Research Journal of Applied Sciences, Engineering and Technology 7(23): 4906-4909, 2014
DOI:10.19026/rjaset.7.881
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 09, 2013 Accepted: January 10, 2014 Published: June 20, 2014

Research Article

Bridging Gape between ITSM, IT-governance and Information Security to Meet Business Needs

[1]Akhtar Ali and [2]Tariq Rahim Soomro
[1]Department of IT, SZABIST Dubai Campus, United Arab Emirates (UAE)
[2]Department of Computer Science, Sindh Madressatul Islam University, Karachi, Sindh, Pakistan

Abstract: To achieve organizational and business specific goals, IT plays a very important and crucial role. IT Services Management increases the efficiency of the IT Department to provide standardized and effective services to the organization stakeholders and it leads to a better IT Governance for the organization. IT Governance helps the organization to achieve its goals with the help of acclaimed best IT practices in the industry. This and explores how mapping of Information Technology Service Management (ITSM), IT Governance and Information Security helps to meet organization and business specific goals and needs.

Keywords: COBIT, ISO, IT governance, ITIL, MOF

INTRODUCTION

The IT Service Management (ITSM) is defining as the implementation and management of quality IT services that fulfil the needs of the business (John, 2004). ITSM focuses on the alignment of IT services with business objectives and trying to improve the performance of entire business organization. In the current competitive business environment, ITSM is the key to the development of any Business. ITSM provide high level service and support to organization. ITSM increase the customer satisfaction which ultimately valued to the business. ITSM focus on over the years, different types of ITSM frameworks, for example, Information Technology Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF), have been proposed and developed for the implementation of IT service management. No doubt each framework has its own characteristics and limitation. ITSM like ITIL and MOF are powerful frameworks to support the delivery of IT-services and COBIT is a use for IT governance, Control and IT audit. But security issues are more important for products as well a service, where a combination of ITSM (ITIL, MOF) and ISO 27002 will provide a strong toolkit to enable delivery of high quality IT-services.

ITIL and MOF are the collection of best practices for the management of IT services. ITIL helps organizations to become aware of the business value of their IT services provide to internal and external stakeholders. ISO/IEC 27001 is a set of guidelines, which can be used by an organization to design, deploy and maintain Information Security Management System (Razieh and Nasser, 2012). COBIT is a high-level IT governance and management framework. It focuses on the broader decisions in IT management and does not dwell into technical details. It is a framework of best practices in managing resources, infrastructure, processes, responsibilities and controls (Varun, 2008). IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. At the same time we need better IT services, good IT governance and security of information. This and explores that how ITIL and MOF align and integrate with COBIT and ISO/IEC 27001 to meet the business challenges we face in today's critical IT environment.

MATERIALS AND METHODS

It service management: Information Technology Infrastructure Library (ITIL) is one of the most famous frame work use for the implementation of IT service management globally and currently owned by UK Office of Government Commerce (OGC). The main disciplines of ITIL (e.g., Service support and Delivery) are Service Level Management, Financial Management, Capacity Management, Continuity and Availability Management, Incident Management, Problem Management, Change Management, Configuration Management, Release Management and the Service Desk function. ITIL help the organization to improve their IT service management, satisfy the customers and ultimately increase the businesses. Quality IT service management is achievable only with the help of ITIL (Alison *et al*., 2007; Jack *et al*., 2007). MOF illustrates

Corresponding Author: Tariq Rahim Soomro, Department of Computer Science, Sindh Madressatul Islam University, Karachi, Sindh, Pakistan

proven team structures and operational processes and implement best Information Technology (IT) practices to improve the capability and quality of IT operations (David *et al*., 2008). MOF is a collection of best practices, principles and models that provide comprehensive technical guidance for achieving mission critical production system reliability, availability, supportability and manageability for solutions and services built on Microsoft products and technologies (Jan *et al*., 2009). MOF provides the fundamentals of operations methodology and a framework for IT operations.

It governance: IT Governance is defined as "an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives". It is the alignment of organizations IT strategy with business strategy, ensuring that companies remains on proper track in order to achieve their strategies and goals and employing best ways to measure IT performance. There are five major focus area that make IT governance are, Strategic alignment, value delivery, resource management, risk management and performance management. Numbers of framework available for the implementation of IT governance, among them are COBIT and ISO 27002 (Craig, 2005; Efrim Boritz, 2007; Bryn, 2008).

COBIT stands for “Control Objectives for Information and Related Technology”, is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. Information Systems Audit and Control Association (ISACA) is the founder for the COBIT framework, which is use for Information Technology (IT) Management and IT governance. The COBIT is the most famous IT governance framework available nowadays. It must be the first choice for the implementation of IT governance in any organization. The latest edition of ISACA's that is globally accepted framework is COBIT5. It provides business view of the governance of Enterprise IT that shows the central role of IT in creating value for enterprise. The COBIT is based on four domains Publish in 6 different publications. For each domain, sub domain has been defined to describe requirements and tools to monitor the IT-process. The COBIT domains cover (John, 2004; Anthony, 2012):

- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring

The ISO 27002 standard is the new name of the ISO 17799 standard and is international standard organization code of practice for information security. ISO 27002 is the enhanced version of ISO 17799. The goal of ISO/IEC 27002 has been to provide information to the parities responsible for the implementation of information security within the organization. ISO 27002 provides Security standards for different IT Services. The standard "established guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organization". It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships. According to ISO "Information Security governance has become an Established and recognized component of Corporate Governance and specifically Information Technology governance". This standard is a globally accepted code of practice for information security management. It is controls based standard for organizations to manage their information security according to thirteen domains The ISO 27002 contents sections are:

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance

ISO 27002 defines information as an asset that may exist in many forms and has value to an organization. The goal of information security is to properly protect this asset and to ensure business continuity, decrease business damage and increase return on investments that is done in the business. As defined by ISO 27002, information security is explained as the preservation of (John, 2004; Daminda, 2008).

Confidentiality: This is to Ensuring that information is accessible only to those authorized and have rights to access it.

Integrity: This is to ensure that information is accurate and no one has to modify it and safe guarding the accuracy and completeness of information and processing methods.

Availability: This is to ensure that authorized users have access to information and associated Assets when needed.

Table 1: ITSM and IT governance matrix

	IT governance frameworks	
ITSM frameworks	COBIT	ISO 27002
ITIL	1.1	1.2
MOF	2.1	2.2

Table 2: ITL alignment with COBIT and ISO 27002

ITIL	COBIT	ISO 27002
ITIL (service support)		
Service desk	DSS02 manage service request and incident AP011 manage quality	6.3.2 reporting security weakness
Incident management	DSS02 manage problems and incidents	13.2.1 establish incident response responsibilities and procedures
Problem management	DSS04 manage problems	13.2.1 establish incident response responsibilities and procedures
Configuration management	BAI010 manage configuration	
Change management	BAI06 manages changes	10.5.1 change control procedures 8.2.1 operational change control
Release management	BAI06 manages changes	10.4.1 control of operational software 10.5.2 technical review of operating system changes release
ITIL (service delivery)		
Service level agreement	APO09 manage service agreements	4.2.2 security requirements for third party contracts 10.2.1 manage third party service agreements
Financial management	APO006 manage budget and cost	
Continuity management	DSS04 manage continuity	14 business continuity management
Capacity management	BAI04 manage availability and capacity	8.2.1 capacity planning
Availability management	BAI04 manage availability and capacity	8.5.1 network control 9.5.5 use of system utilities

Table 3: MOF alignment with COBIT and ISO 27002

MOF	COBIT	ISO 27002
Support	DSS03 manage problems DSS02 manage service request and incident	6.3.2 reporting security weakness
Release	BAI06 manage changes BA103 manage the configuration BA1010 manage assets	10.5.1 change control procedures 8.2.1 operational change control 10.4.1 control of operational software 10.5.2 technical review of operating system changes release
Service	AP009 manage service agreements DSS02 manage service request and incident AP011 manage quality	4.2.2 security requirements for third party contracts 10.2.1 manage third party service agreements
Infrastructure	BAI104 manage availability and capacity AP006 manage budget and cost	8.2.1 capacity planning
Operations	DSS01 manage operation	8.5.1 network control 8.7.4 security of electronics mails 9.5.5 use of system utilities 12.1.7.3 quality and completeness of evidence
Security	APO13 manage security DSS05 manage security service	10.6.1 establish network security controls
Partner	APO10 manage suppliers APO08 manage relationship	

Why to align ITSM, IT governance and information security standard: ITIL and MOF are for IT Management, COBIT is for IT-audit and control and ISO 27002 is for security Management. As different framework and standards evolved, they create confusion specially when using either one of them. When taking a closer look to them, it is very much clear that they successfully can be aligned. To implement a process to deliver IT-services without properly defining measures for monitoring the process will lead to a higher risk and it will not be more efficient and effective. This is one argument to align ITIL with COBIT. Also it is much clear that security is a major concern nowadays, so for any process of ITIL or MOF there must be ISO security standard implementation, Table 1.

RESULTS AND DISCUSSION

Mapping of ITSM, IT governance and IT security: Table 2 will describe the ITIL alignment with COBIT and ISO 27002 and Table 3 will describe MOF alignment with COBIT and ISO 27002 (John, 2004; Robert, 2012; Rene, 2005).

CONCLUSION

In every organization, it is must to deliver IT services in a cost efficient manner, mitigating security risks and comply with legal requirements. The equation is difficult to handle and in some cases it seems like a mission impossible. To be able to survive in this environment a Combination of ITIL or MOF, COBIT and ISO 27002 can be valuable for organization. Organization may use ITIL and MOF to define processes, use COBIT IT audit, benchmarks IT governance and use ISO 27002 to address security issues to mitigate possible risks. It will lead to a better IT service management with a strong IT governance and secured information in the organization.

REFERENCES

Alison, C., H.C. Ashley and R. Stuart, 2007. An Introductory Overview of ITIL® V3. London, ISBN: 0-9551245-8-1, pp: 7-40.

Anthony, N., 2012. Migrating to COBIT5. SIFMA, America, pp: 10: 26.

Bryn, P., 2008. IT governance for CEOs and members of the board. ISACA J., 1: 34-87.

Craig, S., 2005. IT Governance Framework Structures, Processes and Communication. Forrester Research Inc., pp: 2-16.

Daminda, P., 2008. ISO/IEC 27001 Information Security Management System. ISO 27001 Family, pp: 2-21.

David, P., H. Clare and L. Paul, 2008. Microsoft Operations Framework 4.0. ISBN: 9789087532 871, pp: 115-142.

Efrim Boritz, J., 2007. The necessity of good It governance, organization and leadership. University of Waterloo, pp: 3-11.

Jack, D.B., S. Ulrike and B. Peter, 2007. IT Service Management/Governance: Case Study of ITIL/COBIT Frameworks in Three SME. Van Haren Publishing, ISBN: 9080671347, pp: 1-15.

Jan, V.B., Inform-IT and D. Jerry, 2009. Cross-reference ITIL V3 and MOF 4.0. Alignment White Paper, pp: 3-30.

John, W., 2004. Combining ITIL with COBIT and 17799. Scillani Information AB, pp: 1-6.

Razieh, S. and M. Nasser, 2012. A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian J. Sci. Technol., 5(2).

Rene, S.G., 2005. Information security management best practice based on ISO/IEC 17799. Inform. Manage. J., 39(4): 1-6.

Robert, E.S., 2012. COBIT5 Simplified Complex Standard. ISACA Publication, pp: 12-37.

Varun, A., 2008. Comparing different information security standards: COBIT vs. ISO 27001. Carnegie Mellon University, Qatar.