

Introduction to ITIL Service Management and Security Management

By Mark Azzolina

In the late 1980s, the government of the United Kingdom commissioned the Central Computer and Telecommunications Agency (CCTA) to address the rising operational and support costs of IT infrastructures. The government recognized that they and industry alike required controls to manage their IT infrastructure.

In the late 1980s, the government of the United Kingdom commissioned the Central Computer and Telecommunications Agency (CCTA) to address the rising operational and support costs of IT infrastructures. The government recognized that they and industry alike required controls to manage their IT infrastructure. The UK directive to the CCTA resulted in the publication of the “*Government Information Technology Infrastructure Management*,” or GITIM. GITIM described an IT service-management framework and was composed of ten core books devoted to service support and service delivery processes. The core documents were accompanied by 30 complementary documents addressing many specific areas of IT operations.

After the CCTA was reorganized into the Office of Government Commerce (OGC), the second version of GITIM was published in 2000 under a new title: the Information Technology Infrastructure Library (ITIL). Like the first version, the second version of ITIL focused on service management, but it restructured the ITIL publication set into a more concise and usable reference set.

After its introduction, governments and private industry in Europe rapidly adopted the ITIL framework. It was soon recognized as the de facto standard for IT service management providers. It has found such acceptance today that the new British Standard, BS 20000 (previously BS 15000) is heavily based on the ITIL process framework.

ITIL implementations are also catching on in the United States. Many high-profile US organizations have adopted the service management best practices described in ITIL. Procter and Gamble, Boeing, and the Internal Revenue Service are often used as examples of US ITIL success stories. If you want to get an idea of how popular ITIL

implementations are, go to an Internet job search engine and type it in. A recent search on www.dice.com resulted in 691 job postings throughout the US, and according to a META Group operational trends report¹, by the year 2007, 40 percent of US organizations will adopt ITIL as their service management best practice framework.

The current version of ITIL is divided into eight publications commonly known as “sets.” The ITIL processes described within these publications overlap with one another, but together cover IT service management best practices. The eight publications of the IT Infrastructure Library are:

- Service Support
- Service Delivery
- Planning to Implement Service Management
- Software Asset Management
- Applications Management
- Security Management
- The Business Perspective
- ICT Infrastructure Management

Together these publications describe the processes necessary for efficient and financially responsible management of IT organizations and activities. The Security Management book is designed to augment the other document sets by overlaying service management processes. Security Management oversees the implementation of the corporate information security policy through measures, incident

¹ META Group, META Group Operations Strategies 2005/2006 META Trends, February 2005

response, audits of measures and information security status reports. The Security Management measures of control, implementation, security reviews, maintenance and reporting are contained in Chapter 4, “Security Management measures,” of the Security Management book.

According to ITIL, Service Management is composed of Service Support and Service Delivery processes. Because of ITIL’s strong focus on service management, the most important books in the ITIL publication set are the Service Support and Service Delivery books. Half of ITIL service management processes are provided in the former, while the other half are detailed in the latter. Although described in separate ITIL publications, all ITIL service management processes are related and may overlap.

Five disciplines make up ITIL Service Delivery. Each is described below.

- **Capacity Management** ensures that network and IT capacity is always available to satisfy the requirements of the business. This involves more than just monitoring capacity metrics on your network. It also involves the adequate analysis of change requests and their impact on current or future capacity.
- **Financial Management** for IT Services involves the measurement and assessment of costs associated with the IT infrastructure, and for maximizing the return on an organization’s IT investment.
- **Availability Management** is concerned with ensuring that IT services are available and managed through incidents and problems to restore availability and protect against non-availability due to similar problems.
- **Service Level Management** is the oversight of Service Level Agreements (SLAs) and Operating Level Agreements (OLAs) to ensure that agreed-to performance levels are met and service-quality issues are minimized. An SLA is an agreement between the IT service provider and its customers. An OLA is an agreement between the IT service provider and those business entities that provide services to it. For example, power is required to run information systems and networks. The power provider and the IT service provider establish an OLA to define agreed-to service levels.
- **IT Service Continuity Management** involves the management of activities necessary in resuming agreed-to service levels after an interruption to the business.

These are the six ITIL Service Support disciplines:

- **Service Desk** involves the management and operation of the IT services organization’s customer interface. The service desk is expected to respond to customer problems, monitor customer problems through to their resolution, and keep customers informed on progress made on their reported problems or incidents.
- **Incident Management** is the recording and tracking of customer incidents. An incident may become a problem that is addressed in the problem management, change management and configuration management processes.
- **Problem Management** involves the use of incident reports from the service desk to identify the cause of the incident or problem trends.

An SLA is an important component of ITIL processes. It is the foundation of communication between the IT services provider and the IT customer. Without it, there would be no way for the provider or the customer to manage the expectations of the other.

- **Configuration Management** is the maintenance of detailed component documentation that defines the network configuration baseline. Configuration management documentation includes network diagrams, hardware inventory lists, software inventory lists by hardware components, product documentation, user manuals, administrator manuals, operating instructions, design documents, etc.
- **Change Management** is the management of change requests for new functionality or problem resolutions. This includes change impact analysis through change scheduling.
- **Release Management** describes the processes required for delivering and implementing product releases. A product release may include code corrections, new operating system services or products required for the code corrections, or new functionality. It may also include new hardware or firmware upgrades.

ITIL identifies three other “principal elements” to the library. They are the Business Perspective, ICT Infrastructure Management, and Applications Management books. The Business Perspective book covers business issues associated with the operation and management of an information technology organization. The ICT Infrastructure Management book concentrates on the daily management of the IT infrastructure, while the Applications Management book deals with the software development lifecycle, including the clear definition of requirements, through to validation that the original requirements are met.

The importance of the service level agreement (SLA)

An SLA is an important component of ITIL processes. It is the foundation of communication between the IT services provider and the IT customer. Without an SLA, there would be no way for the provider or the customer to manage the expectations of the other. The SLA should clearly define acceptable levels of service and quality as well as processes that are required to correct service-level deficiencies. Using these levels as common points of reference, the provider and the customer can work together in an open environment where performance and expectations are quantifiable.

Security Management

Although ITIL does not identify security management as one of the “principal elements,” it holds a prominent place in the IT Infrastructure Library. The other ITIL publications deal with the management of the IT infrastructure. The Security Management

book focuses on the management of the security of the IT infrastructure. Figure 1 represents how ITIL Security Management interfaces with ITIL Service Management.

The IT service provider and the IT customer agree to service levels and quality standards in SLAs. One section of the SLA should address information security and include agreed-to levels of confidentiality, integrity and availability (CIA). To achieve the information security service levels in the SLA, a corporate information security policy is published and used by the provider and the customer alike. Security Management is the implementation of controls necessary in establishing and maintaining the CIA levels documented in the SLA.

According to the ITIL Refresh Scope and Development Plan², the UK is expected to release the core set of the third version of ITIL by February 2007. The new document set will follow the service management lifecycle, to better serve as a reference. It will be composed of five volumes of guidance:

- Service Strategies
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

As with all ITIL versions, the new version is directed at controlling the spiraling cost of IT operation and management. Considering ITIL's focus on IT best practices, it is no wonder that organizations are reporting significant cost savings with the implementation of ITIL processes. However, the most successful ITIL implementations do not follow ITIL

² Office of Government Commerce, ITIL Refresh: Scope and development plan, June 2006. Office of Government Commerce, Best Practice for Service Delivery, ITIL – The key to Managing IT Services, 2000. Office of Government Commerce, Best Practice for Service Support, ITIL – The key to Managing IT Services, 2000. Office of Government Commerce, Best Practice for Security Management, ITIL – The key to Managing IT Services, 2000. Office of Government Commerce, ITIL Glossary of Terms, Definitions and Acronyms, 2006

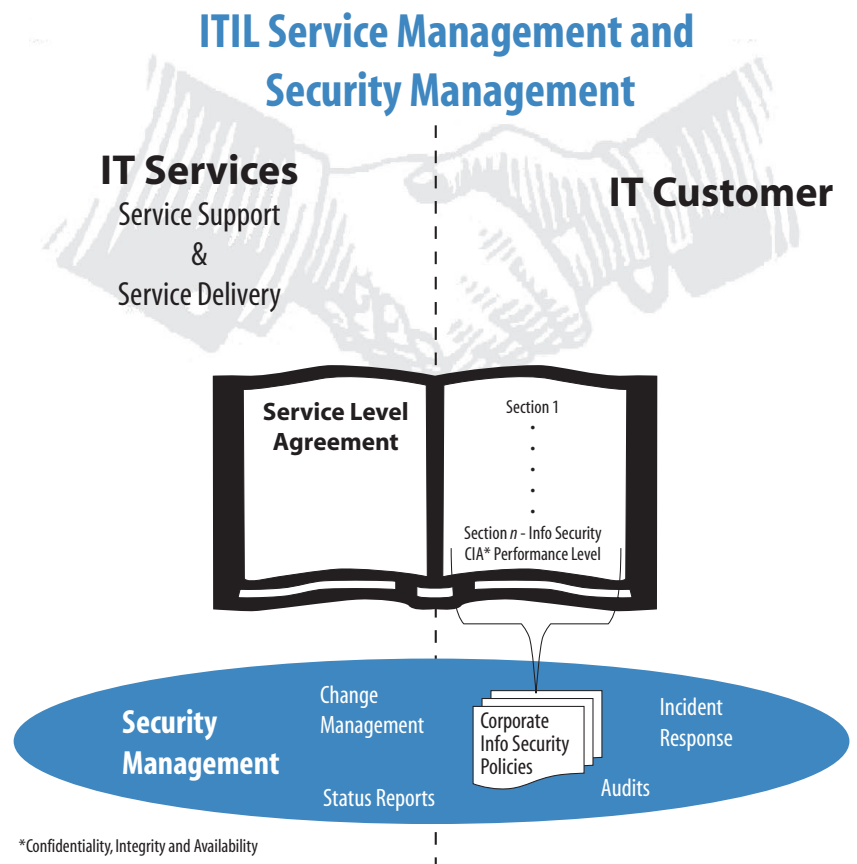


Figure 1. ITIL Service Management and Security Management

processes verbatim. They determine which ITIL processes make sense for their company size, computing environment or required IT investment, and implement ITIL to best fit their organizations.

About the Author

Mark Azzolina, CISSP-ISSMP, is the CEO and Principal Consultant for Compliant IT Services, an IT security and compliance consulting firm. Mark has also been a member of the ISSA-Colorado Springs chapter since 2001. He can be reached at mark@compliant-its.com or (719) 282-1823.