Chapter 5

Audit and Certification

Having set up an information security management system (ISMS) using the International Standards Organization (ISO) standards, an organization is able to manage business risk with repeatable processes using many standards-based policies, procedures, tools, and templates. Business benefits from this approach include leveraging initial investments in procedures, tools, and templates across many parts of the organization. Centralized creation and management of these tools support organizational learning where lessons learned by one result in better practices by all. Moreover, the creation of standards-based traceability matrices that align security initiatives with business drivers provides the ability to prove the business value of information security. With this foundation in good security management practices, many organizations desire to pursue the next step of independent audit of their ISMS and obtain certification that their ISMS meets ISO 27001 standards. This chapter presents details of preparing for and obtaining ISO 27001 certification.

5.1 Objectives

The following is a summary of chapter objectives:

- Learning about the audit process:
  - Interweave three perspectives of the audit process:
    - *Preaudit*, *audit*, and *postaudit*
    - *Four-stage approach* of ISO 27001 certification
    - *Pre-site visit*, *site visit*, *post-site visit*
- Facilitating the audit process
- Preparing to achieve ISO 27001 certification

- Definition of an accredited certification body
- Role of an accredited certification body
- Finding and engaging a certifying auditor

5.2 Certification Process Overview

The pending standard ISO/IEC 27006 (proposed), *Information Technology — Security Techniques — International Accreditation Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems*, provides guidance to accredited certification bodies (third-party auditors) on how to certify and register another organization's ISMS. Because the standard is not yet available, certified accreditation bodies (henceforth called *certifiers* for brevity) perform variations on a very similar process to certify the organization as ISO 27001 compliant. The goal is not 100 percent perfection, given that security is a process and not a goal; the objective is to instill a process to plan, implement, monitor, review, and revise security with changing industry knowledge, business environment, and an evolving threat environment. Therefore, the goal of the certification process is not to prove 100 percent safety, but rather an adequate level of preparedness with appropriate policy, standards, and procedures in keeping with ISO 27001 and ISO 27002.

ISMS certification lasts approximately three years, then requires recertification. A certificate register is available at http://www.iso27001certificates.com/, which shows all organizations that have various ISO certifications and have registered with the site.

The certification process generally consists of the following activities, with slight variations among the certifiers:

- Preaudit
  - Selecting an accredited certification body
  - Audit preparation
- Audit
  - Pre-site visit activity
    - Stage 1
    - Stage 2
  - Site visit activity
    - Stage 3
  - Post-site visit activity
    - Stage 4
- Postaudit

Many certifiers portray their activity in stages and specifically use the term *stages*. Activities in these stages align directly with *pre-site visit*, *site visit*, and *post-site visit* activities, which in turn align with *preaudit*, *audit*, and *postaudit* activities.

The reason for introducing the categorization of pre-site visit, site visit, and post-site visit becomes evident in Chapter 6, "Compliance Management," where achieving ISO 27001 certification is one instance of a compliance management process. The intent of these various perspectives is to add clarity that ties together multiple activities to satisfy a larger goal.

Only an accredited certifying body may certify an organization as ISO 27001 compliant, and the organization must choose a certifying body to perform the audit. Audit preparation is the organization compiling all relevant documentation and notifying appropriate personnel regarding pending phone calls and site visits by the certifiers. Pre-site visit consists of documentation review by the certifier. Site visit is the certifier validating that organizational practices are in keeping with documentation. Post-site visit is the certifier analyzing the results and providing a findings report to the organization. At this point, there may be a certification or the need for corrective action prior to receiving certification. The remainder of this chapter expands on each of the phases or stages in the bullet list above.

5.3 Selecting an Accredited Certification Body

Only an accredited certification body may certify the organization as ISO 27001 compliant. The URL http://www.iso27001certificates.com/ contains a list of accredited certification bodies. The applicable National Accreditation Board certifies the certifier to become an accredited certification body. The organization may not certify itself as ISO 27001 compliant; such an audit must be by a third party. Likewise, if a third party plays a role in establishing the ISMS and that third party is also an accredited certification body, that third party may not audit its own work and a different third-party accredited certification body is necessary to perform the certification audit.

The objective of the certification audit is to confirm that the organization has implemented the ISMS, the appropriate procedures exist to operate, monitor, review, and revise the ISMS, the appropriate documentation exists regarding the ISMS, and organizational practices adhere to the ISMS documentation.

5.4 Certification Preparation Checklist

The certification preparation checklist provides a comprehensive list of materials and activities necessary to prepare the organization for an audit; Table 5.1 provides such a checklist. An internal audit verifies the existence of each document as well as the quality of each document compared to the ISO 27001 and ISO 27002 standards. Moreover, it examines organizational practices in light of the documentation. Again, perfection is not necessarily the goal; the goal is a good solid foundation for information security management that includes security policy, standards, procedures, and practice.

Table 5.1 Certification Preparation Checklist

Documentation	*Description*
Scope	Documentation describing the boundaries of the ISMS.
Information and information assets with classification	Documentation listing important information and information technology assets within scope; include classification of assets specifying importance to the organization.
ISMS policy	Document specifying the organizational policy with respect to the creation and maintenance of an ISMS.
Information security policy	Document that describes the organization's ISMS in layman vocabulary. In some cases, the ISMS policy is part of this document.
Risk assessment	Document describing the risk assessment processes as well as standards, tools, and templates to support the risk assessment activity.
Selection of controls (SoC) from ISO 27001	Document with a list of relevant controls from ISO 27001.
Risk treatment plan	Document with the plan to address organizational risks. The risk treatment plan will evolve from the original document from the plan phase.
Statement of applicability (SoA)	The SoA is a document that includes a list of all ISO 27001 controls and statements for each control on how the organization will address that control in the context of managing business risk.
Information Security Handbook	The Information Security Handbook includes all security controls and procedures for the organization.
Business continuity management	A document to manage the continuity and recovery of the organization in a disaster that includes a business continuity plan (BCP) and disaster recovery plan (DRP).
Training documents and plan	Documents describing the information security awareness, training, and education (SETA) for employees and a plan when each takes place, e.g., new-hire orientation.
Description of ISMS operation	Document that describes the operation and function of the ISMS, including ISMS document locations.
Incident management document	Document describing incident management process.

Table 5.1 Certification Preparation Checklist (Continued)

Documentation	*Description*
Metrics and measurements	Document describing the creation of metrics and how the organization uses them to measure the effectiveness of the ISMS operations. The metrics and measures show business value as well as provide operational feedback to cross-function forum as well as management.
Residual risk update	Only the rare organization has no residual risk. The organization must review and update knowledge of and treatment of all accepted risk (residual risk). There should be a document that describes this process, a process that works in harmony with the risk treatment plan and the SoA.
Audit checklist	Document describing internal audits. The audit checklist is not mandatory for an external audit; however, the external auditor will look for details on how the organization performs an internal audit.
Results from the internal audit	This document is part of that to operate the ISMS. It is often a basis for input in the risk treatment plan to improve the ISMS operation.
ISMS operation improvement plan	Document describing ISMS improvements as a result of internal audit.

The guidelines, tools, and templates herein use specific versions of the ISO security standards, ISO 27001:2005 and ISO 27002. If the audit is to occur against latter versions, adjust the checklist as well as the preparation activities and materials accordingly. Selecting the certifier and preparing material to support the audit and certification process are part of preaudit activities.

5.5 The Audit Stage Process

Table 5.2 presents the four audit stages and a short description of each. These audit stages vary among the different certifiers; however, they all have the same objective and compare organizational preparedness with the same ISO security standard.

Pre-site visit activity includes stage 1 and stage 2 activities. Site visit activities include stage 3 activities, and stage 4 is in post-site visit activities.

5.5.1 Stage 1: Engaging the Certifier and Audit Kickoff

Upon the organization engaging a certifier, the auditor assigned will request documentation regarding the ISMS. This includes all documentation about the ISMS,

Table 5.2 Audit Process

Audit Stage	*Description*
1	Engaging the certifier and kicking off the audit process; handing over the documentation for review.
2	Verifying the existence of the appropriate documentation and the quality of the attributes of the documentation. If the auditor finds the documentation sufficient, he or she will agree to conduct an on-site assessment.
3	Performing the on-site visit and validating the claims of the ISMS documentation. After the on-site assessment, the lead auditor will have a meeting to convey the findings.
4	The auditor analyzes results and produces a findings report for delivery to the organization.

Table 5.3 Audit Report after Stage 1

Audit Report	*Description*
Document review	Report on the review of the documents. Are the documents complete? Is the organization taking the correct measures to document and work with its ISMS? (Are they on the right track?)

risk management, SoA, SoC, implementation plans, management plans, procedures, etc. Remember to convey these documents in a secure manner to the auditor with an appropriate nondisclosure agreement (NDA). (See Table 5.3.) **Note**: A secure manner does not include via plain-text attachments to an e-mail traversing the public network (Internet).

5.5.2 Stage 2: Document Review

The auditor will review the documentation for adherence to ISO 27001 and ISO 27002. The auditor will look for traceable links among ISO 27001, ISO 27002, policy, standards, procedures, and operational practice. He or she is looking for application of the Plan-Do-Check-Act (PDCA) model in the creation and management of the ISMS, and generally a presence of all relevant ISO 27001 features. Because the auditor will map the ISMS to the ISO standards, preparing documents that align with the ISO standards will expedite the process. The security management framework (SMF) and SMF-based templates herein provide such an alignment with the intent to accelerate both the development of the ISMS and the certification process. The auditor will determine if the organization is ready for an on-site audit. If not, the audit process will end with recommendations on improving preparedness.

If the auditor finds the documentation ample, he or she will agree to conduct an on-site assessment. The on-site assessment is looking to validate the existence of the ISMS as described in the documentation. Written policy and procedures are a start; however, the *proof is in the practice*, so to speak. **Caveat**: Practice without supporting policy and procedure is not adequate to achieve certification. Good practices are common; however, capturing those good practices in documentation is not. The good practices are then as good as the people who practice them, and when these people leave the organization, so often does the good practice. Organizational learning and organizational preparedness require adequate documentation to guide all personnel in appropriate action.

Stage 2 is part of the pre-site visit activities. If the audit proceeds to an on-site visit, the auditor should generate a site visit agenda, schedule various interviews and validation activities prior to being on site, and arrange for site contacts that will assist in arranging for the auditor to enter the site and areas relevant to the audit. The on-site contact may also assist in arranging interviews and certifier access to the relevant information and information technology to validate the ISMS security controls. If the auditor is not forthcoming with these materials and this level of planning, suggest that he or she does so to optimize the investment in the audit process.

5.5.3 Stage 3: On-Site Audit

Stage 3 is the on-site visit. The on-site audit occurs after the certifier determines the documentation is in keeping with the ISO security standards. The purpose of the on-site visit is to assess that personnel security awareness and security practices are in keeping with the documentation, that is, to determine the organization actually does what it says it does. This process includes interviews as well as verification and validation of security controls. Verification is ensuring the presence of security services and security mechanisms. Security services may include an incident response center, a help desk, a disaster recovery site, etc. Security mechanisms may include firewalls, intrusion detection systems, anti-malware, etc. However, the presence of these services and mechanisms is one task; determining their quality is another.

Validation determines the quality of the security services and mechanisms, where the quality is gauged against what the organization claims they do. The initial document review determines if policy, standards, and procedures adhere to the ISO standards. Part of the on-site audit determines if practice adheres to these documents. Validation of controls may include the certifier shoulder surfing, or the auditor may perform hands-on validation. For shoulder-surfing validation, the auditor works with the user, administrator, engineer, or other personnel, where those personnel perform activities to show organizational practice is in keeping with policy, standards, and procedures. In other cases, the certifier may request access to perform activities itself. Validation activities will include system log-on (use of unique user IDs and passwords), application log-on, operating system

hardening, secure communications (e.g., virtual private network [VPN]), physical security (e.g., cipher locks), and more.

For example, personal experience includes showing up to an interview with the manager, physical security having entered the facility through the loading dock, waving to the security cameras, and entering a backdoor on the other side of the loading dock. Then, walking up several flights of stairs, entering each floor along the way, opening data closet doors, and talking to a few users in offices along the way asking for directions (no one offered an escort or challenged our presence). This is a good example of hands-on validation of physical security. The personnel, including the security manager, were all nice people, professional, security aware, and under the impression their safeguards were adequate. Personnel badges contained pictures and radio frequency identification (RFID) capability to log entry/exit. The assumption was that all personnel would use the official entrance, hardly the preferred path of those with less than virtuous intents.

The breadth and depth of hands-on validation is the critical path in the duration of the on-site visit. Many activities may depend on initial findings. One method is to make a judgment call on personal credibility during the interviews. A high level of awareness, knowledge of security in general, and knowledge of organizational security objectives and practices result in a high level of confidence on the part of the certifier that the organization gets it and is doing the right things. Some on-site activity is standard and will take place as a matter of course, e.g., checking for password and cipher lock (or equivalent) safeguards on the data center. Other activities will be organization specific; e.g., an organization processing credit card information should take steps to protect customer privacy and identity. The audit will still be ISO 27001 focused; however, the ISO security standards support the need to bolster up security in areas of particular concern to that organization. The validation activities will also vary depending on the initial findings; that is, exploring weaknesses to find the break point and maybe pushing a bit further to determine the implications of the break point.

Audits may be intrusive or nonintrusive. Typically, they are the latter, but verify to ensure everyone involved has the same expectations and understanding. An intrusive audit or assessment may include an intent to break into systems by compromising user IDs and passwords. A passive audit or assessment may just discover the user IDs and passwords, but not attempt to use them in a subversive manner. Likewise, an intrusive audit or assessment may attempt denial of service. Although it is good to know where the break points are, this is not good if such activities actually interrupt production operations.

Table 5.4 shows a list of potential reports resulting from stage 3. The reports include the audit findings in a format that states the compliance requirement, the current state of the organization, a gap analysis, a remediation analysis (options for fixing weaknesses), and recommendations for gap closure. The certifier may use the term *nonconformity*. A nonconformity is a condition contrary to the requirements of the ISO 27001[1] standard. The auditor may further categorize findings in three nonconformity classifications: *major*, *minor*, and *observation*. A major nonconformity

Table 5.4 Audit Reports after Stage 3

Audit Reports	*Description*
Document review	Report enumerating documents that are part of the audit and the status of each document
Summary report	Report of the inspection carried out by the auditor
Audit findings	Report on what the auditor found that is not compliant with the standard and has to be fixed and in place for the next inspection in six months
Recommendation	Report whether the auditor will recommend that the organization should apply for the certification

may be a total breakdown of a system, control, or objective. This may be the complete absence of a particular requirement or the absence of formal documentation or an existing practice. Clauses 4 to 8 are mandatory sections of ISO 27001 to achieve certification; an absence of any of these requirements will likely be a major nonconformity. A major nonconformity will likely result in noncertification against the ISO 27001 standard, and the organization will have to wait for six months to request another audit.

A minor nonconformity results if part of a policy is missing or is sufficiently vague to cause confusion. In this case, the policy (or other document) exists, but the quality of the policy does not meet with the intent of the ISO standards. A minor nonconformity may result as well if the documentation is complete but the practice is incomplete. Similarly, personnel do perform the activities related to the safeguard; however, they do not perform all the activities that constitute conformity with the ISO standards. There may be a grace period shorter than six months to fix minor nonconformities.

The observation nonconformity results if the certifier finds appropriate documentation and practice but sees an opportunity for improvement that will increase the effectiveness of the control or otherwise benefit the organization's security posture. The organization provides a written response to addressing all observations. Similar to the SoA, *addressing* the risk means the organization may rationalize the observed nonconformity through a statement of risk acceptance, or it may state a plan to modify documentation or practice to remediate the risk.

5.5.4 Stage 4: Delivery of Findings

Stage 4 is the formal delivery of the results from the certifier to the organization. Stage 4 is the presentation of findings, gaps (nonconformities), options, and recommendations by the certifier for organization actions. The report(s) will align with specific elements within ISO 27001 and ISO 27002. The certifier provides a

classification for each gap (major, minor, observation). The organization provides a written response to each gap, addressing the nonconformities according to its position of accepting the risk or plans to mitigate the risk. The results of stage 4 are either pass (receive certification) or fail. The organization must wait six months to reattempt certification and perform corrective action during that time according to recommendations by the certifier.

If the organization receives ISO 27001 certification, it is valid for three years, after which there is a renewal process. To prepare for and ease the renewal process, the organization and the certifier may agree upon a three-year surveillance plan for the ISMS. The plan will include a series of reviews and visits by the certifier and which sections or clauses of the ISO standards to focus on for each review and visit. The specific plans may vary slightly according to new details in ISO standard updates or a changing business environment (new legislation, regulation, market demands for increase in or otherwise modified security posture). Each visit is a mini-certification audit resulting in a findings report that includes requirements, gaps, options, and recommendations. This ongoing monitoring of the ISMS is good practice and eases the certification renewal process.

Chapter 6

Compliance Management

The purpose of this book is to assist the reader in establishing an effective information security management system (ISMS) and achieving ISO 27001 certification. The process to establish an ISMS is one instance of an overall *compliance management process*, where the compliance requirements in context of achieving ISO 27001 certification are ISO 27001 and ISO 27002. It is possible to abstract the ISO 27001 certification process described thus far into a general compliance management process accommodating many compliance requirements. Other compliance requirements may be Sarbanes–Oxley, Health Insurance Portability and Accountability Act (HIPAA), or legislation applicable to civilian government (e.g., Federal Information Security Management Act [FISMA]). This chapter presents material regarding an abstract approach to compliance management applicable to all these and more.

Additionally, there is the potential to cross-index compliance requirement elements such that showing compliance for a requirement in one standard implies compliance with another or many others. Therefore, achieving ISO 27001 certification implies at least partial compliance with other security-related legislation, regulation, and standards. Building a security management framework (SMF) with foundation in all organizationally relevant security compliance requirements provides the ability to develop a single methodology and single tool set for discovery, analysis, and reporting that establishes, tracks, and proves compliance with all applicable security requirements.

6.1 Objectives

The following list summarizes the objectives for this chapter:

- Distinguish the difference between a comprehensive compliance management program (CMP) and an information assurance (IA) CMP.
- Present details of an IA CMP.
- Present an IA CMP methodology.
- Enumerate a set of processes, tools, and templates to support an IA CMP.
- Discuss the application of the processes, tools, and templates to plan, establish, implement, maintain, review, and revise (sound familiar?) the IA CMP.

6.2 Introduction to Compliance Management

Compliance management is both very broad and specific to the nature of the organization. For example, a healthcare organization may need to comply with legislation governing hazardous waste disposal. Such compliance is absolutely critical to employee and public safety. Such compliance activity is part of a comprehensive CMP. Compliance management with respect to information and information technology is but one part of this comprehensive CMP. The focus herein is on compliance management with respect to information security; that is, the security of information technology, business functions, personnel, infrastructure, and physical aspects that contributes to information security— also known as *information assurance*. That is, the focus is on an *information assurance compliance management program*. With respect to creating an IA CMP, the following are necessary:

- IA CMP framework
- Process to identify all relevant compliance requirements
- Template(s) to enumerate all relevant compliance requirements
- Creation of requirement traceability matrices
- Cross-index to leverage compliance activities across all applicable requirements, and to avoid redundancy, thus minimizing costs

6.3 IA CMP

As previously mentioned, the map of the territory is not the territory. This text is a map of the ISO standards, a map of how to use them in practical application. This text is not a replacement for the ISO standards. To acquire the ISO standards, go to www.iso.org or use an Internet search engine to find an alternative source. The authors intend the material herein as a supplement to the actual standards applicable

to the organization, not a substitute. An IA CMP consists of the following useful tools, some of which use ISO 27002 as a foundation:

- Compliance management framework
- Security management framework
- Compliance management requirements engineering
- Compliance assessment methodology
- Compliance management tools
- Compliance metrics

6.3.1 Compliance Management Framework

A CMP enumerates all organizational compliance requirements. An effective CMP starts with a compliance management framework. A compliance management framework provides guidance on how to define all organizational-specific compliance requirements; an IA compliance management framework provides focus on security-related compliance requirements. A compliance management *framework* assists to identify and enumerate all relevant compliance requirements.

Note: There is a hesitation to say *all* compliance requirements or *comprehensive list*, as there is a question of necessity to identify, enumerate, and act upon literally all compliance requirements within the formality of the compliance framework. Under the principle of *best–good–good enough*, there is a practical limit to this exercise. To this end, consider that the framework provides the ability to provide adequate identification, enumeration, and planning for compliance requirements that have a direct effect on operations and organizational viability. Point is, the same framework provides the ability to record requirement details to any breadth or depth necessary. Figure 6.1 provides an overview of the compliance management requirements framework.

External compliance requirements reside outside the organization and are most often legislative or regulatory restrictions or guidance imposed on organizational practices. Internal compliance requirements include mission statement, organizational goals, corporate policy, contractual obligations, and enumeration of stakeholder interests.

Explicit compliance requirements are enumerated in a Request for Proposal (RFP) or in a contract. Implicit compliance requirements are derived from explicit requirements or implied by compliance with explicit requirements. For example, a U.S. federal civilian RFP may require compliance with the Federal Information Security Management Act of 2002. The implied requirements in FISMA include the National Institute of Technology (NIST) standards and guidelines, as well as the Office of Management and Budget (OMB) audit standards, as OMB audits gauge the compliance levels of federal organizations against FISMA. A low FISMA compliance level may jeopardize funding; therefore, enumerating the OMB audit

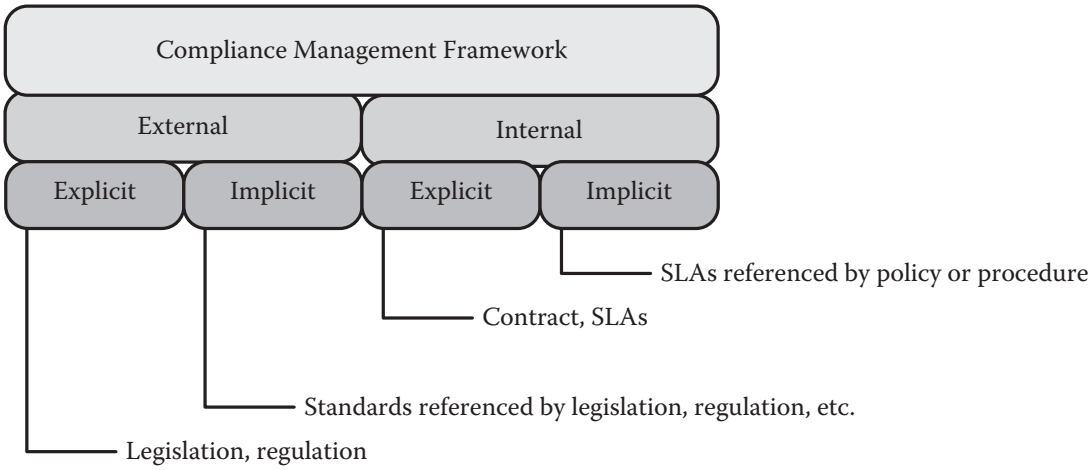

Figure 6.1 Compliance management requirements framework.

guides as an external-implicit compliance requirement is appropriate to mitigate risk of reduced funding.

External-explicit requirements include self-imposed standards of compliance, e.g., ISO 9000, ISO 27001, ISO 27002. The difference is, no legislation compels an organization to become ISO 27001 certified. The organization chooses ISO 27001 as a self-imposed standard for establishing an ISMS. Internal-explicit requirements include organizational mission statement or internal service level agreements (SLAs) between, say, network operations and various business groups. Internal-implicit requirements include adherence to security practices of another organization via business associate agreement. Implicit requirements may also include documents not explicitly enumerated, but part of the project, e.g., principles, constraints, and assumptions (PCAs) or concept of operations (CONOPS). Although not typically thought of as compliance requirements, PCAs, CONOPS, and similar documents provide direction for organization activity, including security; thus, they may fall under at least consideration for the IA compliance management framework.

The intent behind the framework is to provoke thought in various directions and to decompose a larger problem into manageable chunks with a guideline that assists the organization to consider all relevant compliance requirements. The following provides an expansion of the compliance management framework:

- External compliance requirements:
  - Explicit:
    - Legislation
    - Regulation
    - Guidelines
    - Directives
    - Instructions

- Implicit:
  - Any qualification of a necessary supporting activity to adhere to an explicit requirement
  - Any qualification of a supporting activity to minimize organizational risk:
    - For example, litigation management: for example, *Federal Sentencing Guidelines*, Chapter 8, "Sentencing of Organizations"

■ Internal compliance requirements:
- Explicit:
  - Mission statement
  - Policies:
    - For example, ethics policy
  - Procedures
  - Standards
  - Contracts:
    - Partners, vendors, customers
- Implicit:
  - Any qualification of a necessary supporting activity to adhere to an explicit requirement

6.3.2 Security Management Framework

Traditionally, security is an afterthought. In the past, most executives and managers yielded to the need for door locks, perhaps a security guard, and the need for fire control systems, at least after they saw a drop in insurance premiums to provide a payback for the investment. Adding appropriate controls to protect cyber assets or the facilities housing cyber assets is traditionally *a* "*nice to have*" *if there's enough budget left over*. Due to the exploding popularity of computers and the Internet, the business environment is vastly different from just 10 years ago; *security is no longer a nice to have, but a legislative mandate*. In the United States, the Sarbanes–Oxley Act of 2002 (SOX), Section 404 prescribes security controls for financial systems, and the Health Insurance Portability and Accessibility Act of 1996 Final Security Rule (HIPAA FSR) requires the protection of electronic protected health information (ePHI). Other legislation imposes restrictions on data ownership and data custodianship, including the European Directive on Data Protection or the Safe Harbor framework that permits non-European organizations access to data by certifying adequate privacy protection. Moreover, organizations require proof of return on investment (ROI) on all major budget allocations; providing details for return on security investment (ROSI) is difficult to say the least — difficult, but not impossible. The ability to capture details of security planning that align with the business drivers behind them facilitates the ability to show a ROSI, plus more.