DITY™ Weekly Newsletter
itSM Solutions® IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself Vol. 4.32 • August 13, 2008

11 Ways ITIL Improves Security

By Hank Marquis
Hank is EVP of Knowledge Management at Universal Solutions Group, and Founder and Director of NABSM.ORG. Contact Hank by email at hank.marquis@usgct.com. View Hank's blog at www.hankmarquis.info.

ITIL improves security governance. ITIL makes security easier and more controlled, thus making it easier to comply with regulations like Sarbanes-Oxley, HIPAA, FISMA, GLBA, NIST 800-53/FIPS200, FFIEC, and others.

The IT Infrastructure Library® (ITIL®) is best practice. We all know ITIL describes what to do, not how to do it. The descriptive nature of ITIL leads many to wonder what benefits ITIL delivers, if any.

However, without too much thought, anyone familiar with a particular industry or IT segment can soon understand how ITIL best practices can assist virtually any operational aspect of IT.

Let's examine security for example. How can ITIL best practices help with the day to day workings of security?

The ITIL has a dedicated book for security, and includes security as a fabric within which the Service Support and Service Delivery books operate. The ITIL focuses on the process of implementing security requirements identified in Service Level Agreements.

However, as always, the ITIL is descriptive and not prescriptive. Following, I show at least 11 ways ITIL can improve or assist in security, and give you a 9-step plan for improving security using ITIL.

Security and ITIL

ITIL describes a Security Management function (e.g., a group, like Service Desk) that interfaces with other ITIL processes regarding security issues. These issues relate predominantly to the Confidentiality, Integrity and Availability of data, as well as the security of hardware and software components, documentation and procedures.

Virtually every organization faces some form of oversight and regulation. We have all heard of Sarbanes-Oxley, but there are many, many more. HIPAA, FISMA, GLBA, COBIT, NIST 800-53/FIPS200, FFIEC, and others.

There are at least five areas to consider with thinking about security and ITIL:

1. The process of security management
2. The relationships between security and the other ITIL processes
3. External relationships as defined in Underpinning Contracts (UCs)
4. Customer facing requirements as defined in Service Level Agreements (SLAs)
5. Internal relationships between functional organizations as defined in Operating Level Agreements (OLA's)

Here are some easy ways the best practices in ITIL can improve how IT organizations implement and manage information security in response to regulations.

1. Security requires audits, and regardless of the regulatory environment, IT must support audits. Audits require documentation, process control, and clear roles, responsibilities, and authorities. ITIL processes descriptions provide the basis for sound audits.

2. Security requires control over assets. To control assets you must know what you have, where it's located, and who can access it. This basis comes directly from ITIL Configuration Management.
3. Most regulation, including HIPAA and SOX, requires analysis and documentation of changes made to IT systems. In change management many issues are to be ensured. Change Management can perform risk analysis, business impact analysis, and security analysis from a centralized perspective.
4. Security management requires an incident category specifically for security related incidents. The ITIL Incident Management process provides the control and flexibility required to manage security incidents quickly and efficiently without a duplicate organization.
5. Security Incidents require review by security management. Having a single point of contact for all matters relating to IT – the ITIL Service Desk – provides a single reporting source for all Incidents, including those pertaining to security.
6. ITIL focuses security where needed based on business requirements, not technology. This is important since most security operations today do what they feel is best for the business instead of just what the business required. This "gold plating" carries a high cost and keeps IT from being seen by the business as a partner.
7. Since ITIL is all about organizational best practices, the security management process itself can operate in a process-driven, methodical manner. This is absolutely critical to success with security.
8. ITIL requires continuous review, audit, and reporting of processes activities. Security requires continuous reviews to remain vigilant.
9. Availability Management describes a centralized engineering and architecture that always takes into account the Confidentiality, Integrity, and Availability of data (CIA).
10. The Service Level Management process sets up, monitors, reports on, and administers agreements with customers (SLA), suppliers (UC), and other IT functional departments (OLA). These contracts and agreements all require security sections.
11. Establish a link between Problem Management and security alert channels. Relevant security issues should be documented and added to the knowledge base for use by Incident Management and the service desk as well as other IT functional groups.

Summary

ITIL best practices help deliver real security improvements, as well as establishing the controls required for meeting legislative and regulatory requirements.

Here is a simple 9 step plan for improving security using ITIL:

1. Work with customers and the business to understand and document security requirements. It is very important that you take your lead from the business.
2. Review with senior IT leaders to ensure review of all relevant legislative, industry, and corporate regulations.
3. Work with other ITIL process managers to validate the ability to support customer (#1 above) and corporate (#2 above) security requirements identified.
4. Negotiate a Service Level Agreement (SLA) that includes a security section. As always, keep it in business terms, and make sure it is measurable.
5. Based on the SLA(s), create and implement Operational Level Agreements (OLAs) between related technical or functional departments or groups. Each OLA requires a security section that clearly spells out and defines how, for example, security incidents will be handled.
6. Review all Underpinning Contracts (UCs) for security as well. They should all include a security section. For example, defining access to customer information and data confidentiality.
7. Update UCs, define and implement OLA's, then publish the SLA.
8. Report on security as you would report on capacity, availability, or changes.
9. As required, iterate the security sections as required.