of Illinois Library. 5 December 2008. http://www.library.uiuc.edu/orr/

"Objectives of IT Governance." 2008. IT Governance Institute. 19 November 2008.

<http://www.itgi.org/template_ITGI.cfm?Section=Objectives&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19661>

"Process of IT Governance." 2008. IT Governance Institute. 19 November 2008. <http://www.itgi.org/template_ITGI.cfm?Section=Process&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19660>

"Service Design." 2007. ITIL & ITSM World. 5 December 2008. <http://www.itil-itsm-world.com/servd.htm>

"Service Operation." 2007. ITIL & ITSM World. 5 December 2008. < http://www.itil-itsm-world.com/servo.htm>

"Service Strategy." 2007. ITIL & ITSM World. 5 December 2008. < http://www.itil-itsm-world.com/servs.htm>

"Service Transition." 2007. ITIL & ITSM World. 5 December 2008. < http://www.itil-itsm-world.com/servt.htm>

Turner, Mary Johnston. "ISO, ITIL and COBIT Triple Play Foster Optimal Security Management Execution." 2 April 2008. SC Magazine for IT Security Professionals. 19 November 2008. <http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/>

"What is ITIL." 23 September 2008. APM Group Ltd. 5 December 2008. <http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp>

"Version 3." 2007. ITIL & ITSM World. 5 December 2008. <http://www.itil-itsm-world.com/v3.htm>