

BADM 590 MS1

Trustworthy and IT security

COBIT Framework

Submitted By:

Ellan Imad Shtiwi: eshtiwi2@uiuc.edu

Submitted to:

Professor Mike Shaw

mjshaw@uiuc.edu



MS in Technology Management



University of Illinois at Urbana-Champaign

Abstract:

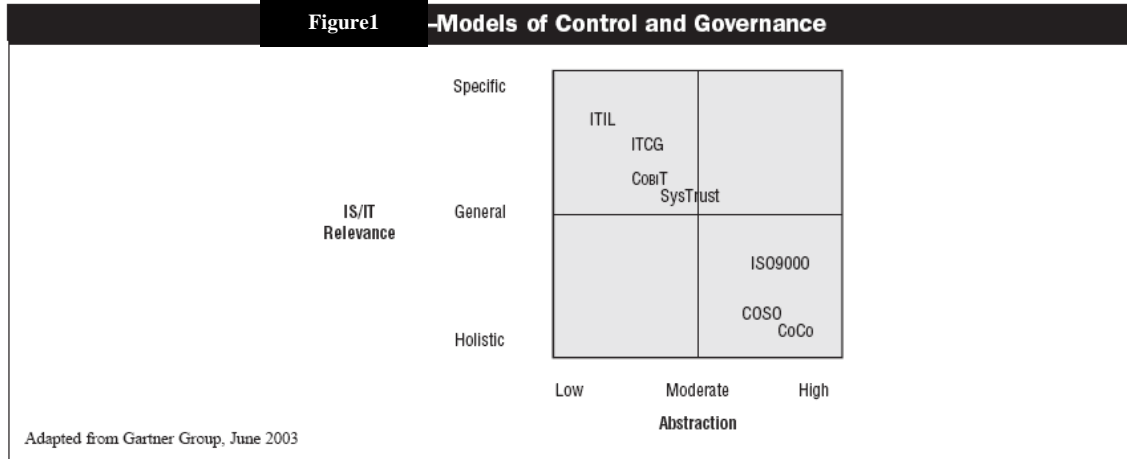
Information technology is an important factor in achieving success in the information economy and central to an entity's operational and financial management. As a result, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance, and provides assurance to critical issues. IT, long considered solely an enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

In my paper, I focused on COBIT which is a framework that aligns IT with business strategy for any company. In addition, I analyze a case study on how Sun Microsystems implemented COBIT? What were the barriers that they faced?

Review and Introduction:

In recent years, it has become very obvious that there is a need for a reference framework for developing and managing internal controls and appropriate levels of security in information technology (IT). IT Governance Institute had seen this need in the market and it started to develop a standard framework that can help companies to mitigate risks and have much more control on the technology they have. In addition, it is a way to align IT within the company overall strategy. COBIT (*Control Objectives for Information and related technology*) provides such a control and security framework for IT.

The relative between all frameworks used in the market and CoBIT are mapped in the below **figure1**. They include IT Infrastructure Library (ITIL), Information Technology Control Guidelines (ITCG), International Organization for Standardization's ISO9000, COSO report (a report on *Internal Control—An Integrated Framework*, sponsored by COSO) and Criteria of Control (CoCo), published by the CICA.



The main idea behind COBIT is to provide a clear policies and organized practices to maintain security and empower control over IT for worldwide professional organizations, governmental. This framework can complete the COSO perspective, which is a management and financial framework for internal control.

Therefore, after COBIT came to the market, it was used by a lot of companies and organizations. In the below figure you can see what CFO of Energy company thinks about COBIT.

What a Chief Finance Officer (CFO) of Energy Company Thinks of COBIT

A US energy company adopted COBIT in response to the Sarbanes-Oxley regulations. It had been looking for a structure, and instead of developing its own control framework, it preferred to adopt an internationally accepted framework—COBIT. The CFO, who is a member of the organization’s IT steering committee, stated: “The board of directors is responsible for our internal controls. They have authorized the board’s audit committee to make sure that we are doing our job. The audit committee has authorized the C-suite (CEO, CFO, COO, etc.) to make sure we are doing our job and the C-suite has asked this IT steering committee to make sure we have adequate internal controls for IT. The IT steering committee, in return, is asking the CIO and his management team to make us comfortable that this is so with regards to IT, and we are going to use COBIT to do it.”

The COBIT Framework

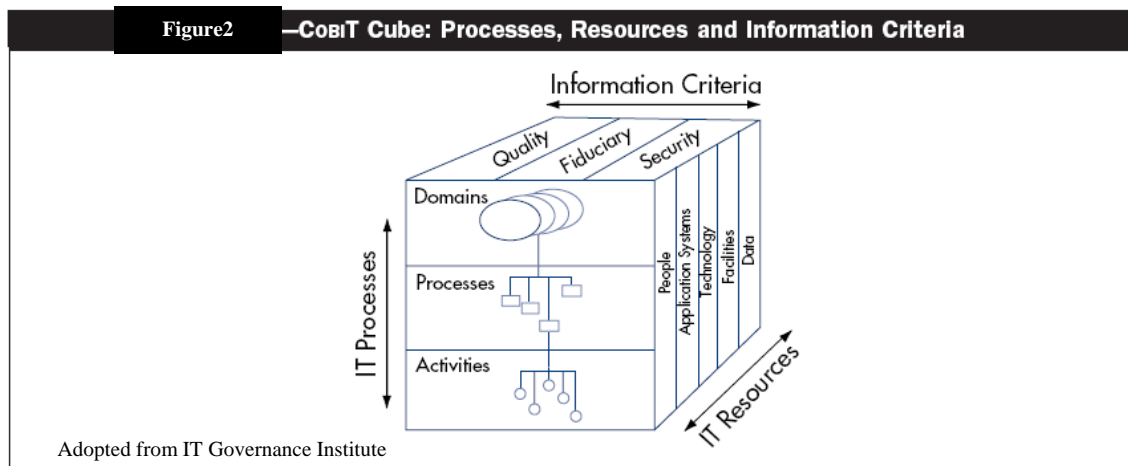
After taking a brief introduction what is COBIT, let us start drill down what is the components of this common framework. In addition, discuss a case study who Sun Microsystems implement it and what were the difficulties that faced Sun Microsystems' CIO.

CoBIT Audience: Management, Users and Auditors:

When IT Governance Institute came out with CoBIT; it designed it to be used by different audience:

- 1) Management: To help them align IT governance with the overall strategy. In addition, to help them balance risk and control the unpredictable IT environment.
- 2) Users: To assure the security on the customers' confidential information.
- 3) Auditors: To provide them with a guidelines or framework to help them to come to an opinion on the level of IT assurance.

CoBIT Framework Specifics:



By looking to **figure2**, we can understand the concept behind CoBIT; it divides into three dimensions. First, **Information Criteria**: To eliminate risk and improve control over your information; some of the following must be available: Effectiveness,

Efficiency, Confidentiality, Integrity, Availability, compliance and Reliability of information. Second, **IT Resources**: They are different tools that we have to use to mitigate risk: Data, Application Systems, Technology, Facilities and People. Third, **IT Processes**: They are well-organized steps divided into four different domains. Auditor must follow them to achieve business goals and information criteria: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (M). In addition, these four processes are divided into 34 different activities and tasks.

However, it is clear that the control measures over the IT processes will not necessarily satisfy all the different business requirements for information to the same degree. This is indicated by using primary (P), secondary (S) or blank indicators:

- **Primary**—The degree to which the defined control objective directly impacts the information criterion concerned
- **Secondary**—The degree to which the defined control objective satisfies only to a lesser extent or indirectly the information criterion concerned
- **Blank**—Could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, a particular control measure does not necessarily impact the whole different IT resource to the same degree. Therefore, CoBIT specifies which resource will be used or affected by this process. By looking to **figure3**, we can see the full picture of CoBIT framework.

Figure 3 CoBIT Summary Table

DOMAIN	PROCESS	Information Criteria						IT Resources						
		Ethicsness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Technology	Facilities	Data	
Plan and Organise	PO1	Define a strategic IT plan	P	S										
	PO2	Define the information architecture	P	S	S	S			✓	✓	✓	✓	✓	
	PO3	Determine technological direction	P	S					✓	✓	✓	✓	✓	
	PO4	Define the IT organisation and relationships	P	S					✓	✓	✓	✓	✓	
	PO5	Manage the IT investment	P	P				S	✓	✓	✓	✓	✓	
	PO6	Communicate management aims and direction	P				S		✓	✓	✓	✓	✓	
	PO7	Manage human resources	P	P					✓	✓	✓	✓	✓	
	PO8	Ensure compliance with external requirements	P				P	S	✓	✓	✓	✓	✓	
	PO9	Assess risks	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10	Manage projects	P	P					✓	✓	✓	✓	✓	
	PO11	Manage quality	P	P		P		S	✓	✓	✓	✓	✓	
Acquire and Implement	AI1	Identify automated solutions	P	S						✓	✓	✓	✓	
	AI2	Acquire and maintain application software	P	P		S	S	S		✓	✓	✓	✓	
	AI3	Acquire and maintain technology infrastructure	P	P		S				✓	✓	✓	✓	
	AI4	Develop and maintain procedures	P	P		S	S	S		✓	✓	✓	✓	
	AI5	Install and accredit systems	P			S	S			✓	✓	✓	✓	
	AI6	Manage changes	P	P		P	P	S		✓	✓	✓	✓	
Deliver and Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2	Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3	Manage performance and capacity	P	P		S				✓	✓	✓	✓	✓
	DS4	Ensure continuous service	P	S			P			✓	✓	✓	✓	✓
	DS5	Ensure systems security								✓	✓	✓	✓	✓
	DS6	Identify and allocate costs		P	P	S	S	S		✓	✓	✓	✓	✓
	DS7	Educate and train users	P	S				P		✓	✓	✓	✓	✓
	DS8	Assist and advise customers	P	P						✓	✓	✓	✓	✓
	DS9	Manage the configuration	P				S	S		✓	✓	✓	✓	✓
	DS10	Manage problems and incidents	P	P			S			✓	✓	✓	✓	✓
	DS11	Manage data				P		P					✓	✓
	DS12	Manage facilities				P	P					✓	✓	✓
	DS13	Manage operations	P	P		S	S			✓	✓	✓	✓	✓
Monitor and Evaluate	M1	Monitor the processes	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M4	Provide for independent audit	P	P	S	S	S	P	S	✓	✓	✓	✓	✓

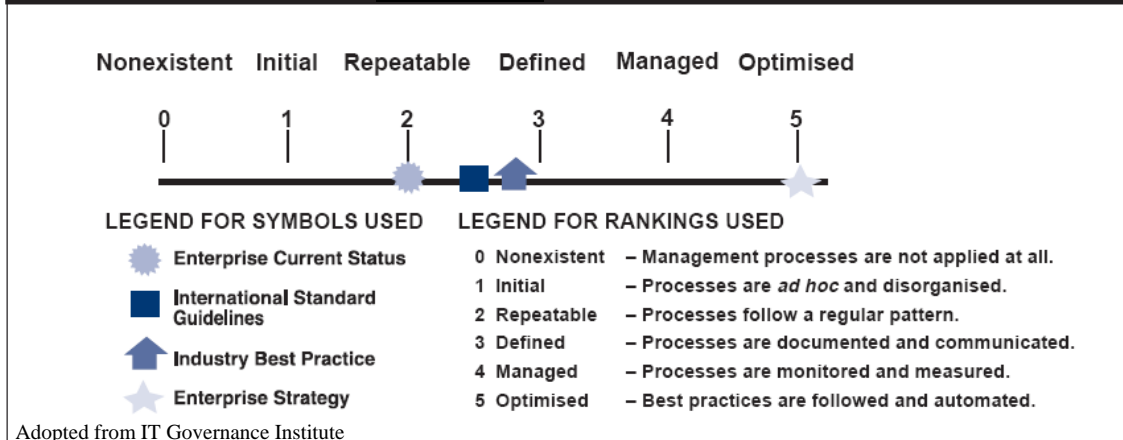
Adopted from IT Governance Institute

Audit and Management Guidelines:

In the last section, I already mention the audit guidelines which represent the IT processes that the auditor must follow it implement CoBIT on a specific company. Therefore, in this section I will mention the different management guidelines that will help them monitoring and improving the performance inside IT processes. The management tools include:

- **Maturity model:** It is a method for scoring or benchmarking a certain process or stage or even a company within the whole industry. In addition, it shows where the company should be to improve their performance. In **figure4** you can see who maturity model look like.

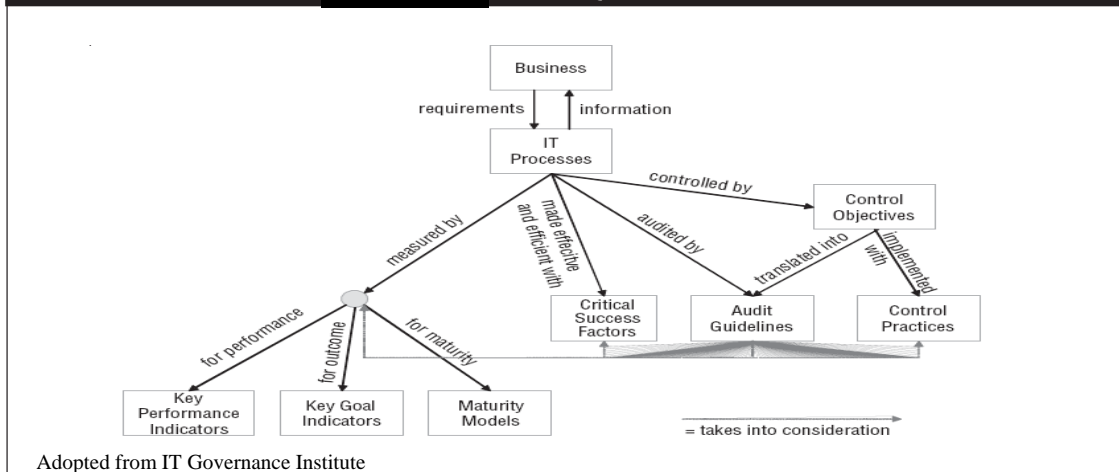
Figure4 -Maturity Model



- **Critical success factors (CSFs):** They define the most important factors that the senior management must implement to achieve control over IT processes. For example: The customers of a process and their expectations are known.
- **Key goal indicators (KGIs):** They tell management, after a while, if the goal of a specific IT process was achieved or not. For example: Achieving targeted ROI.
- **Key performance indicators (KPIs):** They define how well the IT process is performing in achieving the required goal. For example: Service availability and response time

Ones again, in the **figure5**, it combines the whole concepts in one picture.

Figure5 -CobIT Components Linked



Adopted from IT Governance Institute

COBIT and IT Governance Case Study:

In the second section; I will demonstrate how Sun Microsystems started thinking of using COBIT, what were the problems they faced and how they implemented the framework over the whole organization.

Sun Microsystems

ABSTRACT

With the increasing number of the employees to 30,000 plus which you can find them in 100 countries around the world, Sun Microsystems is a well-known hardware, software and services provider. On the other side, because of the demand of optimizing the IT value, Sarbanes-Oxley legislation (SOX), Sun's IT department searched the use of a common framework that will align the technology to its overall corporate strategy. After researching for a time, CIO suggested to use *Control Objectives for Information and related Technology* (COBIT) as a framework to mitigate risk and empower security and control over the IT department.

BACKGROUND

Since 1982, the beginning of singular vision __ The Network is the Computer__ Sun Microsystems had propelled its position as a leader provider of industrial hardware, software and services that make Internet work.

With 600 applications, six data centers, 1,700 data center servers, 600 terabytes of data, four million internal web pages and five million e-mails per day. Sun's information technology (IT) department global scope and scale includes supporting the Sun community saw a need for a framework to formulize the whole picture under the same roof.

Sun Microsystems' IT department was facing many issues in early 2004, including:

- The strong pressure that the company was facing from board's audit committee to find a quantifiable way to assure that the company was working on the right thing in the right way.
- Assuring the internal align of the internal control with the US Sarbanes-Oxley (SOX) Act of 2002 and let the every employee within the company to know the value of a broad internal control framework
- Making a difference between core vs. non-core activities, so the can outsource the non-core activities to third party and focus on it's core activities which will reduce costs
- They want to find a way to reevaluate the IT organization's internal structure and alignment to the corporate strategy to be sure all areas are covered without unwanted redundancy

Some IT staff saw the need of a common framework that will help the company to overcome the above concerns. In fact, the CIO had said that the organization would use *Control Objectives for Information and related Technology* (COBIT) as the framework. Sun's culture is built on innovation, and great value is perceived in contrarian thinking, so even though the CIO had approved the use of COBIT, actual implementation of the framework required an approach that built acceptance and adoption of the various elements of COBIT while taking into account the great process improvement work already being done in a significantly resource-constrained environment.

Simultaneously, the finance department expected to start its SOX reporting by the end of 2004. Sun's finance department was driving the SOX compliance effort, and IT was actively involved. As with most organizations, significant resources were being spent on the SOX compliance effort, and that effort continued even after learning that the first official reporting requirement had been pushed further back.

The following questions needed to be answered:

- How can Sun Microsystems make the awareness of the need of common framework for internal control within the IT people?
- How can we convince senior management the advantages of using common framework rather than making improvements on the existing methods?
- How should Sun identify and evaluate core vs. non-core IT activities?
- How should Sun assure the alignment of the organization's internal IT organizational rights?

PROCESS

Initially, there was limited support for COBIT from some IT executive. However, the CIO and the vice president for IT governance were supporting the framework, but there were good reasons why there was resistance from most of the other executives.

First, the company did not show why they had to use COBIT, what is COBIT and what are the values that COBIT can add to Sun Microsystems?

Second, just before 18 to 24 months, the company had significantly transformed the Sun IT organization, moving from a distributed approach with an IT group for each business unit to one unified Sun IT for one Sun. This facilitated the creation and institutionalization of common standardized processes. Sun embraced Sigma, the IT Infrastructure Library (ITIL) and other process improvement methods. Some questions asked were, "If the organization already knows what it needs to work on, and it follows industry best practices as it makes improvements, what does COBIT give it that it doesn't already have? Does COBIT replace ITIL?"

Even those who were encouraging of using COBIT showed concerns about the potential resource impact. Resources were already thin and limited, and the organization knew that there were no additional resources. Would the company have the necessary resources to implement COBIT?

On the other side, the executives were not sure of supporting COBIT, because the company had begun an intensive implementation of SOX 404 compliance and the expected requirement for the initial was June 2004.

One of the biggest problems was that the internal control framework was developed before the organization had a good understanding of COBIT in general and how COBIT applies to Sun IT specifically. At that moment, the control was just on the financial side, but the company saw that it can expand it beyond that, so if the adoption of COBIT continue the company can cover 22 processes with 194 controls. When those 194 controls are localized, the number grows to 1,114. The application controls cover approximately 125 applications with seven general categories of controls.

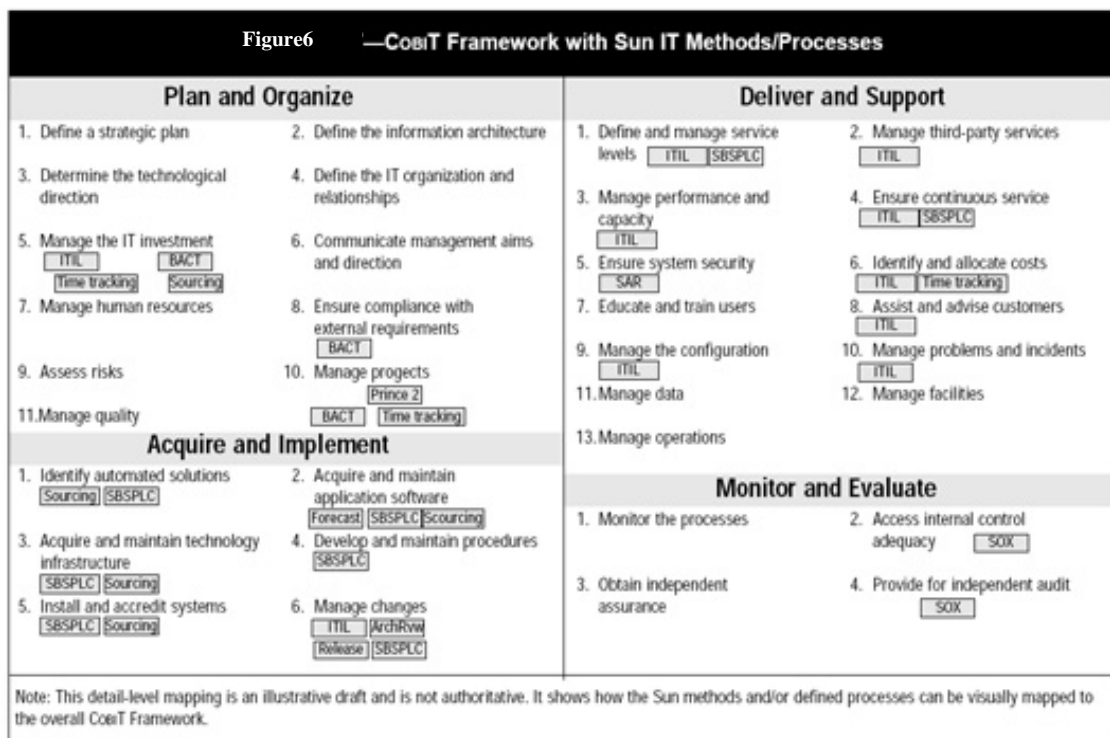
Those categories are:

1. Data security classification
2. System-granted access control
3. Role-based segregation of duties
4. Event-driven authorizations
5. Data validation
6. Interfaces
7. Batch processing

At the same time, the executive managers made decision to take a look over the IT activities that might be candidates for potential outsourcing. This was a great opportunity for CIO to reintroduce COBIT to the IT executives. Very quickly they saw the value of having a common framework that generically described what IT-related work is done in an organization. They decided to take an end-to-end look at the Sun IT processes and activities using the COBIT Management Guidelines and Control Objectives to ensure coverage of all processes. The most senior IT executives did these things by themselves, and the result was called the Sun IT/COBIT Activities Listing, which maps Sun IT processes and activities to COBIT.

Because this mapping was developed by the organization’s IT executives and senior management, it has proven very helpful in building acceptance and adoption of COBIT. Still, this did not eliminate concerns about resource constraints and the impact on ongoing process improvement efforts.

The way that an organization shows the linkage is overlaying its major process/activity names on a one-page representation of the COBIT framework. This has proven to be a powerful way to help people quickly see how COBIT is more inclusive and serves a different purpose than process improvement methods. **Figure6** is an example of this representation.



Consult with process owners to map their efforts to COBIT so that a common language is used across processes. For example, the organization has worked to help those working on enterprise architecture, portfolio management and strategic planning fit their work into the common framework and language.

CONCLUSION

Moving forward, Sun will continue with these future-thinking activities. The organization expects that by conducting compliance framework process assessments, it will further extend the acceptance and adoption of COBIT. By exposing all process owners to COBIT in a meaningful setting, the assessment will help them see the value of adopting elements of COBIT whether or not their process is added to the formal controls framework.

Implementing COBIT at Sun Microsystems has been possible because senior IT management was open-minded about using it in specific situations where the value was absolutely clear. Senior management's growing use and acceptance of COBIT is filtering throughout the organization and encouraging others to look at how COBIT's components can add value to their IT work.

At the end of this case, we can see that Sun Microsystems followed the Digital Liability Management (DLM) approach. They started with the support of the top management then wrote policies and procedures followed by reviewing the hardware and software. Therefore, the most important aspect when you want to implement security or empower the control within your IT department is executive managers not the software or the hardware technology.

Annotated Reference:

1. <http://www.itgi.org/>
2. <http://www.isaca.org/>
3. <http://www.ezcobit.com/UsingCobit/index.html>
4. <http://www.methodware.com/>
5. Presentation that was given by Protiviti's guest speakers.
6. www.protiviti.com
7. <http://www.sec.gov/news/press/2005-134.htm>