Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework

Syed Mubashir Ali
Department of Computing
Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, SZABIST
Dubai, United Arab Emirates

Tariq Rahim Soomro
College of Engineering & IT
Al-Ain University of Science & Technology
Al-Ain, United Arab Emirates

Abstract

The use of information technology (IT) has risen exponentially over the past few decades and has become a necessity for enterprises. Organizations are realizing that IT resources are important strategic organizational asset. This rapid increase in the use of IT has urged organizations into implementing IT standards. There are a number of IT standards and technology frameworks which are supporting organization independently. Information technology infrastructure library (ITIL) is the de-facto IT management framework and one of the most widely used IT standards. Although, ITIL is a comprehensive IT framework but lacks information security management which needs to be catered for effective IT service management. This study will discuss some of the information security standards and the essential controls of information security and propose a modified ITIL framework that will incorporate all the essential controls of information security within ITIL.

Keywords: Information Security, ITIL, ISO/IEC 27002, Technology Framework

1. Introduction

Over the past few years, the increase in the use of technology and the rise in interconnected systems and networked environment, data and information have made the enterprises to implement IT service management standards in order to provide better IT services to their users and clients in order to better support their strategic organizational goals. At the same time, the increased use of technology is now being exposed to a rising number of threats and vulnerabilities. Therefore, it has become a necessity for an organization to have an efficient information security management system. Many service oriented organizations with confidential and sensitive information are moving towards implementing information security standards based on best practices as guidance on how to manage their information security infrastructures and the information residing within their organization.

Compliance with information security standards and best practices can ensure that the organizations' information is secured competently and also helps in reducing and/or avoiding systems and service downtime. There are quite a lot of information security frameworks and best practices that have been developed over the time and are being modified and improved with experience and research by information security practitioners and academic researchers. But implementing multiple technology standards and framework increases complexity and it becomes very difficult to perform business process re-engineering to comply with the requirements of each technology standard to be implemented. (Ali, Soomro, & Brohi, 2013).

This study will propose the framework for ITIL that will include the processes and characteristics from the known security standards and best practices and will provide a comprehensive Information Technology framework that will include the IT Service Management along with IT and Information Security. This proposed ITIL framework will not only improve ITIL but will help organizations to implement a single IT standard for both their IT service management and Information security needs. Section 2 will give a brief overview of some of the globally accepted and used information security frameworks. Section 3 will provide the details about the components and processes of ITIL 2011 framework.

Section 4 will introduce the essential information security controls and maps them to ITIL processes. Section 5 will propose a modified ITIL framework that will integrate all the essential controls and the last part will conclude the findings of this study.

2. Information Security Standards

In this era of information technology, information Security is a major concern for IT professionals. Several technology frameworks exists to help enterprises evaluate their security breaches, employ suitable security controls and act in accordance with governance requirements and confidentiality with information security policies and regulations. (Soomro & Hesson, 2012)

2.1 ISO/IEC 27002

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) form the specialized associations for global standardization. (Sweren, 2006) They jointly published the standard and framework for information security management ISO/IEC 20072. (Năstase,et-al. 2009) The foundation of the standard was initially a document published in 1995 by the government of UK and was again published as BS 7799 by British Standard Institute (BSI). It was again published in 2000 by ISO as ISO 17799. In 2005, a new version appeared along with a new publication, ISO 27001. The two documents are proposed to be used together, with one complimenting the other. (Introduction to ISO 27002).

2.2 COBIT

Control Objectives for Information and Related Technology (COBIT) is a framework of best control practices formulated and maintained by Information Technology Governance Institute (IGTI) , the organization that comes under ISACA (previously known as Information Systems Audit and Control Association) (About ISACA, ; Tuttle & Vandervelde, 2007) for Information Technology (IT) management and IT governance. COBIT splits IT control and governance into 34 processes, and provides a high level Control Objective (CO) for each of these 34 processes. (Von Solms, 2005; Ridley, Young, & Carroll, 2004. It acts as a set of tools that assist executive managers to bridge the gap between control requirements, technical problems and enterprise risks. (Cobit 4.1)

2.3 PCIDSS

PCI DSS or Payment Card Industry Data Security Standard is a standard for information security developed by PCI Security Standards Council which is used globally as a de-facto security framework for financial institutions. (PCI Security Standards) It consists of policies and processes that intend to maintain and improve the security of debit/credit and other electronic card transactions and guard cardholders' data against abuse and fraud. It was developed to enable broad adoption of same and consistent data security methods globally. (Akowuah, et-al, 2012)

2.4 HITRUST CSF

In 2009, The Health Information Trust Alliance (HITRUST) in collaboration with healthcare, Information technology and information security experts developed a Common Security Framework (CSF). (Common Security Framework) It is a framework that provides enterprises especially within the healthcare industry with the required organization, detail and transparency related to information security. (Common Security Framework; ITIL Process Map) Organizations that generate, store or ex-change important health and financial information can use CSF which is the first IT security standard developed explicitly for healthcare data and information. (Common Security Framework)

3. Current ITIL Framework

ITIL has evolved since its first version based on the recommendations from experienced IT professionals and academic researchers who are constantly thriving to improve and standardize the information technology processes worldwide. The current ITIL framework is ITIL 2011 which is composed of the following processes: (ITIL Process Map)

3.1 Service Strategy (SS)

- Strategy Management for IT Services
- Service Portfolio Management
- Demand Management
- Financial Management for IT Services

- Business Relationship Management

3.2 Service Design (SD)

- Design Coordination
- Service Catalogue Management
- Service Level Management
- Risk Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Compliance Management
- Architecture Management
- Supplier Management

3.3 Service Transition (ST)

- Change Management
- Change Evaluation
- Project Management (Transition Planning and Support)
- Application Development
- Release and Deployment Management
- Service Validation and Testing
- Service Asset and Configuration Management
- Knowledge Management

3.4 Service Operation (SO)

- Event Management
- Incident Management
- Request Fulfillment
- Access Management
- Problem Management
- IT Operations Control
- Facilities Management
- Application Management
- Technical Management

3.5 Continual Service Improvement (CSI)

- Service Review
- Process Evaluation
- Definition of CSI Initiatives
- Monitoring of CSI Initiatives

4. Information Security Essential Controls and ITIL

According to (Susanto, Almunawar, & Tuan, 2011), there are 11 essential controls (EC) that need to be the part any technology framework being implemented by any organization in order to have effective information security management. These ECs cover all areas within information security and are as follows:

1. Information Security Policy
2. Communications and Operations Management
3. Access Control
4. Information System Acquisition, Development and Maintenance
5. Organization of Information Security
6. Asset Management
7. Information Security Incident Management
8. Business Continuity Management
9. Human Resources Security

10. Physical and Environmental Security
11. Compliance

Current ITIL framework contains information security management within its Service Design Process. These cover the basic aspects of information security and deal on a level of abstraction. We would first see which of the 11 ECs are already there within existing ITIL processes and then later will propose a modified ITIL framework that will accommodate all the ECs of information security by integrating the processes of other information security standards.

From table 1, it is evident that there are some ECs which are not available in ITIL processes. Therefore, the authors are proposing a framework that will include the missing ECs of information security by integrating the processes from ISO 27002 and PCI DSS into ITIL processes. We will now briefly explain the three ECs of Information Security that are missing in ITIL and later propose the modified framework.

4.1 Information System Acquisition, Development and Maintenance

This EC is an integrated process that describes limitations and technicality of information systems. It begins with the acquisition, then development / deployment and in the end the maintenance and continuance of information systems.

4.2 Human Resources Security

This EC defines the process to make sure that all employees (including clients and / or user of sensitive and confidential information) are competent enough and realize their duties and responsibilities and that their access to the company's information is removed once they leave the organization at the end of their employment.

4.3 Physical and Environmental Security

This EC is about how to take essential measures for safeguarding and protection of the systems, buildings and premise, and the physical infrastructure against threats associated with the physical environment (i.e. fire, flood / natural disasters) in order to avoid damage or unauthorized access to data and information and the systems that underpins them. (Susanto, Almunawar, & Tuan, 2011)

5. Proposed ITIL Framework

The authors have proposed a modified ITIL framework (Figure 1.) based on the 11 ECs that will include all the ECs of information security thus improving ITIL in a way that will help organizations in implementing effective IT service management along with ensuring information and data security.

6. Conclusion

ITIL has been evolving since its inception based on the recommendations and suggestions by experienced technology professionals and academic researchers. This study introduced the common information security frameworks and the information security essential controls and then integrated them into existing ITIL processes and proposed a modified ITIL framework which will improve information and technology infrastructure security that will result in better IT service management. This study focused only on the essential controls of information security based on ISO/IEC 27002, but future research can be done on how to incorporate other information security processes into ITIL.

7. Figures and Tables

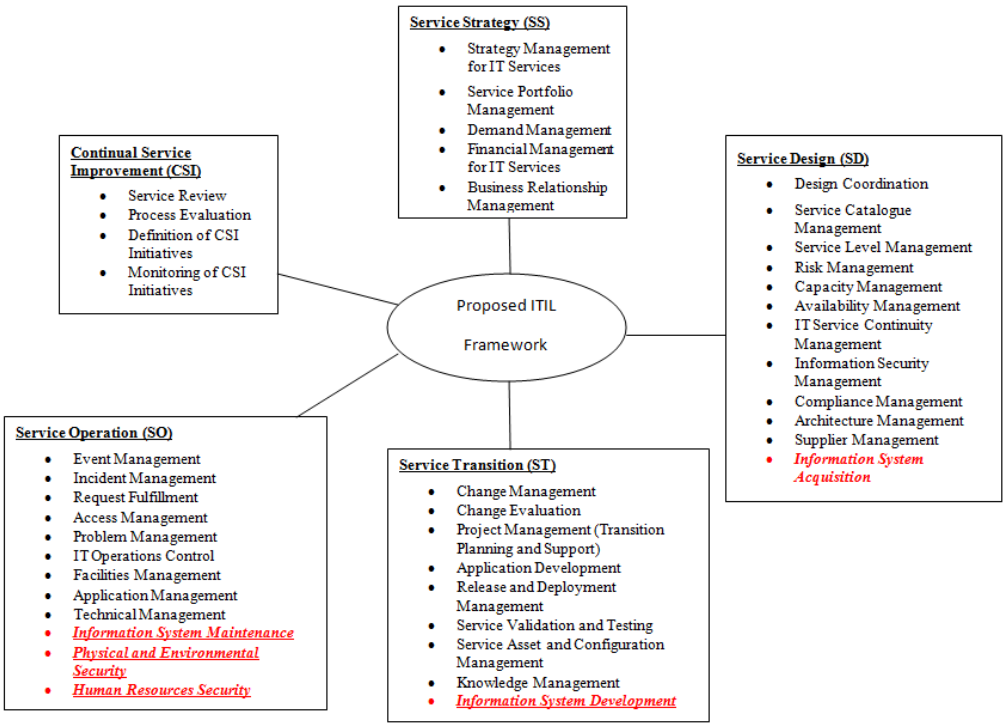

Figure 1: Proposed ITIL framework

Information Security Essential Controls	ITIL Processes
Information Security Policy	• Information Security Management (SD)
Communications and Operations Management	• IT Operations Control (SO) • Business Relationship Management (SS)
Access Control	• Access Management (SO)
Information System Acquisition, Development and Maintenance	N/A
Organization of Information Security	• Information Security Management (SD)
Asset Management	• Service Asset and Configuration Management (ST)
Information Security Incident Management	• Incident Management (SO)
Business Continuity Management	• IT Service Continuity Management (SD)
Human Resources Security	N/A
Physical and Environmental Security	N/A
Compliance	• Compliance Management (SD)

Table 1: Information Security ECs Mapped with Existing ITIL Processes

Reference(s)

Ali, S. M., Soomro, T. R., & Brohi, M. N. (2013). Mapping Information Technology Infrastructure Library with other Information Technology Standards and Best Practices. Journal of Computer Science, 9(9), 1190.

Soomro, T. R., & Hesson, M. (2012). Supporting Best Practices and Standards for Information Technology Infrastructure Library. Journal of Computer Science, 8(2), 272.

Sweren, S. H. (2006). ISO 17799: Then, Now and in the Future. INFORMATION SYSTEMS CONTROL JOURNAL, 1, 34.

Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. Economic Computation & Economic Cybernetics Studies & Research, 43(1), 16

Introduction to ISO 27002 (ISO27002). http://www.27000.org/iso-27002.htm (Accessed on December 1, 2013)

About ISACA. http://www.isaca.org/about-isaca/Pages/default.aspx (Accessed on December 1, 2013)

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. International Journal of Accounting Information Systems, 8(4), 240-263.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security, 24(2), 99-104.

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 8-pp). IEEE.

Cobit 4.1: Framework for IT Governance and Control. http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx (Accessed on December 1, 2013)

PCI Security Standards, https://www.pcisecuritystandards.org/security_standards/index.php (Accessed on December 1, 2013)

PCI DSS Requirements and Security Assessment Procedures. Version 2.0, PCI Security Standards Council LLC, 2010

Akowuah, F., Yuan, X., Xu, J., & Wang, H, (2012), An Overview of Laws and Standards for Health Information Security and Privacy.

Common Security Framework, http://www.hitrustalliance.net/commonsecurityframework/ (Accessed on December 1, 2013)

ITIL Process Map, http://en.it-processmaps.com/products/itil-process-map.html (Accessed on December 1, 2013)

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical & Computer Sciences, 11(5), 2011