RUNNING HEAD: ITIL V3 IMPROVES INFORMATION SECURITY MANAGEMENT

ITIL V3 Improves Information Security Management

Ginger Taylor

East Carolina University

ICTN 6823

Abstract

IT Service Management is becoming a must have for any organization that provides IT Services as its core business function. ITIL (IT Infrastructure Library) is a best practices framework that helps businesses align their IT services with their business objectives. The ITIL V3 framework is the newest version of ITIL and was released as a refresh to V2 in 2007. The major difference with V3 is that it moves from a major operational view of IT service management to a more business lifecycle view of IT service management. This paper will begin with an historical overview of ITIL and then move into a high level overview of Version 3, with particular focus on the Information Security Management process. This paper will address how this process has matured and how organizations can better ensure the confidentiality, integrity, and availability of their IT services by implementing the ITIL framework.

ITIL V3 IMPROVES INFORMATION SECURITY MANAGEMENT

What is ITIL? First off, the acronym stands for Information Technology Information Library, and it falls under ITSM, and ITSM is an acronym for Information Technology Service Management. Information Technology Service Management is defined as a "discipline for managing information technology systems, philosophically centered on the customer's perspective of Information Technology's contribution to the business" (Service Management, n.d). ITIL is a best practices framework for companies that provide IT Services as their core business function. ITIL takes a lifecycle approach to an IT service and incorporates best practices and guidelines within each stage of the lifecycle to help IT companies deliver better services to its customers.

What ITIL is not? ITIL is not a formal standard. It is a framework, so the framework gives best practices, not detailed rules that must be adhered to. According to Weil, "ITIL does not provide specific, detailed descriptions about how the processes should be implemented, as they will be different in each organization. In other words, ITIL tells an organization what to do, not how to do it." (2004, ITIL Overview). It is noted in the third sky training manual for ITIL v3, "that it is important to differentiate between the ITIL framework, which provides guidance and recommendations but not strict prescriptions, and standards such as ISO/IEC 20000, which provide formal requirements which need to be adhered to in order to achieve certification. Frameworks may be adapted as needed and provide room for significant re-interpretation" (2007, p. 36). Organizations can adapt the processes and interpret them to their specific business need.

ITIL History

ITIL has its roots in the UK. The British Government, or more importantly the Central Computers and Telecoms Agency (CCTA), which is the now the Office of Government Commerce, emerged with the ITIL concept in the 1980's. The first version of ITIL was called the Government Information Technology Infrastructure Management (GITIM). The fist ITIL books were published after the CCTA consulted with many industry experts. Each book focused on a particular process that would aid in delivering high quality IT Services. In an article by Ptak he states, "This was an attempt to replace the duplication of effort as every IT organization learned by trial and error how to implement and use IT for meaningful work" (2007, ITIL Roots). ITIL began to catch on outside of the UK to other countries such as Australia, Germany, and the US. It is now the "the most widely accepted approach to IT service management in the world" (Office of Government Commerce, 2008, Service Management ITIL).

The earlier version of ITIL was called ITIL V2 this version is known to be primarily process-based and it was comprised of seven core books. They were Service Support, Service Delivery, ICT Infrastructure Management, Planning to Implement Service Management, Application Management, The Business Perspective, and Security Management. The two books that received the most attention in V2 were Service Delivery, and Service Support, which together encompassed the Service Management part of the framework. Within these books were multiple processes that helped IT organizations deal with daily activities involved in the delivery and management of IT services. Now the v2 has evolved into a newer version called v3. The Office of Government Commerce, who owns ITIL, called v3 a refresh project of v2. This update was released in 2007. The last update to ITIL before this was done in 2000. The format moved to a lifecycle approach from a process-based approach. The books were condensed into five core

books they are: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. The ITIL v3 defines the five core practices as follows:

- **Service Strategy**. How to design, develop, and implement service management not only as an organizational capability but also as a strategic asset.
- **Service Design**. How to design and develop services and service management processes that convert strategic objectives into portfolios of services and service assets.
- **Service Transition**. How to take designed services into the live environment.
- **Service Operation**. How to successfully manage services on an ongoing basis.
- **Continual Service Improvement**. How to create and maintain value for customers through better design, introduction, and operation of services (Third Sky, 2007).

Many have said that the books in v3 follow a more practical approach; Tainter and Likier list the approach they believe the books help companies follow as:

1. How to develop a business-driven strategy for IT service management
2. How to design a system to support the chosen strategy
3. How to transition the newly designed system to the production environment (in terms of people, processes, and technology)
4. How to support operations in an ongoing fashion
5. How to continue improving processes and operations (2007, Topics Realignment).

Based on this approach ITIL v3 is focused more on aligning business requirements with IT service management and optimizing the ROI. The goal is to not focus on just operating the services by following the process, but instead focus on the why rather than just the how. The technology-based services are provided to help them meet their business requirements, and then by using the ITIL framework businesses can continuously add value to the service by following the core practices and processes throughout the service lifecycle while optimizing their ROI.

According to a case study done by Toland and Kashanchi, they followed three companies who were or had implemented ITIL to see if they could identify if ITIL did in fact help them with their strategic alignment. The three companies were from banking, education, and IT business sectors. Of the three companies all of them believed that ITIL had a significant impact on strategic alignment. The participant from the banking "agreed that ITIL is an approach to achieve alignment, as it is a framework based on people's past experiences, problems, and successes" (2006, p. 344). The participant from the IT Company stated that, "ITIL absolutely is the approach to achieve alignment, as there is benefit across the board" (2007, p. 344). And the last participant agreed with the others but noted that, "in order to successfully achieve alignment by ITIL the whole organization has to embrace it" (2007 p. 344). The ITIL framework encompasses all parts of an organization from the help desk to the financial department. Everyone in an organization must buy-in to the framework and believe that it can add value to the everyday job they are doing.

ITIL V3 Information Security Management

As noted above, ITIL has emerged and evolved over the past 20 years into a de facto standard that enables IT companies to restructure the way they provide services. Along with the entire ITIL framework getting a facelift one process in particular that has gained more attention with the v3 refresh is the Information Security Management (ISM) process. Why has this process evolved so? This process has had no choice but to evolve because companies have realized that if they do not manage their IT infrastructure properly the financial implications can be extremely costly. In 2005 Ponemon Institute LLC for PGP Corp., a security software vendor in Palo Alto, California claimed that security incidents reached nearly 14 million per incident. However,

some improvements have been noted, the latest Information Security Breaches Survey was released in April 2008, and it revealed that IT managers and board-level executives are trying to keep their organizations secure, with some success. Also according to the survey, the number of security breaches has fallen by a third in the past two years (Barker, 2008).

Why, has it fallen? Simply put, companies are investing more resources and money into the area of Information Security so they can minimize the implications if they suffer an attack. Companies are buying software that will scan for spyware, encrypting their data, and using authentication when users log on to networks. Companies are investing in good security professionals. One job title that has emerged is the position of Chief Information Security Officers (CISO). This position is charged with aligning the Information Security Management program with the strategic goals of the company. According to Whitten, when CISO's, "focus on the business dimension of their role, they should be evaluating ways to increase value to the organization and integrate security needs with the business goals and objectives. This goes far beyond simply safeguarding the assets they are charged with protecting, In addition, they should understand the organization they are in and the broader industry in which they belong" (2008, p.15). This description of a CISO aligns well with how ITIL has "refreshed" their framework from an operation focus to a core IT/Business Alignment focus. According to an article by Weil, "ITIL can help managers understand that information security is a key part of having a successful, well-run organization" (2004, Ten Ways).

We have noted some advances in how companies are improving their Information Security Management programs, but we do know that there is always room for improvement. According to Chris Potter, a partner in PricewaterhouseCoopers and a survey team leader, there are still

“two fundamental contradictions exposed by the Information Security Breaches Survey report” (Barker, 2008, par 4). He said: "Some 79 per cent of businesses believe they have a clear understanding of the security risks they face but only 48 per cent formally assess those risks. Also, 80 per cent are confident that they have caught all significant security breaches but only 56 per cent have procedures to log and respond to incidents” (Barker, 2008, par. 4). ITIL can help companies assess their risks, and put procedures in place to log and respond to incidents. These two things are clearly laid out in the ISM process. We will discuss this further in this paper. According to an article by Williams, Information Security has to evolve. And with this evolution that are some key concepts that are essential for improving organizational security. Two of these concepts are listed below:

- Process is important, actually even more so, than technology –start with process then add technology to support strong process, not the other way around.
- Security can no longer exist in a silo or vacuum, security programs and security professionals must align themselves with the business or face extinction.(Williams, 2006, par. 12-13).

Both of these concepts will be addressed and improved upon with ITIL implementation.

ITIL v3 has placed the ISM process within the Service Delivery core practice book. The Service Delivery core practice is aimed to:

- Design IT services, together with the governing IT practices, processes and policies, to realize the strategy

- Facilitate the introduction of these services into the live environment ensuring quality service delivery, customer satisfaction and cost-effective service provision (Third Sky, 2007, p.100).

With the placement on Information Security Management within the Service Design core book the process is now integrated with several other processes which enables the ISM process to be streamlined in the Service Lifecycle more easily. The processes within the Service Design practice are:

- Service Catalog Management
- Service Level Management
- Availability Management
- Capacity Management
- IT Service Continuity Management
- Supplier Management
- IT Security Management

The Service Design publication is designed to provide 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 (Office of Government Commerce, 2008, Best Practice). The Service Design practice is not limited to new services only. Companies can go back to the service design practice during any phase of a service lifecycle and change or update according to new technologies or policies that may need to be implemented or changed. This is especially a great practice for the ISM process since the discipline of Information Security Management is ever evolving. New technologies claiming to enhance security of data, as well as new security threats emerge constantly. Due to these and other factors companies will have to update or change their security policies regularly. The ITIL v3 Service Design core practice is designed to continuously improve in all the processes so that

the processes can consistently match the current and future requirements of the businesses mission and objectives. According to the Best Management Practice website, "Service Design contains guidance on designing service solutions aligned to the changing requirements of the business. A holistic approach is used for the design of the new or changed services and all of their constituent components are described, adopting the principle that the better the quality of design, the less rework will be required during subsequent stages of the services lifecycle" (Lloyd & Rudd, 2008, par 2). With this as the goal of the service design practice one can conclude that the ISM process will be continuously adapted to meet the business requirements as well. In the past the ISM process was treated as a separate process that sometimes got overlooked as a significant process within the Service Management lifecycle, with the v3 refresh the ISM process is better encompassed into the service management lifecycle.

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" (Third Sky, 2007, p.112). For most companies the Security objective is to "protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity" (Third Sky, 2007, p 113). Deciding what to protect, how to protect it, and at what level it should be protected has to come from the businesses strategic direction and the executive management. The ITIL v3 ISM process enables businesses to align their strategic direction with their security management process by "designing and building consistent, measurable information security measures into IT services rather than after-the-fact, and this ultimately saves time, money, and effort" (Weil, 2004. Ten Ways).

The ISM process contains several sub-processes in ITIL v3. They are design of security controls, security testing, management of security incidents and security review. The objective of the sub process of the security controls is to design the appropriate technical and organizational measures in order to ensure the confidentiality, integrity, security, availability of an organization's assets, information, data and services. An example of a security control is access rights. By implementing tools such as authorization and authentication within network equipment you are attempting to control who accesses certain network equipment. This will help ensure that management can review who signed on and changed and/or accessed the configuration of a server, or other network device.

The sub-process of security testing is there to ensure that the security mechanisms are tested regularly. Service management as a discipline requires regular reporting. In order to report on the usefulness of a security management process you have to test that your tools and processes work should an attack occur. "The reporting required by ITIL keeps an organization's management well informed about the effectiveness of their organization's information secuirty measures. The reporting also allows management to make informed decisions about the risks their organization has." (Weil, 2004, Ten Ways).

The management of security incidents sub-process is an integral part of the ISM process and it helps organizations to put a number of measures in place to ensure response is appropriate. Measures are placed based on the importance of the information. Measures that ITIL uses for the ISM process are preventative, reductive, detective, repressive and corrective (Third Sky, 2007 p. 114).

Preventative measures help to prevent security incidents from ever occurring. Some preventative measures are controlling access rights, authorization (defining explicitly who is able to access certain information), and authentication (using tools or measures that confirms the identity of those accessing certain information).

Reductive measures are taken proactively to help minimize the damage from a security incident. Some examples are daily backups of data, and testing of disaster recovery plans.

Detective measures are used to help discover if a security incident has occurred. By using detective measures in your ISM process you can help ensure that you discover the security breach as soon as possible (Third Sky, 2007 p. 114). Network monitoring is a great example of using detective measures. By using network management software you can get set parameters for alarms to indicate anything from hardware overheating to unauthorized access being logged.

Repressive measures help to keep a security incident from repeating itself or continuing. An example of a repressive measure is when you lock yourself out of an account by missing the password or pin number.

And lastly there are corrective measures. These measures help repair the damage that was made by the security incident. An example could be restoring the backup, or a back-out plan being taken because of a failure in a system, etc.

Lastly the security review sub-process's objective is to review if security measures and procedures are still in line with risk perceptions from the business side, and to verify if those measures and procedures are regularly maintained and tested (IT Security Management, n.d.). The review sub-process can be managed by the reporting that is required by ITIL as well.

Organizations can review the reports and analyze if new risks have developed that require new measures and/or tools to control and/or mitigate the risks.

Conclusion

The ITIL v3 IT Security Management process was "updated to account for new security concerns" [3] and by implementing ITIL organizations can significantly improve their IT security management. As discussed in this paper the new ISM process within the Service Delivery core practice of ITIL v3 provides several ways that information security can be improved. The ISM process encourages organizations to incorporate security controls, and to test these controls regularly. It also incorporates an incident management process that enables organizations to better respond to security incidents. By implementing this process organizations have a planned and documented process to follow should a security incident occur, rather than running around in "fire fighting" mode at the last minute. The lastly, with ITIL's requirement for continuous review, it can help ensure that information security measures maintain their effectiveness as requirements, environments, and threats change (Weil, 2004, Ten Ways).

Security Level Management is a growing discipline, and the ITIL framework is a highly regarded best practice standard in the ITSM discipline. "The purpose of service level management is to maintain and improve the quality of an IT service. Service level management maintains consensus between a service provider and a recipient concerning the quality of an IT service and monitors, reports, and reviews the quality for a specified period" (Ishibashi, 2007 p 336). With this description of Service level management based on this paper we can deduct that

the ITIL Information Security Management process meets all of these requirements. Information Security can no longer be looked at as a separate discipline it has to be looked at as a service that should be a part of a service lifecycle. By implementing ITIL organizations can better meet information security service expectations with internal and external customers by using standardized processes based on best practices.

.

References

Barker, C. (2008, Apr. 23). Security Breaches Down – but at what price? Retrieved June 4, 2008, from http://software.silicon.com/security/0,39024655,39201844,00.htm?r=1

* Ishibashi, K. (2007, Jan. 18). Maintaining Quality of Service Based on ITIL -Based IT Service Management". *Fujitsu Scientific Technical Journal Vol 43 Issue 3* pp 334-344.

IT Security Management. *In Wikipedia Online Encyclopedia.* Retrieved May 30, 2008 From, http://wiki.en.it-processmaps.com/index.php/IT_Security_Management.

* Kashanchi, R & Toland, J. (2006). "*Can ITIL Contribute to IT/Business Alignment? An Initial Investigation.*" *WIRTSCHAFTSINFORMATIK 48 (5),* pp 340-348.

Likier, M & Tainter, M. (2007,Oct. 25). Key Differences Between ITIL v2 and v3. Retrieved June 4, 2008, from, http://www.itsmwatch.com/itil/article.php/11700_3707341_1.

Lloyd, V. & Rudd, C. (2008). "Service Design". Retrieved June 16, 2008. from, http://www.best-management-practice.com/bookstore.asp?FO=1229358&DI=591432

Office of Government Commerce. (2007). Service Design Contents. Retrieved June 1, 2008 From, http://www.best-management-practice.com/gempdf/Service_Design_Contents.pdf.

Office of Government Commerce Best Management Practice. (2008). Service--Management ITIL. Retrieved June 4, 2008, from http://www.best-management-practice.com/Knowledge-Centre/Best-Practice-Guidance/ITIL/?trackid=002203.

Ptak, R. (2007, Jan. 22). The History and future of ITIL. Retrieved June 1 2008 from http://searchdatacenter.techtarget.com/tip/0,289483,sid80_gci1240168,00.html

Service Management. In *Wikipedia Online Encyclopedia*. Retrieved June 4, 2008, from http://en.wikipedia.org/wiki/IT_Service_Management

Third Sky. (2007). *ITIL Version 3 Foundation Bridge: Education in ITIL Service Management Practices Course Manual.* San Francisco, CA: Third Sky, Inc.

Weil, S. (2004, Dec.22). How ITIL Can Improve Information Security. May 30, 2008, from http://www.securityfocus.com/infocus/1815

* Whitten, D. (2008). *The Chief Information Security Officer: An Analysis of The Skills Required for Success. Journal of Computer Information Systems* Vol. 48 (3) pg 15.5 pgs.

Williams, A. (2006). Information Security Must Evolve. Retrieved June 1, 2008 from, http://techbuddha.wordpress.com/2006/11/13/information-security-must-evolve/