COBIT, ITIL AND ISO 27002 ALIGNMENTS FOR INFORMATION SECURITY GOVERNANCE IN MODERN ORGANISATIONS

A Case Study By Tanvir Orakzai, PhD, Singapore
Email:- tanvir_orakzai@yahoo.com

ABSTRACT

Over the years; there have been a number of methodologies and standards designed to help IT Governance and information security within modern organizations to achieve optimum process to achieve business objectives. Companies pursue the use of various mechanisms to ensure that their IT infrastructure is aligned with the objectives of the business and comply with local and global IT governance rules and regulations. Despite the vast amount of options available, there has been considerable confusion over the various methods used IT manager due to their lack of compressive information Governess approach. This paper proposes the comprehensive alignment of ITIL, COBIT and ISO/IEC 27002 that can be effectively used by any organization as a comprehensive solution to handle IT Governance and Information Technology Management in their organizations.

KEYWORDS

ITIL, COBIT, ISO- 27002, information security, IT Governance, Information Technology Management

INTRODUCTION

IT Governance is about It in the administration of the business is about giving back a ROI as aid to moneymaking business forms, or about the shirking of waste (and It without a business object is a waste of assets), or about the fulfilling of business administrative or consistence prerequisites. Starting here of perspective, the administration arranged approach to It essentially makes viable, business-turned influence simpler.

IT influence' is the in general and thorough supervision of organization It assets administration so that for better and productive and secure administrations incorporating keeping due respect for the investment of all stakeholders to keep benefit edges higher. This is vital, not for charitable explanations however since moguls wouldn't purchase experience an organization (or, rather, they'd demand in an extensive rebate) in the event that it wasn't run that way. The most ideal approach to do this is to guarantee the transparency of an organization's operations to speculators and different stakeholders, by supplying them with suitable and dependable data and this is one of the fundamental concerns of corporate influence, as well as the need to conform to pertinent laws and regulation.

In recent year organizations worldwide have utilized different Information administration strategies to conform to the nearby and worldwide regulations. The most broadly utilized regulation and skeletons are today are ISO 27002, COBIT and ITIL. Every guideline has its certain viewpoints however with certain restrictions. This paper intends to pool the positive purposes of ISO 27002, COBIT and ITIL an exhaustive way to propose an IT Governance structure that protects broader parts of data security administration for the cutting edge organization.

The proficient utilization of data innovation administration has been looked for after by numerous organizations; whereas a few organizations have attained the level of multifaceted nature needed by the utilization of these advances, securing a focused edge in the commercial centre. However the It administration regularly happens by accompanying one or two measures in confinement in light of the fact that It administrators uncover the mixture of regulation excessively intricate to accompany and actualize. The key explanation for why of this article is to address the use joined together systems ISOISO 27002, COBIT and ITIL as an instrument for It administration, recognizing that there are numerous confusions that are might be barely overcome by utilizing just a solitary system.

Successful IT management is essential for the smooth organization of operations incorporating administration of data security to keep its aggressive focal point in the business. These guidelines ought to be straightened to the destinations of the association to accomplish business objectives. In addition the profits, the utilization of It additionally postures incredible hazard to the association, where any mischance spill or consider break of delicate information can demolish an organization notoriety and debase it in the business sector. It is dependent upon the guides of the organization, how they viably they control the It holdings, plan arrangements and relieve the innate dangers.

It is an oversight to see It Governance absolutely a reaction to outside administrative weights, as this causes an at heart unsound mentality: legislation comes to be seen simply as an expense, an expense of working together, over which an organization have no control. Actually, IT Governance may as well guarantee that IT assets are sent and oversaw require viably, in the chase for business procedure. A definitive point of IT Governance is better, quicker, shabbier business. By the by, one part of this is the transparency that guarantees that all the stakeholders in a business can fulfil themselves that the business is constantly completed sincerely and morally, in light of a legitimate concern for the business.

From IT perspective Governance is about mitigating the risk of internal IT-assisted fraud, probably a far greater potential disaster to a company than the high profile risk of external hacking. The positive benefit from this transparency is that it can demonstrate the probity and reliability of a company to third parties: business partnerships will be easier to arrange (thus

enabling greater automation of inter-business processes or ‘straight through processing’) and that raising investment capital (from shareholders) should be easier.
A methodology used by some companies to manage its information technology is COBIT (Control Objectives for Information and Related Technology) developed by ISAC (Information Systems Audit and Control Association). Another widely used method is the ITIL (Information Technology Infrastructure Library) developed by the British Government that has an efficient structure and has been adopted and recognized worldwide as a standard for service management. While the COBIT and ITIL are guidelines, the ISO 27002 are widely used in IT operations to standardize security in organizations. We would be discussing it further in this paper.

ITIL, COBIT AND ISO 27002BACKGROUND

ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

ITIL or Information Technology Infrastructure Library is a library of good practices related to the services of Information Technology (IT). ITIL was developed in Britain in the late 1980´s by the Central Computer and Telecommunications Agency (CCTA)). ITIL provides a framework for good practices to guide the management of IT services. ITIL service strategy provides guidelines for the design development and implementation of service management and service strategy for modern organization. These guidelines empower the organization in relation to the principles that should underpin the management practices of the services.

The ITIL management service represents the development activities of internal and external suppliers, control of services and implementation of control strategies through their life cycle. These principles are extremely useful to develop policies to manage and control the lifecycle of ITIL services. The process of projects service includes the guidelines for design and development of services and processes related to IT management. These actions include the conversion process of strategic objectives which has already been defined in a portfolio of services.

ITIL transition services lists the requirements of service strategy, analyses the services project and effectuates this context into service operations, controlling the risks of failure and providing guidance about the requirements of the Service Strategy encoded in Service Design that are effectively carried out in the service operation, controlling the risks of a failure. This part of the ITIL framework combines practices in the management of the version, program management and risk management and places them in the context of the management services practice.

The Operation of Service incorporates the practices of servicing objectives in order to achieve effectiveness and efficiency in the delivery and support services to ensure a value for the customer and the service provider. Many organizations have been applying continuous improvement in their management processes, production, among others. Following this trend, the organizations have realized that the incremental improvement has had a large effect on service quality, operational efficiency and the continuity of services. ITIL last guidelines aim at continuous and consistent improvement.

COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY)

COBIT (Control Objectives for Information and related Technology) was created by ISACA (Information Systems Audit and Control Association) through the ITGI (IT Governance Institute). COBIT main objective is to provide good practice through a structured international standardization process of IT. COBIT identifies the key IT capabilities of an organisation and aligns IT to the business strategy, maximizing its benefits. COBIT focus is on following key areas: such as strategic alignment of business plan of the company, aligning IT with the company's operations, optimizing resource management to improve return on investment and efficient risk management to reduce significant risks to the company. All these factors form the fundamental of the COBIT.

ISO-27002

ISO 27002 corresponds to a series of guidelines and principles that intends to improve the management of information security in an organizations. The fundamentals of ISO 27001/27002 are listed below:-

- Information; Security Policy.
- Organizing Information Security
- Asset Management.
- Safety of Human Resources.
- Physical Security and the Environment.
- Operations and Communications Management.
- Access Control.
- Acquisition, Development and Maintenance of Information Systems.
- Information Security Incidents Management.
- Business Continuity Management.
- Compliance.

ITIL AND COBIT COMPARATIVE ANALYSIS

The difference within the ITIL methodology is the way the processes are described and treated with different activities. If there is an excellent cost-benefit ratio, it deals with the issues of implementing new technologies and guidance for the analysis of critical success factors. However, the critical success factors are better described and addressed by COBIT.COBIT is better structured to address issues related to IT auditing, being widely used and appropriate for this purpose.

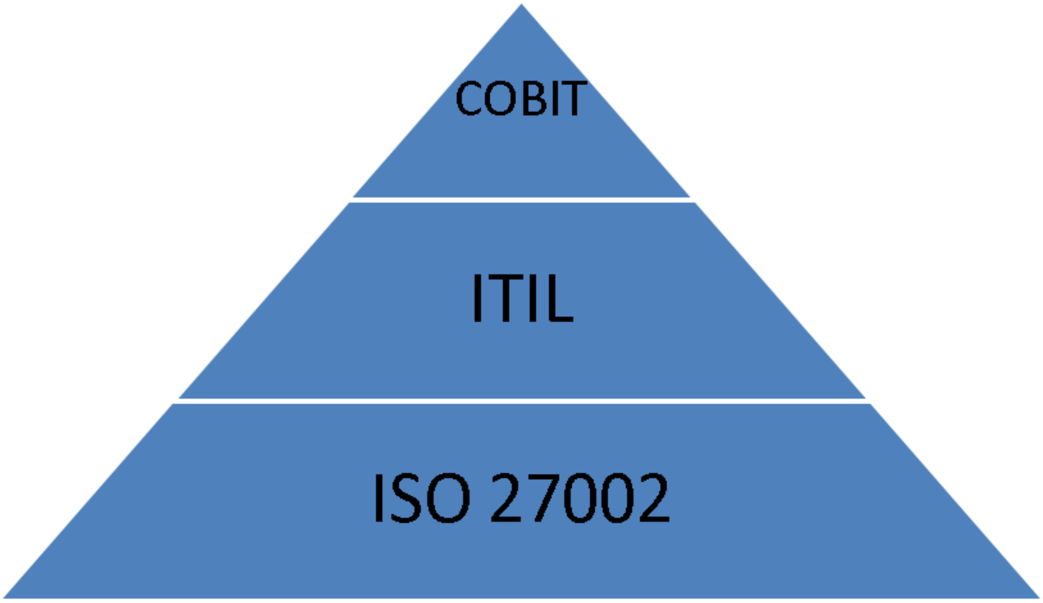
On the other hand, ITIL deals with incident management with a specific approach in its structure that has no equivalent section within the COBIT framework. ITIL handles this in a very comprehensive way and the levels of maintenance of service (SLA) including operating agreements (OLA) compared to COBIT.

The ISO/IEC 27002 standard is related to information security and not to IT management. With these general objectives, it is clear that the ISO/IEC 27002 needs a governance structure to rule over an organization context. Since ITIL and COBIT fall under the governance yet lacking the detail of ISO 27002, the alignment of ITIL and COBIT with ISO 27002 would be ideal to have a balanced approach to IT governance in modern organization.

ISO 27002 has a clear structure that can be applied and implemented completely on an organization with a guarantee of the overall safety of information security that is missing in ITIL and COBIT. The ISO- 27002 has features to preserve the confidentiality, integrity and availability of the information in organizations. Another point that may be compared with these methodologies is related to financial issues, as the ISO 27002 does not address this issue comprehensively. Financial risk and control is more related to general process that has to be set in place via ITIL and COBIT that provides a more active and effective risk management controls process.

As can be seen in the pyramid type figure below, the COBIT provides guidance for overall IT strategy, ITIL delivers details process alighting business objective with the IT, optimizing the resources and creating value for customers, while at lowest level is Information availability, assurance and integrity and minimizing the risks by successfully deployment of operations via ISO 27002.

Regardless of methodology, the goal of IT Governance is to improve an organization competitive advantage, optimize operation and mitigate risks. Often there is this flawed philosophy among IT professionals that IT role in a company is setting up laptops and printers and stopping access to information. In a way most IT departments are lame duck with security guard kind of mentality living in a mistaken belief that IT is just operation and does not need to be aligned with company's business goals. The truth is IT Governance is an integral part of a modern company that must be lean, mean and must compliment business goal in measurable way. Given this perspective it is vital to understand and measure the use of IT in organizations is a more plausible manner via IT indicators that should be aligned with strategic indicators to govern the organization.



CONCLUSION

Good IT governance doesn’t exist in a vacuum. Unless IT Governance practices are institutionalized as part of a formal process that is regularly assessed and updated in the light of changes to the business or technology, nothing will work. Regardless of methodology, the goal of IT Governance is to improve an organization competitive advantage, optimize operation and mitigate risks. Often there is this flawed thinking among IT professionals that IT role in a company is setting up laptops and printers and stopping access to information. In a way most IT departments are lame duck with security guard kind of mentality living in a mistaken belief that IT is just operation and does not need to be aligned with company’s business goals. The truth is that IT Governance is an integral part of a modern organization that must be lean, mean and must compliment business goal in measurable way.

From the above discussion; the proposed suggestion is that ITIL methodology should be used to define the strategies, concepts and processes; COBIT should be used to evaluate the critical success factors and ISO/IEC 27002 standard should guide the IT in relation to issues of IT management and security.

REFERENCES

1) BRENNER, Michael et al. Towards an Information Model for ITIL and ISO/IEC 20000 processes. IEEE Computer Society and Information Engineering. 2009.

2) CHASE, Richard B.; JACOBS, F. Robert; AQUILANO, Nicholas. Administração da Produção para a Vantagem,Competitiva. 10. ed. Porto Alegre: Bookman, 2006.

3) IT GOVERNANCE. Global Status Report. [2008]. Available at: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=50272&TEMPLATE=/ContentManageme nt/ContentDisplay.cfm>. Accessed: May, 30, 2013.

4) ITGTI - IT GOVERNANCE INSTITUTE. Board Briefing On It Governance. 2. ed. 2008. Available at:<http://www.itgi.org/AMTemplate.cfm?Section=Board_Briefing_on_IT_Governance&Template=/ContentMan agement/ContentDisplay.cfm&ContentID=39649>. Accessoem: April, 18., 2013.

5) ITGTI - IT GOVERNANCE INSTITUTE. COBIT 4.1. Ilinois: IT Governance Institute, 2007.

6) NABIOLLAHI, Akbar; SAHIBUDDIN, Shamsul Bin. Considering Service Strategy in ITIL V3 as a Framework for IT Governance. 2008

7) RIDLEY, Gail; YOUNG, Judy; CARROLL, Peter. COBIT and its Utilization: A framework from the literature. IEEE Transactions on Systems, Man and Cybernetics. Part B, Cybernetics, United States, Jan. [2004].

8) SAINT-GERMAIN, Rene. Information Security Management Best Practice Based on ISO/IEC 17799. The Information Management Journal, v.25, n.1, Jul./Aug. 2005.

9) SIMONSSON, Marten; JOHNSON, Pontus. The IT organization modelling and assessment tool: Correlating IT governance maturity with the effect of IT. IEEE Transactions on Systems, Man and Cybernetics. Part B, Cybernetics, United States. 2008.

10) ZHANG, Shaohua et al. ITIL Process Integration in the Context of Organization Environment. IEEE Computer Society and Information Engineering, United States. [2009]. Available at: < http://www2.computer.org/portal/web/csdl/doi/10.1109/CSIE.2009.691> . Accessed: July, 3, 2013.