

TRUSTED DATA CENTERS/TRUSTED DATA SERVICES (TDC/TDS)



Ronald P. Sherwin

Dr. Randy Broadwater

North American Public Sector
IT Infrastructure Solutions
Computer Sciences Corporation

14 February 2008

TABLE OF CONTENTS

1 Executive Summary	1
2 Introduction	2
3 Governance Requirements	3
4 Addressing the Challenge	6
5 Defining and Enforcing the Concept of “Trusted” Employees	19
6 Process Model	22
7 Conclusions	27
8 Recommendations	28
Appendix A: References	29

1 EXECUTIVE SUMMARY

How much trust is enough? Beyond the definitive levels of security that exist for national security systems, there is a tremendous information market (in both government and industry) that uses personal information. Information represents value; positive in that it characterizes a market of consumers, negative that its loss can severely impact the value and respect for a company. Within the Federal Government, protection of information has been built around the requirements of FISMA and the guidelines from NIST.

Secure environments cannot be purchased; they are constructed from standards and legal requirements. An organization's approach to security is an internal policy issue. Control tools are available to assist in managing and protecting an organization's sensitive information. From a federal perspective, providing secure environments to protect information is mandated under FISMA, NIST SP 800-53, and ISO 27001 and 27002. More definitive levels of trust exist through the use of ISO 270001/27002 — which encompasses many of the guidelines from the Secure Systems Engineering — Common Maturity Model (SSE-CMM).

CSC has a legacy of providing IT infrastructure solutions and is a managed services provider with decades of experience. Solutions are extensively researched, tested, and validated in our Centers of Excellence (CoEs) to enhance and expand our offerings in response to the dynamic needs of our public sector clients. CSC became the first worldwide business organization to achieve Level 3 certification against the SSE-CMM model in 1999 and the CSC Global Security Solutions (GSS), and the CSC-led Eagle alliance achieved Level 4 status in 2006.

While these efforts were directed towards classified systems, the potential exists to apply these best practices to civil government and commercial engagements, as well as planning for a trusted service offering. Our service delivery approach, guided by ITIL, focuses on a comprehensive (holistic) solution approach that ties together mission, costs, regulation, strategies, architectures, and services. Our paper provides an integrated approach, which incorporates both the mandatory requirements of the FISMA and NIST, along with the best practices recommended within ISO 27001/27002 and SSE-CMM.

2 INTRODUCTION

There is continuing concern on the part of the Congress and the American public about the ability of federal and state agencies to protect public information. Solutions to avoid data loss are difficult to specify, design, and build, and often require tailored solutions. These solutions must not only protect the information, but must also document the processes that prove they have complied with FISMA and other regulatory requirements. This is particularly difficult for smaller agencies faced with budget and skill constraints.

The risk to government information is real, and the threat is growing. The external risk is both electronic and physical. The internal threat is real as well. The threat from the insider can stem from financial temptation, carelessness, or anger/frustration. The modern data center cannot simply build walls to protect from the outside; it must implement similar protection from the insider as well.

Information now has tremendous economic power — both as a threat and an opportunity. Particularly in the private sector, there have been glaring examples of financial losses triggered by information losses for companies such as TJ Maxx and Societe Generale.

Congress is demanding that agencies clearly demonstrate value in their technical solutions. Government financial and human capital resources are shrinking. Protecting against internal and external threats often requires a wholesale change in business processes. Competing modernization programs makes any large, single capital outlay difficult to defend. Major agencies/departments (e.g., DoD) have declared their intent not to pursue large system integration efforts, but to acquire services.

Technology is rapidly changing the IT environment as well. Instantiations of Web-based services using a service oriented architecture (SOA) approach allows rapid implementation of new customer services, but opens up the door to rogue services and users, if proper governance is not provided. There is growing concern on the part of government customers over the physical surety of commercial facilities. This is a market that has emerged, is evident in the press each day, and needs a focused response to exploit this opportunity.

This paper will attempt to define a standardized process for establishing and validating a “trusted environment.” We will leverage existing technologies, solutions, and processes in a focused manner to develop an integrated “trust” methodology that can be applied in both the public and commercial sector. These trusted solutions could translate to a single “Trusted Data Center” providing customized service in a shared environment, or in the application of a single integrated methodology (“Trusted Data Services”).

Application of FISMA and the NIST Risk Management Framework¹ is insufficient to achieve this goal. Additional processes established in ISO/IEC 20000, ISO/IEC27001, ISO/IEC 27002, COBIT, the Common Criteria, and the SSE-CMM are needed to establish a complete framework. This paper attempts to bring these together in an integrated manner.

¹ NIST Risk Management Framework

3 GOVERNANCE REQUIREMENTS

International, national, and state government regulations can be a major challenge for today’s organizations. There are more than 100 such regulations in the United States alone, and that number continues to grow. These are in addition to numerous industry-specific mandates, international regulations, and standards. They are all designed to safeguard the confidentiality, integrity, and availability of electronic data from information security breaches. Meeting all of these in an integrated and efficient manner will establish a “trusted” environment.

The various publications fall into three areas. These areas are the legal criteria enforceable by law, the guidelines and regulations, and the accepted national and international standards.

Legal Requirements	Synopsis
The Federal Information Security Management Act (FISMA) of 2002	Enacted as Title III of the E-Government Act of 2002, FISMA imposes a mandatory set of processes that must be followed for all information systems used or operated by a U.S. Government federal agency or by a contractor or other organization on behalf of a U.S. Government agency.
Sarbanes-Oxley Act (SOX)	Every company that trades publicly on the U.S. stock exchange is regulated by the Securities and Exchange Commission (SEC). The act was created to restore public confidence by improving corporate accountability and governance.
Gramm-Leach-Bliley Act (GLBA)	Also known as the Financial Modernization Act of 1999, it is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
Health Insurance Portability and Accountability Act (HIPAA)	An act passed in 1996 with the primary goal of reforming the healthcare system. The goal was to improve privacy and security of patients’ medical information. This includes companies that handle medical records electronically. Noncompliance with HIPAA is punishable by fines, but is not as strictly enforced as GLBA noncompliance.
CA SB 1386	This is the first U.S. state law that directly addresses corporate responsibility over the loss of customer data. The California Senate Bill (CA SB) 1386, passed in July 2003, made it mandatory for companies doing business in California to notify their customers if their personal information had been compromised resulting from a computer security breach. Thirty-nine other states have similar legislation.

Table 1. Legal Requirements and Synopsis

Guidelines and Regulations	Synopsis
An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800-12	This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.
NIST Special Publication 800-64. System Considerations in the Information System Development Life Cycle	This guide presents a framework for incorporating security into all phases of the SDLC process, from initiation to disposal.
NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems	The purpose of this publication is to provide guidelines for the security certification and accreditation of information systems supporting the executive agencies of the Federal Government.
NIST Special Publication 800-53A,	This publication provides guidelines for developing security assessment plans and a comprehensive catalog of assessment procedures that can be

Guidelines and Regulations	Synopsis
Guide for Assessing the Security Controls in Federal Information Systems	used to determine the effectiveness of security controls in federal information systems.
NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklist Users and Developers	NIST SP 800-70 was developed to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.
SSE-CMM	SSE-CMM (Systems Security Engineering – Capability Maturity Model) approaches security from a different point of view. It is a process reference model that describes features of processes at different levels of maturity. Rather than looking at SSE-CMM as an overall system requiring full implementation, organizations can use the model as a benchmark to identify current status across a number of information security processes and provide a road map for future improvements.

Table 2. Guidelines, Regulations, and Synopsis

National Standards	Synopsis
Security of Federal Automated Information Resources (OMB Circular A-130, Appendix III)	States that each agency’s program shall implement policies, standards, and procedures which are consistent with Government wide policies, standards, and procedures issued by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management.
Homeland Security Presidential Directive 12 (HSPD-12)	Establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.
Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors	Requires that the digital certificates incorporated into the Personal Identity Verification (PIV) identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
COBIT	COBIT is a mature IT governance standard and focuses on controls that provide management with assurance that IT is operating in a controlled manner. With the introduction of Sarbanes-Oxley legislation in the United States, elements of COBIT have been widely adopted to assist in providing assurance of the effectiveness of internal controls over financial reporting. Like ITIL, COBIT can be used to drive some information security improvements, though its primary focus lies elsewhere. COBIT was released and used primarily by the IT community, and has become the internationally accepted framework for IT governance and control.

Table 3. National Standards and Synopsis

International Organization for Standardization (ISO)

To achieve compliance with ISO guidelines, organizations must establish an effective system to facilitate the management of its core processes. Processes such as customer satisfaction, product quality, compliance, or environmental processes all require effective controls to meet ISO standards. Most forward-thinking companies have automated critical procedures to help increase operational efficiency and reduce error, using the latest technology solutions available on the market.

International Standards	Synopsis
ISO 9000	The quality management family is defined by ISO 9000. The ISO 9000 series of standards is the most widely accepted quality assurance model in the world.
ISO 14000	Environmental management is addressed through the ISO 14000 family. The goal of this body of standards is to help minimize harmful effects on the environment caused by its activities, and to achieve continual improvement of its environmental performance.
ISO 20000	<p>This new standard is based on the British standard BS 15000 and is closely aligned with the IT Infrastructure Library (ITIL®). ISO 20000 is a code that provides a yardstick for measuring and validating an organization's success in implementing best practices as defined by ITIL.</p> <p>ISO 20000 is really two specifications, ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005; we refer to them as ISO 20000-1 and 20000-2. ISO 20000-1 is the specification for Service Management. It defines the processes and provides assessment criteria and recommendations for those responsible for IT Service Management. Organizational certification uses this section.</p> <p>ISO 20000-2 documents a "code of practice" that explains how to manage IT with regard to ISO 20000-1 audits. Both ISO 20000-1 and ISO 20000-2 are directly derived from ITIL best practice.</p>
ISO 27001	<p>ISO 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005 — Information Technology — Security Techniques — Information Security Management Systems — Requirements, but it is commonly known as "ISO 27001." It is intended to be used in conjunction with ISO/IEC 27002. It is derived from BS 7799 – Part 2, which became ISO/IEC 27001 in November 2005.</p> <p>Increasing IT security requires best practices, such as ITIL, ISO/IEC 27001, and ISO/IEC 27002. Creating a more mature IT security environment requires the complementary and overlapping IT governance frameworks such as ITIL, ISO/IEC 27001, and ISO/IEC 27002. By following these systematic approaches to IT, an organization can adopt the security regime that best fits their organization.</p>
ISO 27002	The Code of Practice for Information Security Management — lists security control objectives and recommends a range of specific security controls. It was derived from (British Standard) BS 7799 – Part 1, which became ISO/IEC 17799, and was renamed to ISO/IEC 27002 in July 2007.
Common Criteria for Information Technology Security Evaluation	The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140-2, Common Criteria does not provide a list of product security requirements or features that products must contain. Instead, it describes a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard manner.

Table 4. International Standards and Synopsis

4 ADDRESSING THE CHALLENGE

Developing an integrated “trust” methodology that provides a common trust process acceptable and agreed upon by more than one party is a challenge. Technologies have existed for several years to provide for a trusted environment, but trust takes on different meanings to different parties. Security, and hence trust, cannot be solved by technology alone — security policies, establishing a common federated trust environment, and agreement on how to verify information requests are the road blocks.

Industry best practices have long been viewed as the logical approach to deliver goods or services to a customer base whether that base is internal, external, or both. The Information Technology Infrastructure Library (ITIL) takes this approach progressively one step further (i.e., successful innovations gradually become best practices, best practices quickly become good practices, which become commodities, generally accepted principles, or regulatory requirements²).

Following a single legal requirement, standard, framework, or guideline alone will not deliver a secure computing environment. Therefore, we draw from the guidance of An Introduction to Computer Security: The NIST Handbook (particularly chapter 7, which evolved into The Risk Management Framework); the industry standards of ISO/IEC 20000, 27001, and 27002; COBIT; the Common Criteria; the SSE-CMM; and ITIL to recommend best practices, processes, and metrics to construct a methodology for implementing Trusted Data Centers/Trusted Data Services.

By taking the position that Trusted Data Centers/Trusted Data Services are innovative solutions delivered as services to a customer, they then fall under the Service Life Cycle. The Service Life Cycle is an approach to IT Service Management that emphasizes the importance of coordination and control across the various functions, processes, and systems necessary to manage the full life cycle of that service.

The present security model focuses primarily on causes of security problems and the addition of processes to deal with the problems. This model operates by following trends, which may result in resources being allocated to security solutions and sites that are still vulnerable to compromise.

The security of an organization is a process, not a technology. In most cases, security professionals react to security flaws instead of examining the events that caused them. This reaction is fundamentally flawed; it tends to deal with the effects and fails to reveal the root cause that triggered the event.

A trusted solution is achieved through the proper modeling of the environment. A complete design requires taking a holistic view, one that understands all of the interacting systems and the environment that supports this whole system. The systems-design process questions the assumptions that surround the system and that system’s environment.

Most systems fail due to problems with the requirements definition. Once the requirements are defined, architecting the system can begin. Systems engineering recognizes that the design process is an iterative process; this helps to revisit assumptions about the environment and other related systems while designing the system.

² ITpreneurs, Service Management as a Practice, Nederland BV 2007

By understanding how the system and the environmental boundaries are interconnected, the framework for the system begins to take shape. The support for other systems can be identified, as well as how they need to be supported. When problems surface, they can be traced to poorly defined requirements or misconceptions of how they should be implemented. Well-defined system requirements lead to a better understanding of the systems environment.

Once the requirements are defined, the activities required to meet them can be addressed. This area provides the necessary parameters for the systems architecture and establishes the metrics to measure performance.

By using the systems approach to security, the enterprise is concerned with the overall purpose and function of the system, not just the security aspects. The focus is more on the procedures, which enforce well-defined and realistic requirements.

While ITIL provides the processes to deliver a secure system as a service, the design of a secure system is an engineering problem. The systems engineering approach, combined with the guidance from SSE-CMM, provides a proven framework for defining and building secure systems. This framework proves that security can be defined as a system, and ITIL provides the processes to deliver the secure system as a service. This interaction results in a secure system where the qualities exceed the sum of the system components.

Designing a secure system requires attention in four areas: 1) defining system/environmental boundaries, 2) establishing systems objectives, 3) determining program structure and activities, and 4) defining the system's management. All four of these areas can be addressed by the ITIL service strategy.

ITIL and COBIT are not primarily focused on security; however, both contain processes that address security issues. While the architecture of the ITIL core is based on the Service Life Cycle, it contains processes that address information security management. COBIT focuses on controls that provide management with assurance that IT is operating in a controlled manner. With the introduction of Sarbanes-Oxley legislation in the United States, elements of COBIT have been widely adopted to assist in providing assurance of the effectiveness of internal controls over financial reporting. Like ITIL, COBIT can be used to drive some information security improvements, though its primary focus lies elsewhere.

Other standards are entirely given over to security, such as a number of NIST standards and ISO 27001 and 27002. The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. In 2002, the Federal Information Security Management Act (FISMA) set aside money for NIST to develop new standards for securing government agencies. The British government originally developed ITIL for similar reasons.

ISO/IEC 20000 (which replaces BS15000) defines the requirements for an IT Service Management System. It sets out the main processes to deliver IT services effectively. The standard itself aligns with ITIL, and specifies key process groups. The standard is comprised of two volumes:

1. ISO 20000-1 is the specification, providing recommendations for those responsible for IT Service Management. It defines the overall processes.

2. ISO 20000-2 is a code of practice, describing specific best practices for the processes within ISO 20000-1.

Figure 3 shows the relationships between ISO 20000 and ITIL processes.

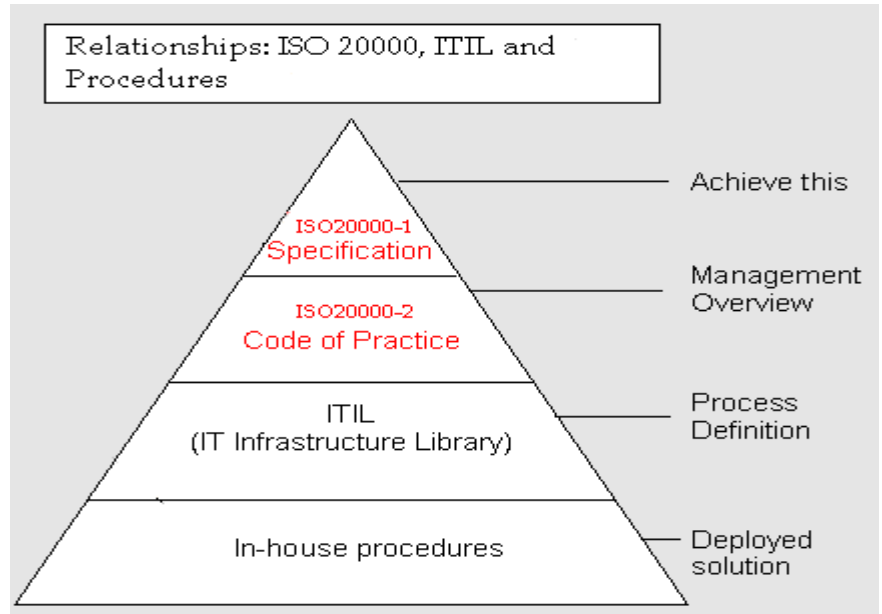


Figure 1. ISO 20000, ITIL, and Process Relationships

The International Organization for Standardization (ISO) is the world’s largest developer of standards. This organization has released over 15,000 standards in total, including a number related to information security. ISO 27001 consists of very short control statements across many areas of security. Where ISO 27001 helps companies identify what they should do, ISO 27002 provides additional guidance regarding what companies need to think about as they work to achieve appropriate levels of security.

The intention of ISO 27001 is to create a level playing field that can be applied worldwide. Benchmarking against it can be a useful indicator of core security controls and practices, and some ISO 27001 controls address areas frequently requested by auditors under Sarbanes-Oxley Section 404 and other regulatory requirements. It is intended to be used in conjunction with ISO/IEC 27002, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls.

Regulatory compliance provides a number of direct, practical reasons for implementing an information security policy and information security management system (ISMS) that is capable of being independently certified as compliant with the new international information security standard ISO/IEC 27001:2005. Examples:

- An ISO/IEC 27001-certificated ISMS will ensure that your company is in compliance with the whole range of information-related legislation, including (as applicable) HIPAA, GLBA, SB 1386 and other state breach laws, PIPEDA, FISMA, and EU Safe Harbor regulations

- An ISO/IEC 27001-certificated ISMS will ensure that your company has in place the general control environment on which a successful SOX s404 report depends
- A certificate tells existing and potential customers as well as regulators that your company has defined and put in place effective information security processes, thus helping create a trusting relationship.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad:

Confidentiality (ensuring that information is accessible only to those authorized to have access)

Integrity (safeguarding the accuracy and completeness of information and processing methods)

Availability (ensures that authorized users have access to information and associated assets when required)

ITIL Information Security Management and Availability Management align to this security management recommendation.

SSE-CMM (Systems Security Engineering – Capability Maturity Model) approaches security from a different point of view. It is a process reference model that describes features of processes at different levels of maturity. Rather than looking at SSE-CMM as an overall system requiring full implementation, organizations can use the model as a benchmark to identify current status across a number of information security processes and provide a road map for future improvements.

The SSE-CMM³ initiative started under NSA-sponsorship in 1993, with the intent of developing and implementing security engineering processes similar to those being developed for software development (Software Engineering Institute [SEI] CMM). The intent of the SSE-CMM was to:

- Serve as a tool for organizations to evaluate their security engineering practices
- Develop methods that can be used to certify that specific levels have been reached
- Most importantly, serve as the basis for customers to determine a provider's security engineering capabilities

The SSE-CMM is a process model and was first applied by CSC in its work in support of classified systems. It is, however, easily extensible to other information systems (such as financial, contractual, personal) where information has value that must be protected. In the market-driven economy, products rarely come to market with the specific security attributes needed for each product. The SSE-CMM provides the process for supplementing these capabilities in the actual IT implementation. There are five levels in the maturity model.

³ www.sse-cmm.org

CMM – Behavioral Characterization of the Maturity Levels

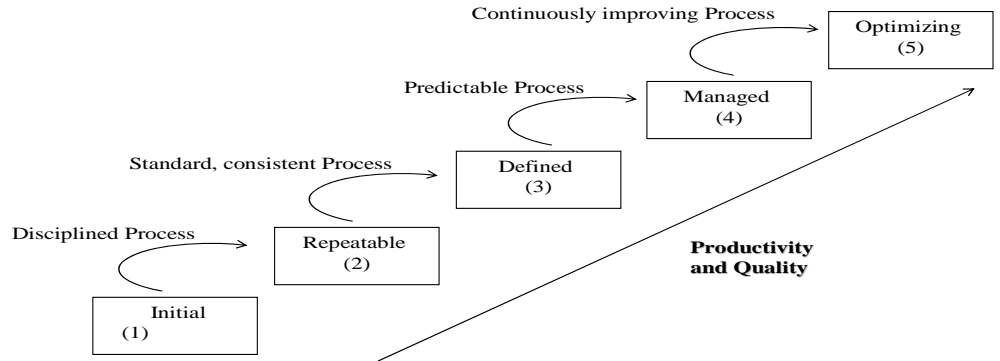


Figure 2. SSE-CMM Diagram⁴

CSC became the first worldwide business organization to achieve Level 3 certification against the SSE-CMM model in 1999, and CSC Global Security Solutions (GSS) and the CSC-led Eagle alliance achieved Level 4 status in 2006. While these efforts were directed towards classified systems, the potential exists to apply these best practices to civil government and commercial engagements, as well as planning for a trusted service offering. All of the IT Security Guidance documents cover essentially the same material. However, they do it in different ways and they place different emphasis on various topics. In addition, they include different material germane to the particular culture, jurisdiction, and domain for which they are written. The advantages of one are only equaled by the advantages of another within their target area of usage.

All of the IT Security Guidance documents can be used with the SSE-CMM. All of the Process

Areas of the SSE-CMM can be (relatively) easily mapped to the topic areas of the different IT Security Guidance documents. Conversely, all of the topic areas of the various IT Security Guidance documents can be related to the Process Areas of the SSE-CMM.

The ISO/IEC standards and the SSE-CMM model mentioned above are tightly coupled with and mirror the ITIL functions and processes. Table 5 below shows the mapping between these publications and Figure 3 graphically depicts the overlap of these standards and frameworks.

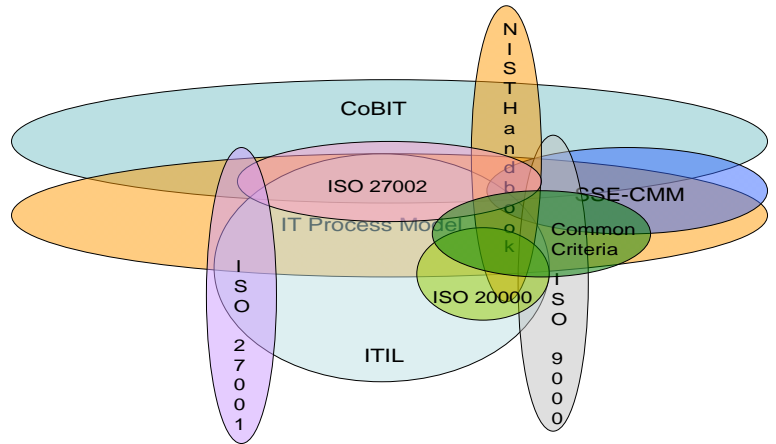
SSE-CMM PA = Process Area	ISO/IEC 27001	ISO/IEC 27002	ITIL V2	An Introduction to Computer Security: The NIST Handbook
PA 01 – Administer Security Controls	Section 5, Personnel Security Section 6, Communications and operations Management	Chapter 2, Security Policies Chapter 6, Communications and Operations Chapter 9, IS Acquisition,	Information Security Management, Capacity Management, Availability Management, Service Level Management, Release Management	Chapter 10, Personnel/User Issues Chapter 14, Security Considerations in Computer Support

⁴ www.sse-cmm.org

SSE-CMM PA = Process Area	ISO/IEC 27001	ISO/IEC 27002	ITIL V2	An Introduction to Computer Security: The NIST Handbook
		Section 8, Systems Development and Maintenance	Development and Maintenance	
PA 02 – Assess Impact	Introduction	Chapter 1, Risk Assessment and Treatment	IT Service Continuity Management, IT Security Management	Chapter 7, Computer Security Risk Management
PA 03 – Assess Security Risk	Introduction	Chapter 1, Risk Assessment and Treatment	IT Service Continuity Management, IT Security Management	Chapter 7, Computer Security Risk Management
PA 04 – Assess Threat	Introduction	Chapter 1, Risk Assessment and Treatment	IT Service Continuity Management, IT Security Management	Chapter 7, Computer Security Risk Management Chapter 4, Common Threats
PA 05 – Assess Vulnerability	Introduction	Chapter 1, Risk Assessment and Treatment	IT Service Continuity Management, IT Security Management	Chapter 7, Computer Security Risk Management
PA 06 – Build Assurance Argument	Section 10, Compliance	Chapter 12, Compliance	Availability Management, Capacity Management	Chapter 9, Assurance
PA 07 – Coordinate Security	Section 2, Security Organization Section 6, Communications and operations Management	Chapter 2, Security Policies Chapter 3, Organization Chapter 6, Communications and Operations	IT Security Management, Availability Management, Capacity Management	Chapter 6, Computer Security Program Management
PA 08 – Monitor Security Posture	Section 10, Compliance	Chapter 12, Compliance	Incident Management, Problem Management, Service Level Management, Capacity Management, Availability Management	Chapter 12, Computer Security Incident Handling Chapter 18, Audit Trails
PA 09 – Provide Security Input	Section 1, Security Policy Section 3, Asset Classification and Control	Chapter 2, Security Policies Chapter 4, Asset Management	Configuration Management, Asset Management, IT Security Management	Chapter 5, Computer Security Policy Chapter 13, Awareness, Training, and Education Chapter 15, Physical and Environmental Security
PA 10 – Specify Security Needs	Section 1, Security Policy Section 7, Access Control Section 8, Systems Development and Maintenance Section 9, Business Continuity Planning	Chapter 2, Security Policies Chapter 8, Access Control Chapter 9, IS Acquisition, Development and Maintenance Chapter 11, Business Continuity Management	IT Service Management, Business Service Management, IT Service Continuity Management, Release Management	Chapter 8, Security and Planning in the Computer System Life Cycle Chapter 11, Preparing for Contingencies and Disasters Chapter 16, Identification and Authentication Chapter 17, Logical Access Control Chapter 19, Cryptography
PA 11 – Verify and Validate Security	Section 10, Compliance	Chapter 12, Compliance	Service Level Management, Availability Management, IT Security	Chapter 8, Security and Planning in the Computer System

SSE-CMM PA = Process Area	ISO/IEC 27001	ISO/IEC 27002	ITIL V2 Management	An Introduction to Computer Security: The NIST Handbook Life Cycle 18, Audit Trails

Table 5. ITIL V2 Process Mapping to Other Standards and Frameworks



How the standards overlap

Figure 3. Standards and Framework Overlap

While Table 5 shows a cross-mapping of the standards and frameworks, it is not intended to be nor is it claimed to be the definitive mapping. Each chapter, section, process area, and ITIL process can be further matrixed against the subsections under their respective documents.

Process definitions describe actions, dependencies, and sequence and have the following characteristics:

- Processes are measurable — we are able to measure the process in a relevant manner. It is performance driven.
- They have specific results — the reason a process exists is to deliver a specific result. This result must be individually identifiable and countable.
- Processes have customers — every process delivers its primary results to a customer or stakeholder. They may be internal or external to the organization but the process must meet their expectations.
- They respond to specific events — while a process may be ongoing or iterative, it should be traceable to a specific trigger.

The ISO/IEC standards, the NIST Risk Management Framework, and the SSE-CMM all address security risk to an organization and help establish security metrics. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached. They are useful to senior

management, decision makers, users, administrators, or other stakeholders who face a difficult and complex set of questions regarding security, such as:

- How much money/resources should be spent on security?
- Which system components or other aspects should be targeted first?
- How can the system be effectively configured?
- How much improvement is gained by security expenditures, including improvements to security processes?
- How do we measure the improvements?
- Are we reducing our exposure?

ITIL Version 3 aligns well with the SSE-CMM process model of system life-cycle development for secure systems. With questions like those posed above, the Service Strategy volume defines the risk, the service model, and process steps required to answer these questions and the four areas that require attention under the systems engineering approach.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140-2, Common Criteria does not provide a list of product security requirements or features that products must contain. Instead, it describes a framework in which computer system users can *specify* their security requirements, vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard manner.

The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system — the security controls necessary to protect individuals and the operations and assets of the organization.

It is impossible to construct effective security architectures without conducting an initial risk assessment. A risk assessment is a high-level, mandatory exercise that varies in complexity based on the size and business profile of an organization. The scope of the assessment includes an assessment of the people, processes, and technology required to effectively manage the business.

From this assessment, a risk management framework is developed. A comprehensive risk assessment includes the following key steps:

- Identify all key requirements
- Identify those that apply to your staff, processes, and systems
- For each area of potential risk, identify the nature of that risk as it applies to the firm
- Use a risk rating scale, score the risk, and record it

- For each identified risk, prescribe a mitigating, controlling, or corrective action, and timescale for completion (including assigning it to a person or function)

The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, and regulations. The NIST Handbook: An Introduction to Computer Security⁵ (Chapter 7) contains the following activities related to managing security risk (also known as the NIST Risk Management Framework), is paramount to an effective information security program, and can be applied to both new and legacy information systems within the context of the service life cycle⁶ (ITIL):

- Step 1: Categorize the information system and the information resident within that system based on impact. FIPS 199 and NIST SP 800-60
- Step 2: Select an initial set of security controls for the information system based on the FIPS 199 security categorization and apply tailoring guidance, as appropriate, to obtain a starting point for required controls. FIPS 200 and NIST SP 800-53
- Step 3: Supplement the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances. NIST SP 800-53 and SP 800-30
- Step 4: Document the agreed-upon set of security controls in the system security plan including the organization's justification for any refinements or adjustments to the initial set of controls. NIST SP 800-18
- Step 5: Implement the security controls in the information system.
- Step 6: Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **NIST SP 800-53A**
- Step 7: Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable. NIST SP 800-37
- Step 8: Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis. NIST SP 800-37 and SP 800-53A

⁵ An Introduction to Computer Security: The NIST Handbook, SP 800-12

⁶ Information Technology Infrastructure Library (ITIL) Version 3, September 2007

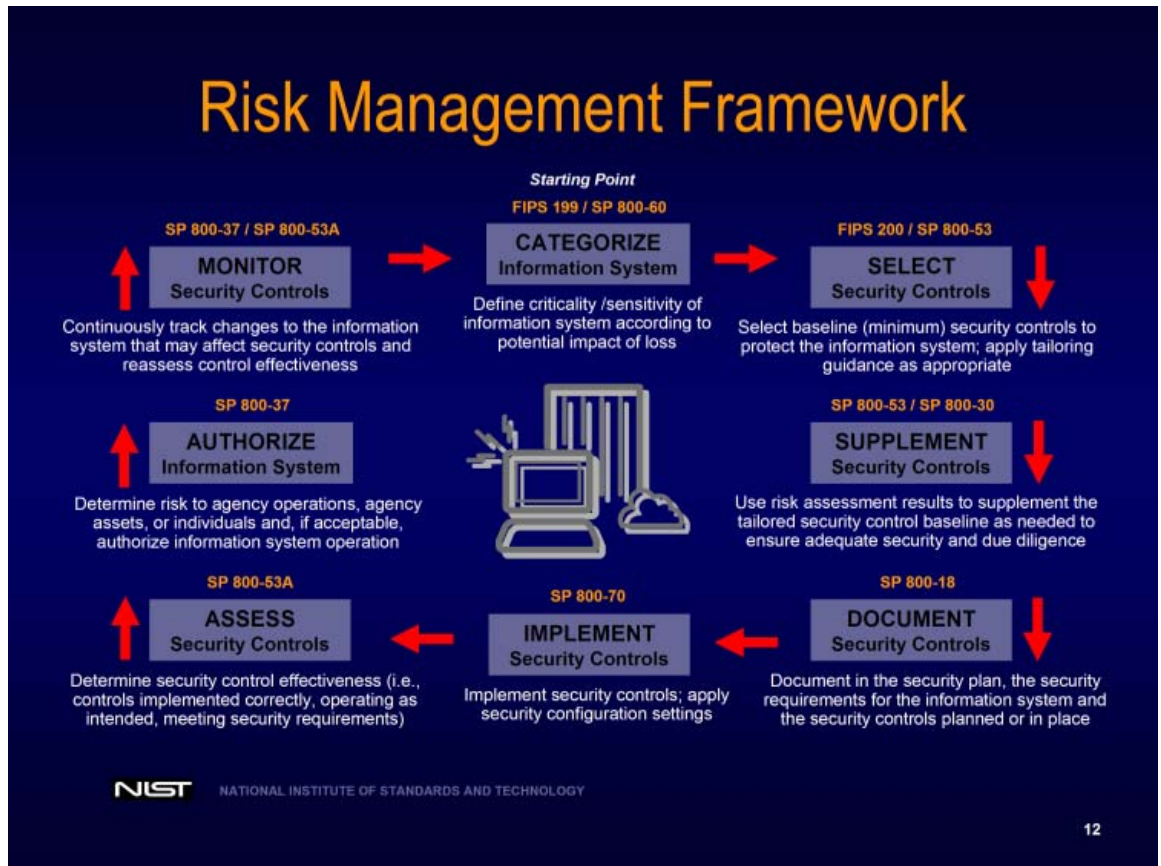


Figure 4. NIST Risk Management Framework⁷

The management and mitigation of risk in any endeavor carries with it a dollar value. When it comes to security risk, the solution converges to how much money an organization is willing to spend to protect its collective resources.

Step 1. Define (Categorize) the information system (i.e., Top Secret, Secret, Unclassified but Sensitive, or some comparable domain distinction) based on the impact of compromising that information.

Architecting a trusted environment from scratch is a good time to consider the operating system that will deliver the information. If a legacy system is to be tightened down to handle security data, then the operating system again deserves a closer look.

As part of its Information Assurance mission, the National Security Agency has long been involved with the computer security research community in investigating a wide range of computer security topics including operating system security. Recognizing the critical role of operating system security mechanisms in supporting security at higher levels, researchers from NSA’s Information Assurance Research Group have been investigating an architecture that can provide the necessary security functionality in a manner that can meet the security needs of a wide range of computing environments.

End systems must be able to enforce the separation of information based on confidentiality and integrity requirements to provide system security. Operating system security

⁷ <http://csrc.nist.gov/groups/SMA/fisma/documents/risk-framework-2007.pdf>

mechanisms are the foundation for ensuring such separation. Unfortunately, existing mainstream operating systems lack the critical security feature required for enforcing separation: mandatory access control. As a consequence, application security mechanisms are vulnerable to tampering and bypass, and malicious or flawed applications can easily cause failures in system security.

The results of several previous government research projects in this area have been incorporated by industry in a security-enhanced Linux system. This version of Linux has a strong, flexible, mandatory access control architecture incorporated into the major subsystems of the kernel. The system provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications. Similar security extensions have been applied to Solaris as well.

Linux was chosen as the platform for this work because its open development environment provided an opportunity to demonstrate that this functionality can be successful in a mainstream operating system and, at the same time, contribute to the security of a widely used system. Additionally, the integration of these security research results into Linux may encourage additional operating system security research that may lead to additional improvements in system security. Security-enhanced Linux is not an attempt to correct any flaws that may currently exist in Linux. Instead, it is simply an example of how mandatory access controls that can confine the actions of any process, including a super user process, can be added into Linux.

The security mechanisms implemented in the system provide flexible support for a wide range of security policies. They make it possible to configure the system to meet a wide range of security requirements. The release includes a general-purpose security policy configuration designed to meet a number of security objectives as an example of how this may be done. The flexibility of the system allows the policy to be modified and extended to customize the security policy as required for any given installation.

Examples of current trusted operating systems are:

- Red Hat Enterprise Linux v.5
- Trusted Solaris v8
- XTS-400 STOP 6.0
- SE Linux
- IBM AIX 5L
- IBM zOS

Step 2. Determine (Select) an initial set of security controls for the information system to obtain a starting point for required controls.

Selecting a set of security controls takes into account the policy definitions, edge equipment required to protect the information, firewalls, and vendor tools, such as identity management software, access control, authentication, entitlement, etc. Security controls aimed at inside or employee management are addressed in Section 4.

ISO/IEC 27002, the Code of Practice for Information Security Management, sets forth a set of security control objectives and recommends a range of specific security controls. Organizations that implement an Information Security Management System (ISMS) in

accordance with the best-practice advice in ISO/IEC 27002 are likely to simultaneously meet the requirements of ISO/IEC 27001, but certification is entirely optional (unless mandated by the organization’s stakeholders).

The Control subprocess organizes and manages the Security Management process itself. The Control subprocess defines the processes, the allocation of responsibility, the policy statements, and the management framework.

The Security management framework defines the subprocesses for the development of security plans, the implementation of the security plans, the evaluation, and how the results of the evaluations are translated into action plans.

The activities that take place during this process are summed up in Table 6.

Activities	Sub-Activities	Descriptions
Control	Implement policies	This process outlines the specific requirements and rules that have to be met in order to implement security management. The process ends with POLICY STATEMENTS.
	Setup the security organization	This process sets up the organizations for information security; for example, in this process the structure for the responsibilities are set up. This process ends with SECURITY MANAGEMENT FRAMEWORK.
	Reporting	In this process the whole targeting process is documented in a specific way. This process ends with REPORTS.

Table 6. (Sub) Activities and Descriptions Control Subprocess ITIL Security Management

Step 5. Implement the security controls in the information system.

The Implementation subprocess makes sure that all measures, as specified in the plans, are properly implemented. During the Implementation subprocess, no (new) measures are defined or changed. The definition or change of measures will take place in the Plan subprocess in cooperation with the Change Management Process.

The activities that take place in the implementation process are summed up in Table 7.

Activities	Sub-Activities	Descriptions
Implement	Classify and Manage IT Applications	Process of formally grouping Configuration Items by type (e.g., software, hardware, documentation, environment, application) Process of formally identifying changes by type (e.g., project scope change request, validation change request, infrastructure change request) This process leads to ASSET CLASSIFICATION AND CONTROL DOCUMENTS.
	Implement Personnel Security	Measures are adopted here in order to give personnel safety and confidence and measures to prevent a crime/fraud. The process ends with PERSONNEL SECURITY.
	Implement Secure Management	In this process specific security requirements and/or security rules that must be met are outlined and documented. The process ends with SECURITY POLICIES.
	Implement Access Control	In this process specific access security requirements and/or access security rules that must be met are outlined and documented. The process ends with ACCESS CONTROL.

	Reporting	In this process the whole “implement as planned” process is documented in a specific way. This process ends with REPORTS.
--	-----------	---

Table 7. (Sub) Activities and Descriptions Implementation Process ITIL Security Management

Step 6. Evaluate (Assess) the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The evaluation of the implementation and the plans is very important. The evaluation is necessary to measure the success of the implementation and the Security plans. The evaluation is also very important for the clients (and possibly third parties). The results of the Evaluation subprocess are used to maintain the agreed measures and the implementation itself. Evaluation results can lead to new requirements and lead to a request for change. The request for change is then defined and it is then sent to the Change Management process.

Mainly there are three sorts of evaluations; the self-assessment, the internal audit, and the external audit.

The self-assessment is mainly carried out in the organization of the processes. The internal audits are carried out by internal IT auditors, and the external audits are carried out by external, independent, IT auditors. An evaluation based on the communicated security incidents will also take place. The most important activities for this evaluation are the security monitoring of IT systems, verifying if the security legislation and the implementation of the security plans are complied with, and tracing and reacting to undesirable use of IT supplies.

The activities that take place in the evaluation process are summed up in Table 8.

Activities	Sub-Activities	Descriptions
Evaluate	Self-Assessment	In this process an examination of the implemented security agreements is done by the organization of the process itself. The result of this process is SELF- ASSESSMENT DOCUMENTS.
	Internal Audit	In this process an examination of the implemented security agreements is handled by an internal EDP auditor. The result of this process is INTERNAL AUDIT.
	External Audit	In this process an examination of the implemented security agreements is handled by an external EDP auditor. The result of this process is EXTERNAL AUDIT.
	Evaluation Based on Security Incidents	In this process an examination of the implemented security agreements is done based on security events, which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. The result of this process is SECURITY INCIDENTS.
	Reporting	In this process the whole Evaluate implementation process is documented in a specific way. This process ends with REPORTS.

Table 8. (Sub) Activities and Descriptions Evaluation Subprocess ITIL Security Management

Step 7. Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.

Step 8. Monitor and assess security controls in the information system on a continuous basis. It is necessary for security controls to be monitored. Because of changes in the IT infrastructure and changes in the organization itself, security risks are bound to change over time. By monitoring the security controls, service level agreements and security plans can be modified accordingly.

An area of critical importance for an organization is to provide security controls and tools that protect sensitive information, not only from outside compromise, but from insider breaches as well. The following section, Section 5, will address this area in greater detail.

5 DEFINING AND ENFORCING THE CONCEPT OF “TRUSTED” EMPLOYEES

Trust is an essential pillar of the employer/employee relationship, and no organization wants to deliberately foster a workplace environment of suspicion and surveillance. While technology has solved many of the problems posed by hackers and viruses, security experts are the first to admit that there are few technologies that can protect against a trusted user with a bad habit.

Short of stationing a security guard at every desk, how does an organization ensure that its trusted employees and contractors do not accidentally or deliberately misuse the very business processes that they have been given trusted access to? The recent Societe Generale trading problems are a glaring (multibillion dollar) example of such misuse.

One answer is a policy enforcement solution that aims to securely manage the behavior of trusted users, whether they like it or not. Policies based on security controls can be established to address: 1) authentication, 2) protect data, 3) provide network attestation and platform measurement, 4) address application protection, and 5) ensure content protection.

These policy-based security controls are selected and applied based on a risk assessment of the information system. The risk assessment process identifies system threats and vulnerabilities. Then, security controls are selected to reduce (mitigate) the risk.

Security controls are measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability (C.I.A.) of the information system. Note that the terms “safeguard” and “countermeasure” are sometimes used as synonyms for security control.

“Trust, but verify.” — Ronald Reagan

Employee management security controls provide the “verify” for trusted employees and mostly fall into the administrative control category. Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization’s sensitive information.

Today, most corporate networks are focused on protecting their resources against outsider threats coming from the Internet. Security is focused on establishing a perimeter between the private internal network and the public network by enforcing access-control strategies and securing data as it flows outwards to the Internet. They design their networks using

firewalls and Intrusion Detection Systems (IDS) to prevent hackers from entering inside their private network. The problem with this network design is: “What if the attack comes from the inside the network?”

This type of attack is referred to as an insider attack, where the attack emanates from inside the network. An insider is normally a current employee, a former employee, or an outside contractor working for the company. It can also be a person working for or trusted by the victim that has access to confidential information within the company. Insiders most likely have specific goals and objectives to disrupt or damage a company’s network operations. An insider attack can affect all components of computer security. They can attack the confidentiality, integrity, and availability of network resources. Insider attacks are becoming more common and more damaging. According to the CSI/FBI 2005 Computer Crime and Security Survey, most organizations had from one to 10 insider attacks in the past 3 years, averaging 56 percent of all attacks. The following was found in another study conducted by the Secret Service last year.⁸

- 80 percent of insiders who launch attacks had exhibited negative behavior previously.
- 92 percent had a demotion, transfer, termination or warning.
- 86 percent were IT workers and of those, 38 percent were system administrators.
- 96 percent were male and almost one-third had a criminal record.
- 57 percent were perceived to be disgruntled.
- Revenge was the most common motive for attack.

In a recent study conducted by the Ponemon Institute, they found that nearly 60 percent of U.S.- based businesses and government agencies believe they are unable to effectively assess or quantify insider threat risks within their organizations, leaving them open to breaches of private data, failed audits, and potential fraud.⁹ Insider threats are particularly obscure and difficult to protect against. Not only do the attackers have immediate access to the network, but they require such access in order to perform their daily duties. It is human nature for us to trust people who work within the company and not trust people who do not. Since the attacker has access to user accounts or e-mail, they most likely have access to private information. Furthermore, insider threats may not receive the same amount of attention as outsider threats because of the privacy restrictions that are present in government work environments. Due to the high level of legal and ethical issues, employers may not be as aggressive in their oversight and compliance efforts regarding insider security threats.

In the past, many employees would give out access rights based on a peer’s profile, but it is not efficient, nor is it prudent from a security and regulations standpoint to give employees more access than they need to applications and data. A company should only provide the minimum access employees need to do their job effectively and only for as long as they need to do that job.

⁸ Gaudin, Sharon. “Study Highlights Insider Threats.” Information Week. 25 Aug. 2006. 21 May 2007 <<http://www.informationweek.com/showArticle.jhtml?articleID=192300421>>

⁹ Ponemon Institute Study. 5 March. 2007. 21 May 2007 <http://www.ponemon.org/press/SailPoint_IDM_Survey_FINAL1.pdf>

Five years ago software that could handle access rights to this granularity did not exist. Today entitlement management technology can implement policies that say who can have access to what and at what time and in what context. The level of controls can be very deep and broad. Entitlement management products typically pull identity management data from Lightweight Directory Access Protocol (LDAP), Active Directory, or human resources directories, and integrate with identity- and access-management tools to build entitlement policies.

Implementing application data security and entitlement management tools enforces corporate security policies without the appearance of fostering a workplace environment of suspicion and surveillance.

6 PROCESS MODEL

This paper has developed a process model that draws the best practices and processes from the Information Technology Infrastructure Library (ITIL), An Introduction to Computer Security: The NIST Handbook, the already described ISO/IEC standards, COBIT, SSE-CMM, and the Common Criteria.

The developed process for delivering a trusted environment has been put forth as a service delivery offering and contains built-in methodologies that are derived from the Service Life-Cycle Management model. Figure 5 below illustrates the secure environment process model.

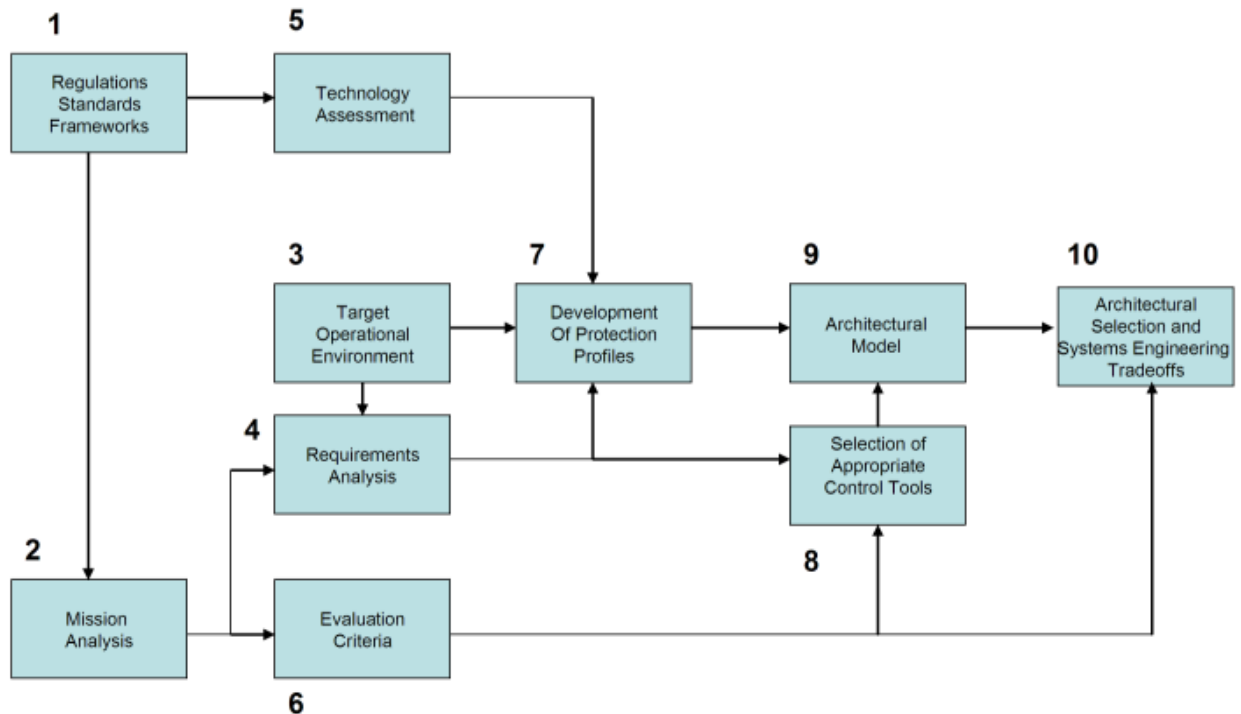


Figure 5. Secure Environment Process Model

Each of the boxes in the above model is numbered to identify which subprocess is to be completed prior to beginning the next subprocess.

Box 1, Regulations, Standards, and Frameworks, requires that the high-level governance documentation be reviewed. We have identified in previous discussion which documents provide the best practices, establish metrics, and define processes for the design.

Box 2, Mission Analysis, is the process by which the operating plan and contingency plans are developed. It includes organizing the team to meet the mission objectives, allocating resources to perform the critical tasks, and monitoring the team and the environment to adjust resources as necessary. To be effective it must at a minimum:

- Define tasks based on mission requirements
- Question data or ideas as they relate to mission accomplishment
- Discuss long- and short-term plans for the mission

- Identify the impact of potential hazards and unplanned events on the mission
- Structure tasks, plans, and objectives related to the mission
- Thoroughly critique existing plans for potential problems

From an ITIL v3 perspective, this is the Service Strategy; all aspects related to the tasks that make up the operating plans, including organizational risk, take place in this subprocess.

Box 3, Target the Operational Environment. The Common Criteria evaluation is a framework for evaluating IT products and systems that is recognized by governments and IT professionals around the world as a critical measure of the quality of an information technology security product. Regardless of the classification level of the operating environment, security control tools can be evaluated against this framework to ensure their suitability for the classification level being used. Following the guidance from the NIST Risk Management Framework provides insight into what is appropriate for this process.

Box 4, Requirements Analysis, states that requirements must be actionable, measurable, testable, related to identified business needs or opportunities, and defined to a level of detail sufficient for system design. Although this process takes place in the ITIL v3 Service Strategy process, the output from this process is a direct input to the Service Design process. The ISO/IEC 27001 Section 8, ISO/IEC 27002 Chapter 9, NIST Handbook Chapter 14, and the ITIL processes of Information Security Management, Capacity Management, Availability Management, Service Level Management, and Release Management all provide detailed guidance in performing this task.

Best practices take the composed list of requirements merely as clues and repeatedly ask “why?” until the actual business purposes are discovered. Results from completing the processes of Box 2 and Box 3 provide input to this process.

Box 5, Technology Assessment, is the study and evaluation of new technologies and how they may be leveraged into existing or new systems. Not every emerging or slightly new technology may be applicable to an organization’s business or operational goals. A careful evaluation must be conducted to capture return on investment numbers: “Is there a new risk introduced by the technology as it is leveraged into legacy systems?”, “What is the learning curve for end users?”, and “What is the impact on IT resources that have to manage and maintain the technology?” Answers to these questions will provide a moving-forward plan that affects the entire organization, and due diligence is the theme.

Box 6, Evaluation Criteria. The Mission Analysis of Box 2 provides the criteria necessary to establish evaluation guidelines for the selection of appropriate control tools. The Common Criteria, COBIT, and ISO/IEC 27001 Section 1, ISO 27002 Chapter 2, and the NIST Handbook (Chapter 8) provide valuable guidance for completing this subprocess.

The output from this process will lead to a short list of security controls to use in Box 8, whether they are changes to existing policy, or call for the formulation of new policies, or introducing new vendor products into the legacy system.

Box 7, Development of Protection Profiles. A Protection Profile (PP) is an implementation-independent specification of information-assurance security requirements. Protection profiles are a complete combination of security objectives, security-related functional requirements, information assurance requirements, assumptions, and rationale.

The purpose of a PP is to state a security problem rigorously for a given collection of systems or products — known as the Target of Evaluation (TOE) — and to specify security requirements to address that problem without dictating how these requirements will be implemented.¹⁰

A PP specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products. Among others, it typically specifies the Evaluation Assurance Level (EAL), a number from 1 through 7, indicating the depth and rigor of the security evaluation, usually in the form of supporting documentation and testing that a product meets the security requirements specified in the PP.¹¹ The Common Criteria is the best source of guidance for this process.

Box 8, Selection of Appropriate Control Tools. The Risk Management Framework, presented earlier, provides the guidance for this process. In addition, close attention should be given to the security controls themselves, making sure they meet or exceed the security policies established from previous processes.

The National Institute of Standards and Technology has released a suite of tools to help automate vulnerability management and evaluate compliance with federal IT security requirements.

The Security Content Automation Protocol (SCAP) is an expansion of the National Vulnerability Database. It is an automated checklist that uses a collection of recognized standards for naming software flaws and configuration problems in specific products. It can help test for the presence of vulnerabilities and rank them according to severity of impact. The checklist files are mapped to NIST specifications for compliance with the Federal Information Security Management Act, so that the output can be used to document FISMA compliance. SCAP is intended to help make the step from FISMA compliance to operational IT security.¹²

Box 9, Architectural Models, that can manage change effectively, are generally more successful than those that cannot. Many organizations know that they need to improve their IT-related development processes in order to successfully manage change, but do not know how. Such organizations typically either spend very little on process improvements, because they are unsure how best to proceed, or spend a lot on a number of parallel and unfocused efforts to little or no avail.

Capability Maturity Models (CMM) address this problem by providing an effective and proven method for an organization to gradually gain control over and improve its IT-related development processes. Such models provide the following benefits:

- They describe the practices that any organization must perform in order to improve its processes.
- They provide a yardstick against which to periodically measure improvement.
- They constitute a proven framework within which to manage the improvement efforts.

¹⁰ http://en.wikipedia.org/wiki/Protection_Profile

¹¹ http://en.wikipedia.org/wiki/Protection_Profile

¹² NIST releases FISMA security control tools, By William Jackson, Government Computer News January 22, 2008

The various practices are typically organized into five levels, each level representing an increased ability to control and manage the development environment.

An evaluation of the organization's practices against the model — called an *assessment* — determines the level at which the organization currently stands. It indicates the organization's maturity in the area concerned, and the practices on which the organization needs to focus in order to see the greatest improvement and the highest return on investment.

The benefits of capability maturity models are well-documented for software and systems engineering. Their application to enterprise architecture has been a recent development, stimulated by the increasing interest in enterprise architecture in recent years, combined with the lack of maturity in this discipline.

Evaluating IT-related development processes against the SSE-CMM should be considered a best practice within an organization.

Box 10, Architectural Selection and Systems Engineering Trade-offs. The Software Engineering Institute at Carnegie Mellon developed an Architecture Tradeoff Analysis Model (ATAM) that is the leading method in the area of software architecture evaluation. This model can easily be adapted for IT security architectures. Proven benefits of the ATAM include:

- Clarified quality attribute requirements
- Improved architecture documentation
- Documented basis for architectural decisions
- Identified risks early in the life cycle
- Increased communication among stakeholders

However, the most important results are improved architectures.

The systems engineering approach was used to develop how the secure environment should be designed. Selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk — that is, the risk to the organization or to individuals associated with the operation of an information system.

The guidance from the SSE-CMM should be followed to ensure a repeatable process by different people, over time. A policy should be defined and enforced by procedures and automated tools and reviews.

The systems designer can choose from various methods to design the system that best fits the needs of the entity. The systems approach provides a suitable framework for defining and designing security systems. This approach recognizes not only that security can be defined as a system, but also that the security system exists and interacts with other systems and the environment. This interaction results in a security system where the system qualities exceed the sum of the system components.

A holistic network security system exists within IT; therefore, the network security system can be said to support IT. IT typically acts as a support structure for the organization; thus, the security system should support the organization, not the other way around.

7 CONCLUSIONS

While researching the documentation to develop this paper, it became obvious that no single standard, legal requirement, recognized guidelines or frameworks could ensure the delivery of a completely “Trusted Environment.” As the diagram in Figure 3 illustrates, each document contains complementary areas that are directly related to providing a trusted environment, as far as the technology and best practice processes are concerned. But technology alone cannot guarantee a trusted environment; it takes majority consensus from the using body that everyone is following the same methodology to safeguard that environment.

It also became apparent that there are too many regulating documents to be realistically followed, and in many instances, the processes identified are redundant across several standards. For example, risk is addressed in every document referenced in this paper; however, each document has its own processes for assessing the threat, the vulnerability, the impact, and validating and verifying the risk. However, we have identified pivotal documents that provide the proper framework for developing a trusted or secure environment, and we list them in Section 7.

Additionally, we discovered that when security requirements are considered at all during the system life cycle, they tend to be general lists of security features such as password protection, firewalls, virus detection tools, and the like. These are, in fact, not security requirements at all, but rather implementation mechanisms intended to satisfy unstated requirements such as authenticated access. As a result, security requirements that are specific to a system and that provide for protection of essential services and assets are often neglected. In addition, the attacker perspective is not considered, with the result that security requirements, when they exist, are likely to be incomplete. We believe that a systematic approach to security requirements engineering will help avoid the problem of generic lists of features and will take into account the attacker perspective.

We also found that standards, by their very nature, cannot exactly match the requirements of every organization, and due diligence needs to be practiced when determining what is appropriate for each circumstance. It is also critical to construct security policies that will ensure compliance with the organizational security requirements.

8 RECOMMENDATIONS

The challenges that organizations face in designing, developing, and deploying a trusted system can be traced back to the guidance documentation. There are too many guides, they provide conflicting advice, and they do not address the interdependencies that systems require to maintain a secure environment. Additionally, the guides overlook the importance of conducting a comprehensive analysis of the network or the environment the systems must operate within. Finally, they do not consider application compatibility and are often too simplistic.

The approach we are recommending looks at the problem from a different point of view. Whether you are an organization or a contractor to an organization is immaterial to our approach. You provide services to a customer base; that base may be internal to your organization or as a contractor, external to your organization. The point is that you provide a service.

The design, development, and deployment of a Trusted Data Center or Trusted Data Service should be viewed as providing a service. As such, there are service-oriented tools that can assist in the delivery of that service. The most widely used service-oriented tool is the Information Technology Infrastructure Library (ITIL), particularly Version 3, which has as its core architecture the Service Life-Cycle model. ISO/IEC 20000 was derived from the ITIL framework; therefore our approach is standards-based.

While ITIL provides the framework for service delivery, it is weak in the area of security, and it is not a systems engineering framework for the design of new or the redesign of existing systems. It cannot be used alone to achieve our goal of providing a trusted system. However, by injecting into the ITIL Service Life-Cycle processes the systems approach, and using the guidelines from the Risk Management Framework, along with the governance of ISO/IEC 27001, 27002, the Common Criteria, SSE-CMM, and the COBIT, we develop a methodology to reach our objective.

Starting with the Service Strategy volume of ITIL, define the service, define the requirements, (paying close attention to the security requirements) define what needs to be measured, and identify the governance documentation to be used. We recommend:

- The NIST Risk Management Framework
- SSE-CMM, which provides metric guidance
- ISO/IEC 27001 for security requirements
- ISO/IEC 27002, which lists security control objectives and recommends a range of specific security controls
- The Common Criteria, which provides the framework for specifying security requirements
- COBIT for providing controls that provide management with assurance that IT is operating in a controlled manner

The Service Strategy then serves as the input to the Service Design process and begins the development of the service.

APPENDIX A: REFERENCES

Control Objectives for Information and Related Technology (COBIT)

Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

Homeland Security Presidential Directive 12 (HSPD-12)

Information Technology Infrastructure Library (ITIL): www.itil.co.uk/

ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005: www.bsi-global.com/ICT/Service/bs15000-1.xalter

NIST Special Publication 800-64, System Considerations in the Information System Development Life Cycle

NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems

NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

NIST Special Publication 800-70, Security Configuration Checklist Program for IT Products — Guidance for Checklist Users and Developers

Security of Federal Automated Information Resources (OMB Circular A-130, Appendix III) — Certification and Accreditation

The Federal Information Security Management Act of 2002, enacted as Title III of

The E-Government Act of 2002