Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management

Razieh Sheikhpour[1*] and Nasser Modiri[2]
[1]*Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran*
[2]*Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*
r_sheikhpour@yahoo.com*, nassermodiri@yahoo.com

Abstract

This paper explores the role of information security management within ITIL service management and how ITIL and ISO/IEC 27001 are aligned and can work together to improve information security management.

Keywords: Information security Management, Integration, Organization, ITIL, ISO/IEC 27001, Best Practice

Introduction

The use of information technology brings significant risks to information systems and particularly to the critical resources, due to its own nature (Pereira & Santos, 2010). Therefore, the security of information needs to be managed and controlled properly. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO, 2005a,b; Thomson & Solms, 2005; Solms, 2005; Larrocha *et al.,* 2010).

As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained so that resources are used efficiently. Some of the best practices such as ITIL and ISO/IEC 27001 can be used as a foundation for the development of a sound information security process (ISO, 2005a; Larrocha *et al.*, 2010). ISO/IEC 27001 standard specifies requirements for the design and implementation of an appropriate Information Security Management System (ISMS) in an organization, ensuring that adequate and proportionate controls are selected to protect information assets and to give confidence to interested parties (Jaschob & Tsintsifa, 2006).

ITIL is a collection of best practices for the management of IT services. ITIL helps organizations to become aware of the business value their IT services provide to internal and external stakeholders. The ITIL security management process describes the structured fitting of security in the management organization (Wegmann, 2008; Rezakhani *et al.*, 2011).

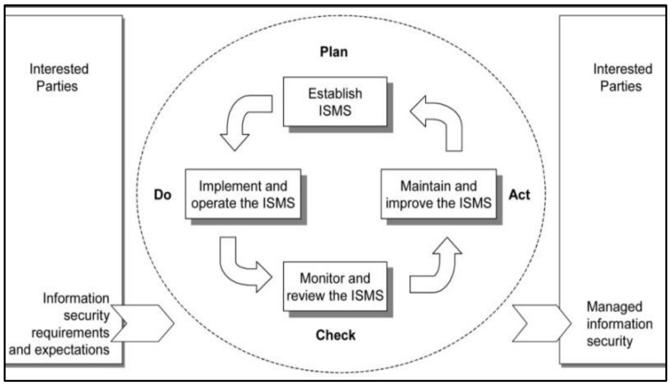
Integration of security best practices like ISO/IEC 27001 into service management best practice processes like ITIL enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels (Warre, 2010). In this paper, we describe an approach for Integration of ITIL and ISO/IEC 27001 services to improve information security management.

ISO/IEC 27001 Standard

ISO/IEC 27001 has its origins from a code of good practice published by the UK department of Trade and Industry in 1989, which slowly evolved into BS7799. ISO/IEC 27001 is a set of guidelines, which can be used by an organization to design, deploy and maintain Information Security Management System (ISMS) (Boehmer, 2008).

This standard is used throughout the world by organizations, both commercial and government, as the basis for the management of the organization’s policy and implementation of information security. It is being used by small, medium and large organizations across a diverse range of business sectors. In fact the standard is designed to be flexible enough to be used by all types of organization. The standard has become the de facto ‘‘common-language’’ for information security management. The ISO/IEC 27001 ISMS standard adopts the well-known PDCA process approach as illustrated in Fig.1. The PDCA approach is also called a continuous improvement since the management system is regularly monitored and reviewed to check whether the controls to manage the risks are still effective and if they are not, then improved controls need to be implemented (Humphreys, 2008; Tsohou *et al*, 2010).

Fig. 1. PDCA model applied to ISMS processes (ISO, 2005b)


Interested Parties
Plan
Establish ISMS
Interested Parties
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Information security requirements and expectations
Check
Managed information security

The PDCA cycle has these four phases: a) “Plan” phase - establishing the ISMS: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives. b) “Do” phase - implementing and operating the ISMS: Implement and operate the ISMS policy, controls, processes and procedures. c) “Check” phase - monitoring and reviewing the ISMS: Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review. d) "Act" phase - maintaining and improving the ISMS: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS (ISO, 2005a,b).

ITIL Framework

The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector. ITIL was first developed by the British Central Computer & Telecommunications Agency, which merged with the UK Office of Government Commerce (OGC) in 2001 (Zegers, 2006; Wegmann, 2008). ITIL presents a broad set of management procedures, which apply to all aspects of IT infrastructure, with which an organization can manage its IT operations (Zegers, 2006, Wegmann, 2008). The ITIL v3 Core consists of five publications, each providing guidance on a specific phase in the service management lifecycle. The ITIL Core publications are as follows: (Zegers, 2006; Sahibudin *et al*, 2008; Esmaili *et al.*, 2010)

Service strategy

The service strategy provides guidance on how to design, develop and implement service management from organizational capability perspective and strategic asset. It provides guidance on the principles underpinning the practice of service management which are useful for developing service management policies, guidelines and processes across the ITIL service lifecycle. Service strategy guidance is applicable in the context of other parts of ITL lifecycle. Service Strategy covers these parts of IT systems: the development of markets, internal and external, service assets, service catalogue and implementation of strategy through the service lifecycle.

Service design

Service design is guidance for the design and development of services and service management processes. It covers design principles and methods for converting strategic objectives into portfolios of services and service assets. The scope of service design includes the changes and improvements necessary for increasing or maintaining value to customers over the lifecycle of services, the continuity of services, achievement of service levels and conformance to standards and regulations. It guides organizations on how to develop design capabilities for service management.

Service transition

Service transition is guidance for the development and improvement of capabilities for transitioning new and changed services into operations. Service transition provides guidance on how the requirements of Service strategy encoded in service design are effectively realized in service operation while controlling the risks of failure and disruption. This part of ITIL framework combines practices in release management, program management and risk management and places them in the practical context of service management.

Service operation

Service operation tries to embody practices in the management of Service Operation. It includes guidance on achieving effectiveness and efficiency in the delivery and support of services so as to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through service operation, therefore making it a critical capability.

Continual Service Improvement

Continual service improvement is including of instrumental guidance in creating and maintaining value for customers through better design, introduction and operation of services. It combines principles, practices and methods from quality management, Change management and capability improvement. Organizations learn to realize incremental and large-scale improvements in service quality, operational efficiency and business continuity.

ITIL security management

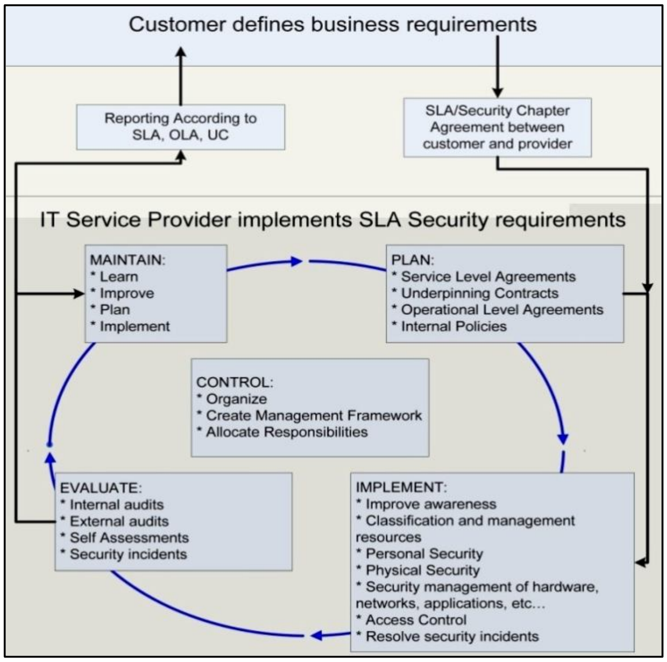
ITIL can help companies assess their risks, and put procedures in place to log and respond to incidents. ITIL, and more specifically the ITIL security management process, is widely used for the implementation of information security within an organization. ITIL v3 has placed the information security management process within the Service Design core practice book. The goal of the information security management process is to align IT security with business security and ensure that information security is effectively managed in all services and service management activities (OGC, 2007; Taylor, 2008).

The security management process consists of activities that are carried out by the security management itself or activities that are controlled by the security management. Because organizations and their information systems constantly change, the activities within the security management process must be revised continuously, in order to stay up-to-date and effective. Security management is a continuous process and it can be compared to the Quality Circle of Deming Plan-Do-Check-Act. The inputs are the requirements which are formed by the clients. The requirements are translated into security services, security quality that needs to be provided in the security section of the service level agreements. Fig.2 shows ITIL security management framework.

The five elements within this framework are as follows (OGC, 2007):

Control: The objectives of the control element are to: Establish a management framework to initiate and manage information security in the organization; Establish an organization structure to prepare, approve and implement the Information Security Policy; Allocate responsibilities; Establish and control documentation.

Fig. 2. ITIL security management framework (OGC, 2007)


Customer defines business requirements
Reporting According to SLA, OLA, UC
SLA/Security Chapter Agreement between customer and provider
IT Service Provider implements SLA Security requirements
MAINTAIN:
* Learn
* Improve
* Plan
* Implement
PLAN:
* Service Level Agreements
* Underpinning Contracts
* Operational Level Agreements
* Internal Policies
CONTROL:
* Organize
* Create Management Framework
* Allocate Responsibilities
EVALUATE:
* Internal audits
* External audits
* Self Assessments
* Security incidents
IMPLEMENT:
* Improve awareness
* Classification and management resources
* Personal Security
* Physical Security
* Security management of hardware, networks, applications, etc…
* Access Control
* Resolve security incidents

Plan: The objective of the plan is to devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.

Implement: The objective of the implementation is to ensure that appropriate procedures, tools and controls are in place to underpin the Information Security Policy.

Evaluation: The objectives of the evaluation element are to: Supervise and check compliance with the security policy and security requirements in SLAs and OLAs; Carry out regular audits of the technical security of IT systems

*Maintain***:** The objectives of this maintain element are to: Improve security agreements as specified in, for example, SLAs and OLAs; Improve the implementation of security measures and controls.

Integration of ITIL and ISO/IEC 27001 services for information security management

ISO 27001:2005 and ITIL v3 are very complementary. The purpose of both standards is to identify best practices. ITIL is focused on service management best practices. ISO 27001 are focused on information security best practices. Both are based on the Plan-Do-Check-Act (PDCA) model (Warre, 2010). If an organization addresses all of the security controls within ISO 27001:2005, therefore a large part of ITIL processes will be covered- especially the section information security management ensure systems security.

ITIL identifies the details of the structure and implementation of the information security management process with the best practices for implementing an Information Security Management System (ISMS) included in the ISO 2700x family of standards (Taylor, 2008). From an ITIL perspective, most of the security controls identified in ISO 27001 are already part of service management. ITIL specifically references ISO 27001 and the requirement for an Information Security Management System. Therefore ITIL and ISO/IEC 27001 can aligned and work together to develop information systems of organizations. The relationship between subjects and control parameters of both standards have been described earlier (Warre, 2010).

An integrated approach for complementary use of ITIL and ISO/IEC 27001 describes a cross-reference between information security management topics in ISO/IEC 27001 and ITIL. For example ISO 27001 defines ISMS as ”that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security”. ITIL specifically references ISO 27001 (Service Design section 4.6.4.3) and defines ISMS as the “framework of policy, processes, standards, guidelines and tools that ensures an organization can achieve its information security Management Objectives” ISO 27001 describes the model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The ISMS identifies the organization’s strategic direction for security and ensures that the objectives are achieved. The ISMS ensures that information security risks are appropriately managed and that information resources are used responsibly.

From an ITIL perspective, the ISMS addresses: Security policy and supporting policies; Security plan; Security organizational structure; Management of security risks; Communication strategy and plan for security. Table 1 shows a cross-reference between all information security management topics in ISO/IEC 27001 and ITIL. Here, a number of scenarios where such complementary use of ITIL and ISO 27001 can be very beneficial are discussed.

Scenario 1

Suppose the company does not have a comprehensive IT service management plan, but the information security department had been proactive, and had started using ISO 27001 as an information security management guideline. The risk management department, now decides to use ITIL as an IT service management framework, and expects the information security department to follow suit. Since information security department has addressed security controls within ISO 27001, therefore a large part of ITIL processes have been covered. The benefit of the complementary approach discussed above, is that the information security department does not have to change anything, using the integrated approach, the information security department can now immediately inform the risk management department or other, precisely which processes from ITIL have been implemented through ISO 27001.

Table 1. A cross-reference between ISM topics in ISO/IEC 27001 and ITIL

ITIL	ISO/IEC 27001
1. Service Strategy	
1.1.Demand management	-
1.2.Financial management	-
2. Service Design	
2.1. Information Security Management	
2.1.1. Information Security Management System	
Service Design: Information Security Mgmt: 4.6.4.3 The Information security management system (ISMS)	4.2.1 Establish the ISMS
2.1.2. Authorized Services/Ports/Protocols	
Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)	4.2.1 Establish the ISMS
2.1.3. Risk Management Methodology and Guidelines	
Service Transition: 4.6.5.9 Risk Management Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS) Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management	4.2.2 Implement and operate the ISMS
2.1.4. Security Policies	
Service Design: Information Security Mgmt: 4.6.4.1 Security framework Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy	4.2.1 Establish the ISMS
2.1.5. Data Classification & Information Handling	
Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)	4.3 Documentation requirements
2.1.6. Security Plan	
Service Design: Information Security Mgmt: 4.6.4.1 Security framework Service Design: Information Security Mgmt: 4.6.5.1 Security controls Service Design: Information Security Mgmt: 4.6.6.2 Outputs	4.2.1 Establish the ISMS
2.2. Capacity Management	
2.2.1. Capacity Monitoring	
Service Design: Capacity Management: 4.3.5.4 The underpinning activities of Capacity Management Service Design: Capacity Management: 4.3.5.5 Threshold management and control	4.2.3 Monitor and review the ISMS
2.2.2. Capacity Review	
Service Design: Capacity Management: 4.3.5.7 Modeling and trending	4.2.3 Monitor and review the ISMS
2.3. Availability Management	
2.3.1. Assessment of Risks Related to Availability	
Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - Service Failure Analysis Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - Single Point of Failure analysis Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - Fault Tree Analysis Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management - Risk Analysis and Management	4.2.2 Implement and operate the ISMS
2.3.2. Availability Monitoring	
Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces Service Design: Information Security Mgmt: 4.6.6.2 Outputs Service Design: Information Security Mgmt: 4.6.9 Challenges, Critical Success Factors and risks Service Design: 4.4 Availability Management	4.2.4 Maintain and improve the ISMS
2.4. Service Level Management	
2.4.1. Security Related Service Level Targets	
Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces Service Design: Information Security Mgmt: 4.6.6.2 Outputs Service Design: 4.2 Service Level Management	4.2.3 Monitor and review the ISMS
2.5. IT Service Continuity Management	
2.5.1. Service Continuity Management Process	
Service Design: 4.5 IT Service Continuity Management	4.2.1 Establish the ISMS
2.5.2. Service Continuity Risk Assessment	
Service Design: IT Service Continuity Management: 4.5.5.2 Stage 2 - Requirements and strategy	4.2.1 Establish the ISMS
2.5.3. Service Continuity Plans	
Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 -Implementation	4.2.1 Establish the ISMS
2.5.4. Testing of Service Continuity Plans	
Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 - Implementation	4.2.2 Implement and operate the ISMS
2.6. Supplier Management	
2.6.1. Security Requirements Identified in Third Party Agreements	
Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces Service Design: 4.7 Supplier Management	4.2.1 Establish the ISMS
3.Service Transition	
3.1. Release & Deployment Management	

3.1.1. Risk Assessment of Proposed Releases	
Service Transition: Evaluation: 4.6.5.9 Risk Management Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS) Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management	4.2.2 Implement and operate the ISMS
3.2. Asset & Configuration Management	
3.2.1. Asset Inventory	
Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS) Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business Service Transition: Service Asset and Configuration Management: 4.3.4.2 Basic concepts Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System Service Transition: Service Asset and Configuration Management: 4.3.5.3 Configuration identification	4.2.1 Establish the ISMS
3.2.2. Asset Review	
Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS) Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business Service Transition: Service Asset and Configuration Management: 4.3.5.6 Verification and audit	4.2.3 Monitor and review the ISMS
3.2.3. Secure Baselines	
Service Transition: Configuration Management 4.3.5.3 Configuration identification - Identification of configuration baselines	4.2.2 Implement and operate the ISMS
3.2.4. Clock Synchronization	
Service Transition: Service Asset and Configuration Management: 4.3.5.3 Configuration identification Service Operation : Event Management : 4.1.5.6 Event correlation	4.2.2 Implement and operate the ISMS
3.2.5. Configuration Control	
Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS) Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control	4.2.2 Implement and operate the ISMS
3.2.6. Verification of Actual Configurations	
Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS) Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control	4.2.2 Implement and operate the ISMS
3.3. Service Validation & Testing	
3.3.1. Security Acceptance Testing	
Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing	4.2.2 Implement & operate the ISMS
3.4. Change Management	
3.4.1. Change Approval	
Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces Service Transition: 4.2 Change Management	4.2.2 Implement and operate the ISMS
3.4.2. Risk Assessment of Proposed Changes	
Service Transition: 4.2 Change Management Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS) Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces	4.2.2 Implement and operate the ISMS
3.4.3. Update Log Management System	
Service Transition: Change Management: 4.2.6 Process activities, methods and techniques	4.2.2 Implement & operate the ISMS
3.4.4. Update Configuration Management Database (CMDB)	
Service Transition: 4.2 Change Management Service Transition: Service Asset and Configuration Mgmt: 4.3.1 Purpose, goal and objectives	4.2.2 Implement and operate the ISMS
3.4.5. Post-Change Security Verification	
Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing	4.2.2 Implement & operate the ISMS
3.4.6. Change Reconciliation	
Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces Service Transition: 4.2 Change Management	4.2.3 Monitor and review the ISMS
3.5. Knowledge Management	
3.5.1. Security Awareness Education & Training	
Service Transition: 4.7 Knowledge Management	5.2.2 Training, awareness and competence
4. Service Operation	

4.1. Event Management	
4.1.1. Event Logging	
Service Operation: Event Management: 4.1.5.2 Event notification	4.2.2 Implement and operate the ISMS
4.1.2. Health and Performance Monitoring	
Service Operation: Event Management: 4.1.5.2 Event notification	4.2.2 Implement and operate the ISMS
4.1.3. Event Correlation & Alerting	
Service Operation: Event Management: 4.1.5.4 Event filtering Service Operation: Event Management: 4.1.5.5 Significance of events Service Operation: Event Management: 4.1.5.6 Event correlation	4.2.2 Implement and operate the ISMS
4.1.4. Periodic Review of Security Events	
Service Operation: Event Management: 4.1.5.5 Significance of events Service Operation: Event Management: 4.1.5.6 Event correlation	4.2.2 Implement and operate the ISMS
4.2. Incident Management	
4.2.1. Incident Response Procedures	
Service Operation: Incident Management: 4.2.5.3 Incident categorization Service Operation: Incident Management: 4.2.5.7 Investigation and Diagnosis Service Operation: Incident Management: 4.2.5.8 Resolution and Recovery	4.2.2 Implement and operate the ISMS
4.3. Problem Management	
4.3.1. Post Incident Review	
Service Operation: Problem Management: 4.4.5 Process activities, methods and techniques	4.2.3 Monitor and review the ISMS
4.3.2. Security Advisories and Vendor Patch Review	
Service Operation: Problem Management: 4.4.5.1 Problem detection	4.2.3 Monitor and review the ISMS
4.4. Request Fulfillment Management	
4.4.1. Verification of requester's credentials	
Service Operation: Request Fulfillment: 4.3.5.3 Other approval Service Operation: Access Management: 4.5.5.1 Requesting access Service Operation: Access Management: 4.5.5.2 Verification	4.2.2 Establish and operate the ISMS
4.5. Access Management	
4.5.1. Requests for Access	
Service Operation: Request Fulfillment: 4.3.5.3 Other approval Service Operation: Access Management: 4.5.5.1 Requesting access Service Operation: Access Management: 4.5.5.2 Verification	4.2.2 Establish & operate the ISMS
4.5.2. Revocation of Access Rights	
Service Operation: Access Management: 4.5.5.2 Verification Service Operation: Access Management: 4.5.5.6 Removing or restricting rights	4.2.2 Establish & operate the ISMS
4.5.3. Periodic Review of Access Rights	
Service Operation: Access Management: 4.5.5.5 Logging and tracking access	4.2.3 Monitor & review the ISMS
4.5.4. Periodic Review of Access Attempts	
Service Operation: Access Management: 4.5.5.5 Logging and tracking access	4.2.3 Monitor & review the ISMS
5. Continual Service Improvement	
5.1. Review Effectiveness of Processes	
All ITIL v3 processes	4.2.3 Monitor & review the ISMS
5.2. Review of Security Policies	
Service Design: Information Security Management: 4.6.4.2 The Information Security Policy	4.2.3 Monitor & review the ISMS
5.3. Preventive/Corrective Actions Management	
Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces	4.2.3 Monitor & review the ISMS 4.2.4 Maintain & improve the ISMS 8 ISMS improvement
5.4. Non-Conformance Management	
Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces	4.2.3 Monitor & review the ISMS 4.2.4 Maintain & improve the ISMS
5.5. Security Risk Assessments	
Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques	4.2.1 Establish the ISMS 4.2.3 Monitor & review the ISMS
5.6. Technical Infrastructure Review	
Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques	4.2.3 Monitor and review the ISMS
5.7. Independent Security Review	
Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques	4.2.3 Monitor & review the ISMS

Scenario 2

The company had implemented an IT service management framework based on ITIL, and the information security department had subsequently also based on the some ITIL processes. The information security department now decides to use ISO 27001, maybe because of its more detailed contents, or maybe because the company has decided to get officially certificated against ISO 27001, or for whatever reason. Using the integrated approach, the information security department can now easily determine which of the ISO 27001 objectives are already satisfied through their use of ITIL, and which must still be given attention.

Scenario 3

If a company implement an IT service management framework based on ITIL because of its wide coverage of information technology topics and an information security management guideline based on ISO 27001 because of its more detailed information security requirements, the company can better meet IT service and information security. Using the integrated approach, company will able to implement both frameworks without no additional cost and time and also information security department can work easily with other department like risk management department

Scenario 4

Company A, having an IT service management framework based on ITIL, takes over company B, who has an information security framework based on ISO 27001. The benefit of the complementary approach, is that the company does not have to change anything, Using the integrated approach determines which processes of ITIL can align to which phases of ISMS life cycle.

Conclusion

Information security describes activities that relate to the protection of information and information infrastructure assets against the risks of loss, misuse, disclosure or damage. There is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted. Systems such as ITIL and ISO/IEC 27001 can be used together as a foundation for the development of a sound information security process. Both ITIL and ISO 27001 identify the requirement to build security into all aspects of the service in order to effectively manage risks in the infrastructure. Since both of them are based on PDCA cycle, many clauses in ITIL service management and ISO 27001 information security management system standard are the same or similar. This paper described the role and importance of effective information security management, how it is supported by ISO/IEC 27001 and the way it harmonize with ITIL. Integration of ISO/IEC 27001 into ITIL service management processes enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels.

References

1. Boehmer W (2008) Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001. *Proc. Second Int. Conf. Emerging Security Information, Sys. & Technologies*. pp: 224-231.
2. Esmaili HB, Gardesh H and Shadrokh Sikari SH (2010) Strategic Alignment: ITIL Perspective. *Proc. 2nd Intl. Conf. Comput. Technol. & Develop. (ICCTD)*. pp: 550-555.
3. Humphreys E (2008) Information security management standards: Compliance, governance and risk management. *J. Info. Secur. Tech. Rep*. 13(4), 247-255.
4. International Organization for Standardization (ISO) (2005a) ISO/IEC FDIS 17799 Information Technology – Security Techniques – Code of Practice for Information Security Management, *ISO/IEC FDIS 17799:2005(E),* Geneva.
5. International Organization for Standardization (ISO) (2005b) ISO/IEC 27001 Information technology- Security techniques- Information security management systems-requirements, *ISO/IEC 27001:2005(E).* ISO Copyright Office. Published in Switzerland.
6. Jaschob A and Tsintsifa L (2006) IT-Grundschutz: Two-Tier risk assessment for a higher efficiency in IT security management. *ISSE 2006- Secur Electro Bus Process. Inform. Secur. Solut. Eur. Conf*. Rome, Italy. pp: 95-101.
7. Larrocha ER, Minguet JM, Díaz G, Castro M and Vara A (2010) Filling the gap of Information Security Management inside ITIL®: proposals for postgraduate students. *IEEE EDUCON Edu. Engg.* pp: 907-912.
8. Office of Government Commerce (OGC) (2007) ITIL V3-Service design book, The Stationery Office, UK.
9. Pereira T and Santos H (2010) A security audit framework to manage Information system security. *J. Comms. Comput. Inform. Sci*. 92: 9:18.
10. Rezakhani A, Hajebi A and Mohammadi N (2010) Standardization of all Information Security Management Systems. *Int.J.Comput.Appl*. 18(8), 4-8.
11. Sahibudin Sh, Sharifi M and Ayat M (2008) Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *Proc. 2nd Asia Intl. Conf. Modelling & Simulation*. pp:749-753.
12. Solms B (2005) Information Security governance: COBIT or ISO 17799 or both? *J. Comput. Secur.* 24, 99-104.
13. Taylor G (2008) ITIL V3 Improves Information Security Management. East Carolina Univ., Jul 11.
14. Thomson KL and Solms R (2005) Information security obedience: a definition. *J. Comput. Secur.* 24(1),69-75.
15. Tsohou A, Kokolakis S, Lambrinoudakis C, Gritzalis S (2010) Information Systems Security Management: A Review and a Classification of the ISO Standards. *J. Next Generat. Soc. Technol. Leg Issues*. 26: 220:35.
16. Warre KV (2010) Security controls in service management. SANS Institute reading room. from http://www.sans.org/search/results.
17. Wegmann A, Regev G, Garret G, Maréchal F (2008) Specifying Services for ITIL Service Management. *Proc. Int. Workshop Service-Oriented Computing Consequences for Engineering Requirements (SOCCER'08).* pp:1-8.
18. Zegers N (2006) A methodology for improving information security incident identification and response. *Master Thesis Inform.& Econom, Erasmus Univ. Rotterdam*.