IT Governance

Minghai Geng

BADM 559 Term Project

December 15, 2008

Geng
BADM 559
12/15/08

Information Technology (IT) Governance is a broad and emerging topic that currently encompasses many factors. Simply, IT governance is the process of making decisions about IT investments. The emergence of IT governance came about from concern over the performance and management of risk for IT systems. Demand for IT governance increased due to increases in required regulations and degrees of compliance. Specifically, companies in the United States dealt with increased regulations from the introduction of the Sarbanes-Oxley Act. European companies meanwhile dealt with similar circumstances to their IT governance from the Basel II Accord. Additionally, IT governance emerged when companies realized IT projects could easily get out of control and significantly affect the performance and finances of their organization.

This report will provide a brief insight into IT governance and its components. It will cover frameworks that support the application and administration of IT governance. It will also look at how companies differ with their day-to-day activities with regards to IT governance. The main question I want to analyze is if there is a discernable difference in what companies from different backgrounds seek to gain out of IT governance. The two backgrounds I am looking at are companies from a consulting background and private industry firms. I will weigh this question with inputs and insights from a slew of esteemed professionals, specifically the speakers from Protiviti, Ernst & Young, Motorola, Monsanto, and State Farm. I seek to determine what IT governance means to them and what aspects they consider the most important.

Regulatory Acts

Sarbanes-Oxley

On July 30, 2002, the United States government enacted into law the Sarbanes-Oxley Act (SOX). Named after sponsors Senator Paul Sarbanes (D-MD) and House Representative Michael Oxley (R-OH), the act was a response to numerous and significant accounting scandals by large

corporations such as Enron, Adelphia, and WorldCom to name a few. This legislation established stricter standards for all publically traded U.S. companies. SOX increased the accountability for financial statements of company executives and established tougher criminal penalties for non-compliance.

11 titles make up the entirety of the Sarbanes-Oxley Act. Those titles covered numerous areas, from the creation of the Public Company Accounting Oversight Board (PCAOB) to auditor independence to corporate responsibility to a number of other things. Additionally, SOX established harsh civil and criminal penalties for firms, executives, and auditors who do not follow their guidelines or provide false certifications. Overall, SOX enabled accountability from corporate executives and established a proper method to maintain, audit, and report financial information.

Basel II Accord

What SOX is to U.S. companies, Basel II in a sense is to European firms. Published in June 2004, the Basel II Accord is recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. The Basel Committee, created in 1974 is an institution created by the governors of central banks in countries that are part of the Group of Ten. Called the Group of Ten, it is actually comprised of eleven nations; similar to how the Big Ten conference includes eleven schools. Those nations include Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States. The purpose of the Basel II Accord is to protect banks against financial and operational risks. This international standard provides guidelines on how much capital banking regulators should put aside for guarding against these risks. The intent is to protect international financial systems against bank collapses.

The Basel II Accord can be broken down into three segments. The first segment deal with three major risks banks face. Those risks are credit risk, operational risk, and market risk. We can calculate credit risk using a standardized approach, foundation internal rating-based approach (IRB), and/or advanced IRB. For operational risk, the three approaches are basic indicator approach, standardized approach, and advanced measurement approach. To figure out market risk, the best approach is simply value at risk (VaR). The second segment of Basel II has to do with the regulatory response to actions from the first segment. There is also a framework provided for dealing with systemic risk, pension risk, concentration risk, strategic risk, reputation risk, liquidity risk, and legal risk. The last segment increases the required amount of disclosures. This allows the market to have a better idea of overall risk position.

Frameworks

SOX Section 302[1]

An important framework is Section 302 of the Sarbanes-Oxley Act. Section 302 designs internal procedures that make sure financial disclosures are accurate. Specifically, the framework requires the employment and involvement of a "signing officer." The framework requires that the signing officer reviews periodic reports for untrue statements of a material fact and to make sure all reported financial information are fairly presented. Additionally, the signing officer is responsible for establishing and maintaining a suitable framework for internal controls, making internal controls known, evaluating internal control effectiveness, and presenting conclusions on the effectiveness of internal controls. What makes the framework suitable is freedom from bias, consistent measurements, completeness, and relevancy. Section 302 also requires additional

[1] Jones, Ronald. "The Sarbanes-Oxley Act of 2002." Securities Lawyer's Deskbook. 20 July 2002. <http://www.law.uc.edu/CCL/SOact/sec302.html>

disclosure for all significant deficiencies in the design or operation of those internal controls. Section 302 also required external auditors to issue an opinion on the maintenance of internal control over financial reporting in all material aspects. This is additional to the opinion on financial statement accuracy. The SEC removed this requirement in 2007.

ITIL

The Information Technology Infrastructure Library (ITIL) is a series of rules for managing IT infrastructure, development, and operations. The current version published in May 2007 is ITIL v3. Its core pronouncements include service strategy, service design, service transition, service operation, and continual service improvement.

Service strategy encourages the development of a best practice in a long term service strategy. It focuses on identifying opportunities to develop services that meet the requirements of internal or external customers. Service strategy covers general strategy, design strategy, competition and market space, implementation, service management as a strategic asset, financial management, service portfolio management, and maintenance and continual improvement of the service.

Service design makes sure the design of IT projects conforms to a best practice. It focuses on what activities help develop a strategy by designing a document to address all aspects of a service and propose related support activities. Key areas include architectural design, documentation, and future business requirements. Additionally, service design covers areas that include design packaging, catalog management, level management, capacity management, IT service continuity, information security, and supplier management.

Service transition involves the delivery of services into operational use. Specifically, they focus on implementation of service design activities. Service transition is more involved on the

side of projects rather than the business. Service transition covers the management of changes to the business environment, service asset and configuration management, release and deployment management, change management, and knowledge management.

Service operation covers the best practice for achieving delivery of services and cover activities required to operate and maintain a service. Considered is the monitoring of problems and balance between service reliability and cost. Other key issues involve balancing conflicting goals, event management, incident management, problem management, event fulfillment, asset management, technical and application management.

Continual service improvement involves aligning IT services to changing business needs. It involves identifying and implementing improvements to IT processes that serve business core strategies. It seeks to improve service quality, process effectiveness, efficiency, and cost effectiveness of IT processes.

COBIT

Control Objectives for Information and related Technology (COBIT) is a framework for IT that provides a set of generally accepted measures, indicators, processes, and practices to maximize the benefits derived from the use of IT. COBIT looks to develop appropriate IT governance and control in a company by aligning IT with the business, making sure they maximize benefits, use resources responsibly, and manage risks appropriately. First released in 1996, the latest edition is COBIT 4.1 released in May 2007. COBIT 4.1 has 34 high level processes that cover 210 control objectives. COBIT classifies those processes and objectives into four areas: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation.

COBIT's first area is planning and organization. This area covers how a company can use information and technology to help achieve their goals and objectives. This area spans 10 processes which include defining a strategic IT plan and direction, defining the information architecture, determining a technological direction, defining IT processes, managing IT investments, communicating management's direction, managing IT human resources, managing quality, assessing and managing IT risk, and managing projects.

COBIT's second area is acquisitions and implementation. This area involves identifying IT requirements in order to acquire and implement the right technology into a company and its core business processes. Additionally, this area addresses maintenance for their IT system and components. The processes covered are identifying automated solutions, acquiring and maintaining application software, acquiring and maintaining technology infrastructure, enabling operation and use, procuring IT resources, managing changes, and installing solutions and changes.

The third branch under COBIT's tree is delivery and support. This part focuses on the execution of applications, its results, and support processes that enable effective and efficient execution. Some support processes include security issues and training. The full list of processes are defining and managing service levels, managing third-party services, managing performance and capacity, ensuring continuous service, ensuring system security, identifying and allocating costs, educating and training users, managing service desk and incidents, managing configurations, managing problems, managing data, managing the physical environment, and managing operations.

The fourth leg on the COBIT animal is monitoring and evaluating. This area deals with a company's strategy in assessing needs and the effectiveness of their current IT systems in

meeting objectives with their design and with regulatory requirements. The shortest list of processes, monitoring and evaluating cover said actions for IT processes, internal control, ensuring regulatory compliance, and providing IT governance.

ISO/IEC 27001

Published in 2005, ISO/IEC 27001 is a standard of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This framework covers areas such as information technology, security techniques, and information security management systems. ISO/IEC 27001 certification involves a three phase audit process. The first step is a review of the existence and completeness of key documents such as a company's security policy, risk treatment plan, and statement of applicability. The second step is a detailed audit that tests the existence and effectiveness of information security controls stated in documents from step one. The third and final step involves reassessments to confirm that companies remain in compliance.

ISO/IEC 38500

The ISO/IEC 38500 framework, published in 2008, deals with corporate governance of information technology. This framework covers effective IT governance for the highest level of organizations. They confer to companies legal, regulatory, and ethical obligations related to their IT use. ISO/IEC 38500 contains three sections and six principles for good corporate governance of IT. The sections are scope, framework, and guidance. The principles include responsibility, strategy, acquisition, performance, conformance, and human behavior.

Geng
BADM 559
12/15/08
Consulting Firms

Protiviti[23]

Protiviti is a company that operates globally as a leader in risk consulting and independent internal audit services. Founded in 2002, they hired approximately 800 former Arthur Andersen employees as the foundation for their new company. Protiviti has a wide range of service offerings. Services related to IT include the following: CIO solutions, enterprise information management, IA technology/tool implementation, and IT audit services.

These services help Protiviti's clients identify, assess, and manage operational and technology-related risks. They also assist in implementing and monitoring IT projects.

- *Anil Harjani & Clint Fransen*

Protiviti on September 3, 2008 provided speakers Anil Harjani, IT internal audit and Clint Fransen, CIO solutions to speak about how IT governance applies to them. Anil's responsibilities involve IT general controls application reviews, information security risk assessments, technology change reviews, and IT SOX implementation. Clint's responsibilities include risk assessments, business impact analysis, disaster recovery and planning, pandemic planning, testing, and program audits.

Anil and Clint's involvement with IT governance center on IT controls. They state that IT controls improve IT operations, security, and audit performance. Focusing on specific IT controls can improve performance. Those control activities fall under six control groups. They are access controls, change controls, configuration controls, release controls, service level

[2] Harjani, Anil & Clint Fransen. "IT Governance & Controls." 3 Sept. 2008.

[3] Kula, Nicolas & Alex Goebel. "Intro to ITIL v3." 8 Oct. 2008.

controls, and resolution controls. To measure performance from these controls, Protiviti uses 25 measures that encompass operations, security, and audit.

Through their research, Anil and Clint determines there is a statistically significant relationship between the number of controls and improvements in performance. They find that ITIL and COBIT frameworks do improve performance, but that assertion is expected. Through use of Protiviti's 25 performance measurements, Anil and Clint determine that foundation controls confer the greatest positive impact. Accordingly, firms that use foundation controls have a higher performance level than firms who do not. Now that they determined the effectiveness of foundation controls, the top performing controls differ based on firm size. Controls that differentiate medium and low performers are activities that organizations use to build their controls systems. These activities include defining processes, roles, and service levels. On the other end, controls that differentiate top and medium performers are activities that sustain and continually improve controls systems. These activities encompass enforcing processes and consistent use of other controls to proactively stabilize the IT environment. Overall, their findings state top performers have a lower rate of unplanned work, better success rate, higher first fix rate, support more servers per system administrator, do more maintenance, and have better security sufficiency.

- *Nicholas Kula & Alex Goebel*

Protiviti also provided two other speakers on October 8, 2008 that spoke about their involvement and experiences regarding IT governance. They were Nicholas Kula, a manager in their CIO solutions department, and Alex Goebel, a senior consultant also in CIO solutions.

Giving an overview of ITIL, they state that early involvement in planning contributes to solving business challenges. ITIL reduces risks, reduces cost, and increases return on investment

(ROI). Additionally, use of the ITSM model helps companies adjust the quality of IT services and benefit from publically available models to avoid unnecessary duplication of work. Simply, ITSM helps companies deliver more value for less monetary investment. Some of the ITSM model's key benefits are reducing cost, improving quality and customer satisfaction, easier communications, and reducing problems and IT system downtime. The bottom line regarding ITIL and the ITSM model is that it provides a repeatable documenting process that is essential to improving IT service delivery and management.

Ernst & Young[4]

Ernst & Young (E&Y) is a worldwide organization many consider to be one of the largest professional services firms. E&Y is one of the Big Four accounting firms, along with Deloitte Touché Tohmatsu, KPMG, and PricewaterhouseCoopers. The company Ernst & Young resulted from a series of mergers, with the most recent being the merger of Ernst & Whinney with Arthur Young in 1989. However, components of the company have been in existence since 1849.

E&Y offers three main service segments. Those services are Assurance and Advisory Business Services (AABS), Tax Services, and Transaction Advisory Services (TAS). One of the departments within E&Y and listed under their AABS line is their Technology and Security Risk Services (TSRS) practice. On September 10, 2008, Richard Castle, an executive director in TSRS and Aileen Wright Bacon, a senior manager in TSRS spoke on what IT governance means to them and their company.

Richard and Aileen spoke about how there are increasing expectations of IT organizations. They mention that IT leaders must balance business and IT needs across IT and

[4] Castle, Richard & Aileen Bacon. "Ernst & Young – Advisory Services." 10 Sept. 2008.

business alignment, compliance and risk, and cost and effectiveness of delivery. IT and business alignment involves bringing IT in line with overall business strategy. Forming the foundation for effective IT alignment are direction, development, and delivery. Benefits of alignment include higher earnings per share (EPS), return on investment (ROI), revenue growth, return on assets (ROA), and return on equity (ROE). Richard and Aileen echoed the sentiment that business and technology alignment is synonymous with improved financial performance.

Private Industry Firms

Motorola[5]

Motorola is a multinational corporation which operates in the telecommunications industry. Motorola is a Fortune 100 company that currently employs around 66,000 people. Motorola designs, manufactures, and sells wireless telephones and other telecommunication related products.

Motorola was gracious enough to send Dean Haacker to speak on October 1, 2008. Being a private industry company, Motorola's IT governance involves their ITG system which provides a central electronic file repository for all business case information. This system breaks classification of business issues into a four step process. Those steps are high level business case, request review, detailed business case, and business case review. The first step, high level business case, involves translating business strategy and objectives into IT requests. After figuring out project dynamics, request review simply involves weighing costs and benefits of business cases for approval or rejection. Following this step, Motorola must establish a detailed business case. This step involves determining customer requirements, alternatives and recommended solutions, scope, and budget among other things. This phase in their project

[5] Haacker, Dean. "IT Portfolio Management and Governance." 1 Oct. 2008.

process determines business value to Motorola. The next and final step, business case review, once again involves reviewing parameters of business cases for approval or rejection. From this process, Motorola can determine which IT projects to pursue that will create value for the company. The ITG system helps Motorola determine proper allocation of project funding since less than 10% of IT budgets are discretionary while fewer than 12% of companies accurately measure the value of their IT investments. This process creates value by helping Motorola determine which projects to invest in with such a small amount of capital. The effects of this ITG system on Motorola results in improving spending efficiency and correspondingly improving return on investment (ROI).

Monsanto Company[6]

The Monsanto Company is a multinational agricultural biotechnology company founded in 1901. Employing approximately 18,000 employees, Monsanto is a leading global provider of technology-based tools and agricultural products that improve farm productivity and food quality. Their mission is to meet the world's growing food needs, conserve natural resources, and protect the environment.

On November 5, 2008, Mark Showers of Monsanto spoke to us about their approach to IT governance. His IT philosophy is build the right things the right way and to capture value through that. For that purpose, Mark emphasizes the need for business acumen and savvy, technical and architectural competence, and the ability to measure and articulate value. Monsanto's IT strategy involves a rolling 3-5 year cycle to match business dynamics. Monsanto divides their IT approach into two teams, the business IT team responsible for business driven strategy components and the enterprise architecture team responsible for functional strategy

[6] Showers, Mark. "IT Strategy Development and the CIO View of Project Management." 5 Nov. 2008.

components. IT fills a major role in Monsanto's R&D by meeting needs in phases along their pipeline.

State Farm[7]

State Farm is an insurance and financial services company founded in 1922. They are a Fortune 50 company who employ over 67,000 people across the United States and Canada, as well as over 17,000 agents and 390+ claim officers. State Farm utilizes 24 operation centers within 13 zones and has 335,000+ workstations.

State Farm provided Sam Howard on November 12, 2008 to speak about State Farm's approach towards IT governance. State Farm controls one of the world's largest private information networks, consisting of more than 40,000 circuits. Their network contains 25,000 servers and 4,500 terabytes of information, more than the Library of Congress. State Farm employs 5,800+ internal employees and 4,800+ external associates to work on just their information systems and 600+ active projects.

State Farm, through Sam views IT governance as a risk management approach that creates accountability and a direction for compliance. A challenge State Farm faces is getting over 10,000 people working on one of the largest networks in the world to follow common practices that support compliance goals. Thus, project, program, and portfolio management is very important to State Farm. Service management is also important to State Farm. It allows them to manage, maintain, and deliver stable and available IT services to their business partners. It ensures this process is running in an efficient and cost effective manner. Mr. Howard believes in linking IT projects to business capacities through service and portfolio management. Most

[7] Howard, Sam. "Service Management and IT Governance: As Easy as 1, 2, Pi." 12 Nov. 2008.

important, he believes that IT governance must be simple for easy adoption and avoiding delays and internal disliking.

Conclusion

While these firms do not focus on the same aspects of IT governance, the basics are there. They are focuses on IT controls, performance measurement, cost effectiveness, capital investment allocation, and strategy development. Frankly, with the term IT governance encompassing any decision making choices for the purposes of IT investments, the term is too broad for there to be significant similarities. The only discernable difference in IT governance strategy relates to their individual company business strategy, with consulting companies focused more on controls and generating a attractive ROI for their clients and private companies focused on cost, performance, and business capacities.