Information Security and Service Management for State & Local Governments

Security and Risk Management

ISSM and ITIL/ITSM Interrelationship

Introduction

Over the last decade, there has been a radical change in the way organizations operate.

Public sector IT executives bear greater responsibility and accountability than ever before. Agency managers no longer view IT merely as a provider of technology, responsible for maintenance and support. IT is a partner in delivering the mission of the agency.

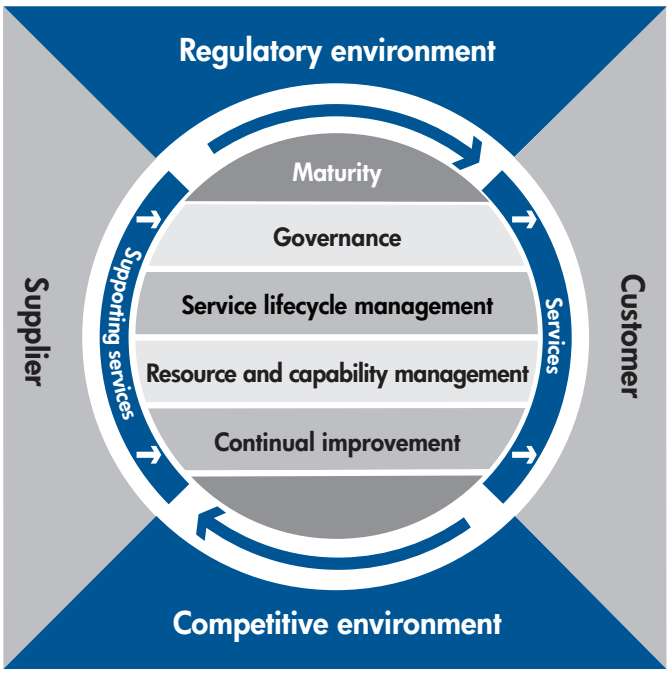
For agencies and organizations to achieve meaningful service outcomes, technology and agency decision makers need to align their goals and strategies more closely while dealing with an increasing amount of technologies, threats, and regulatory compliance requirements.

Therefore organizations need to build and run an integrated service management system that addresses security and risk management as well as the regulatory compliance imposed on the agency while ensuring that agreed services are provided to internal and external customers and managed end-to-end.

Standards that can be leveraged for such integrated service management system include ISO 9001 (processes), ISO/IEC 20000 (service management), ISO/IEC 27001 (security), COBIT (IT organizations), and many others. These standards typically provide a control framework for a given topic and scope without significant and detailed guidance on how to implement the control framework. For implementation, agencies are also turning to sources of industry best practice such as ITIL (from the British Government) and CMMI (from the Software Engineering Institute of Carnegie Mellon).

This white paper describes how HP is helping customers to build and run an information security management system using the HP Information Security Service Management (ISSM) Reference Model as an integral part of a service management system provided by the HP Service Management Framework which is bringing together relevant international standards with HP and industry best practices.

Figure 1. HP Service Management Framework



An Integrated Service Management System

Hewlett-Packard (HP) has developed the **HP Service Management Framework** to provide an integrated service management system for agreed, predictable, and consistent delivery of services that balance performance, quality, risk and cost. It reduces complexity, brings organizations up-to-speed quickly and takes everything service providers need to do to mitigate operational risk and drive positive business outcomes into account. With this framework, executives responsible for generating positive results through information technology can understand the requirements and best practices required for effective service management better.

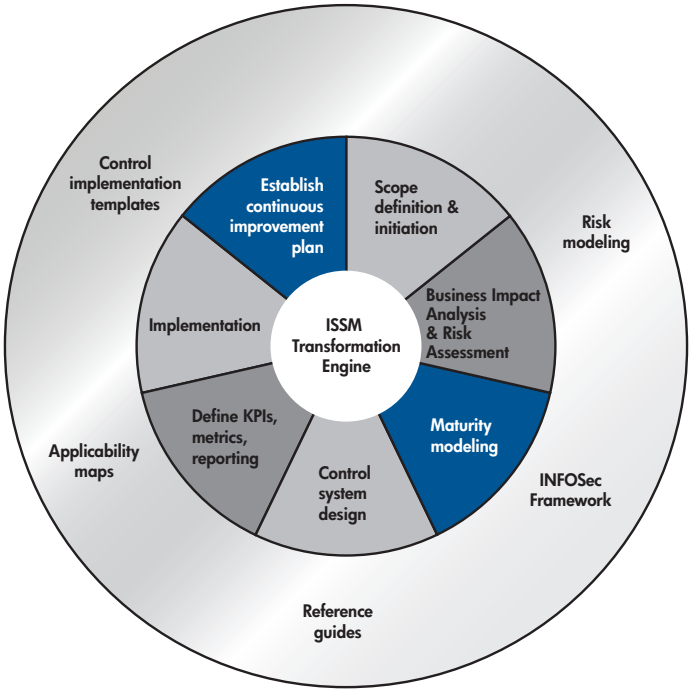
The HP Service Management Framework is a holistic approach for service providers that want to build and run an effective service management system. The framework organizes the service assets within a service provider (for example, people, processes and technology) and brings together international standards (for example, ISO/IEC 27001, ISO/IEC 20000), industry best practices (for example, ITIL v3, COBIT, CMMI) and HP best practices (for example, HP Information Security Service Management (ISSM) Reference Model, IT Governance Capability Model and the HP IT Service Management Reference Model).

The purpose of the HP Service Management Framework is to help enterprises:

- Position themselves correctly as service providers with appropriate inputs and outputs
- Provide consistent quality services that will achieve desired outcomes
- Manage all of the service assets required
- Understand the many standards and sources of best practice for service management
- Transform themselves into a strategic partner to the business side of the agency

HP's Service Management Framework provides detailed guidance on implementation and operation of a successful service management system.

Figure 2. HP ISSM Reference Model



Information Security Service Management

In order to address topics like security, governance, risk, and compliance, the **HP Information Security Service Management (ISSM) Reference Model** was developed. This is a holistic, standards-based security model that guides an organization toward a defense-in-depth approach to managing and mitigating operational risk through the deployment of highly operationalized security controls.

The HP ISSM Reference Model helps organizations to build and run an information security management system within the context of a service management system. The ISSM reference model components include:

1 **Risk Modeling**—Modeling helps to capture and summarize likely threats and impacts quickly

2 **ISSM Framework**—This organizational structure articulates risk management emphasis, describing present and future control state with associated maturity and compliance ratings

3 **ISSM Transformation Engine**—This calculates compliance gaps between an organization's present and future state, compensating controls in order to determine the level of adherence to standards and regulations

4 **Reference Guides**—These authoritative sources of security controls provide deployment guidance, referring to standards and industry best practices

5 **Applicability Maps**—These critical touch points show where security controls are applied throughout an enterprise

6 **Control Implementation Templates**—Technical specifications and standards provide detailed guidance on the implementation of compensating controls

The purpose of the HP ISSM Reference Model is to help enterprises:

- Establish a rational basis for control system decision-making
- Ensure security alignment with business objectives
- Uncover inadequate or failing internal processes to reduce operational risk
- Identify threats and vulnerabilities early and aligns proper compensating controls
- Structure complex security environments into a cohesive architecture of manageable components
- Implement a pragmatic, quality-driven security solution
- Provide a vehicle for facilitating security messaging across business functions

Addressing the security gap

By their very nature, international standards and industry best practices provide requirements, control frameworks, and concepts that must be translated and implemented to each organization's unique context and mixture of resources and capabilities. And also every organization has a unique set of technologies/products to deliver and manage services with. For example, if the perfect organizational structure would exist, then everybody would already have it by now.

Specifically for security management, the most common standards used are ISO/IEC 17799, ISO/IEC 27001, and COBIT. Unfortunately, none of these standards provide detailed design and implementation guidance.

Also ITIL—which is often expected to provide more depth—does not provide nor has a good track record for a direct security treatment but only references to the standards mentioned before. Let's look at an overview of the security management gap within ITIL:

Version:	Effective Dates:	Books:	Security Treatment:
ITIL Version 1	1986 to 1999	30	Not available
ITIL Version 2	1999 to 2006	10	Referenced ISO 17799, COBRA, ISO Interactive Manuals
ITIL Version 3	2007 to now	5	Referenced ISO/IEC

Understanding the international standards and industry best practices around security today, HP recognizes the need to bridge the "security gap" and offer a current and more in-depth Information Security Management approach that could "snap" into any organization's current or planned Service Management implementation efforts. To that end, HP developed the Information Security Service Management (ISSM) Reference Model.

The ISSM Reference Model offers (very) prescriptive design guidance and implementation blueprints on how to deploy a best-practice information security service management system through an INFOSec program. Although this is an excellent foundation, without the application of service management practices to ensure that the security controls are implemented within the processes, it runs the risk of becoming ineffectual.

The combination of the HP ISSM Reference Model and the HP Service Management Framework results in an approach to security where safeguards and controls are aligned to process and offered as strategic value-added services. This is accomplished by relating and integrating People, Policies, Processes, Products, and Proof points (P5 Model) completely to an organization's IT processes.

HP's ISSM Reference Model has been designed as complimentary to ITIL and as an integral part of the HP Service Management Framework. The ISSM Reference Model, by design, supplements and overcomes the inherent deficiencies existing within Version 1 and 2 of ITIL in the area of Security Management as well as provides practical implementation guidance to (the ITILv3 reference to) ISO/IEC 27001.

Ostensibly, the ISSM Reference Model becomes the new and vastly-improved Information Security Management process and system indicated within the ITILv3 Service Design book and joins the following other processes included within this document:

- Supplier Management
- Availability Management
- IT Service Continuity Management
- Capacity Management
- Service Level Management
- Information Security Management (ISSM)

The ISSM Reference Model also benefits substantially from service management by applying the processes necessary to deploy high-value and cost-effective security services. For example, ISO/IEC 27001 provides little in the way of budget management; however, ITILv3 has a well defined Financial Management process that articulates the basis for managing and controlling the operational cost of an Information Security Management System through an INFOSec program.

This, as well as other Service Management processes provide the operationalization guidance necessary to run an enterprise INFOSec program as a business function and best-in-class operation.

By applying Service Management guidance, the ISSM Reference Model components benefit directly from the following service management function and processes:

- Service Desk/Request and Incident Management
- Problem Management process
- Change Management process
- Service Asset and Configuration Management process
- Release and Deployment Management process
- Service Validation and Testing process
- Service Design Processes

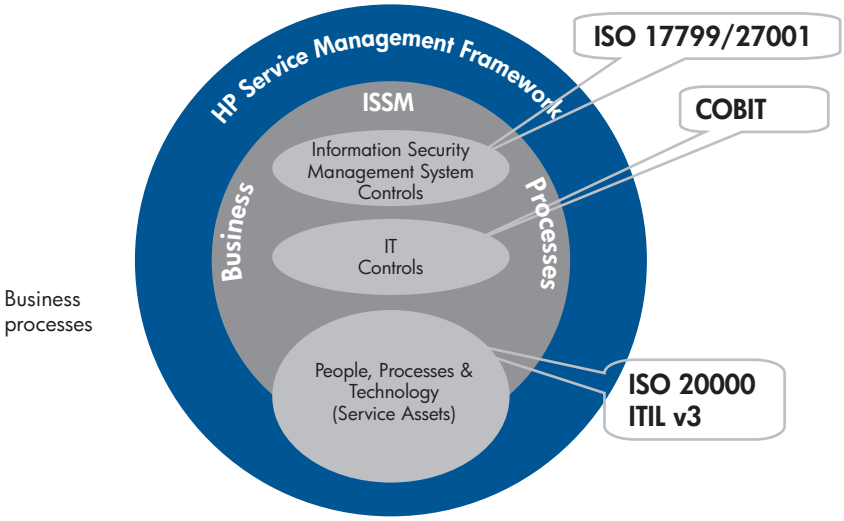
Making a direct correlation to the HP Service Management framework is one of the best ways to understand what the HP ISSM Reference Model provides. For example, ITILv3 is a comprehensive set of standards and the HP Service Management Framework is the realization of those standards in a practical sense, which guides their applicability and deployment within a service provider environment. HP's ISSM Reference Model is to the ISO/IEC 27001 security standards as the HP Service Management Framework is to ITILv3 in as much as both are based on internationally recognized standards and practices that take purposeful approaches to integrating IT and agency management functions.

Figure 3. The HP SMF and the HP ISSM Reference Model.

The following depiction shows the relation between the HP ISSM Reference Model and the HP Service Management Framework

HP ISSM and Service Management

Based on Open Standards



Bringing Security and Service Management together

The security controls defined and managed within the ISSM Reference Model are implemented using service management best practices on how to apply and manage service assets such as people, process and technology, which brings high-operational value to the compensating controls defined within the HP ISSM Reference Model.

Considering the substantial "security gap" in ITIL the ISSM Reference Model is ideally suited and positioned to address the Security Management Process and System within a Service Management implementation.

The following table shows in general how the HP Service Management Framework is complemented by the HP ISSM Reference Model.

HP ISSM Reference Model complements the HP Service Management Framework

ISO 9001:2000	Service Management	Security & Risk Management
Tier 1—policies and processes	ITIL V3, HP Service Management Framework	ISSM Framework, Risk Modeling
Tier 2—operating procedures	HP Service Management process guides	Reference Guides, Applicability Maps
Tier 3—work instructions	HP Service Management work instructions	Control Implementation Guides
Tier 4—forms and templates	HP Service Management templates, HP Software settings	ISSM Transformation Engine

In particular, the following HP Service Management Framework processes are being complemented by the HP ISSM Reference model materials:

1. Availability management
2. IT Service Continuity Management
3. Information Security Management
4. Assess and Manage IT Risks
5. Capacity Management
6. IT Financial Management
7. Service Level Management
8. Release and Deployment Management
9. Incident Management
10. Problem Management
11. Change Management
12. Service Asset and Configuration Management
13. Service Validation and Testing process
14. Service Design Processes

Summary

ITILv3 does not actually provide detailed guidance on security management but rather references ISO/IEC 27001 as the suggested path for designing and deploying an Information Security Management System. HP's Information Security Service Management Reference Model complements the HP Service Management Framework and is ideally suited and positioned to address the Information Security Management System within a Service Management implementation.

To learn more, visit www.hp.com/hps/security

4AA1-9600ENW, April 2008

invent

Technology for better business outcomes