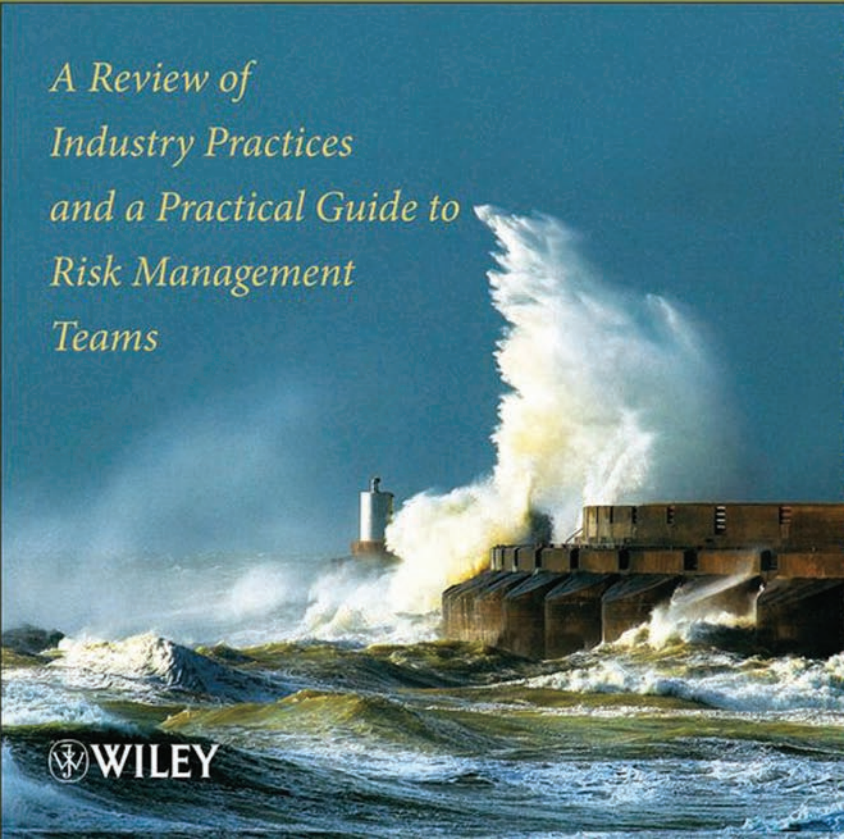
JAKE KOUNS AND DANIEL MINOLI

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS



A Review of Industry Practices and a Practical Guide to Risk Management Teams

WILEY

PART I

INDUSTRY PRACTICES IN RISK MANAGEMENT

CHAPTER 1

INFORMATION SECURITY RISK MANAGEMENT IMPERATIVES AND OPPORTUNITIES

1.1 RISK MANAGEMENT PURPOSE AND SCOPE

1.1.1 Purpose of Risk Management

This text deals with information technology (IT) risk management (ITRM), which, given the context of this text, we also just refer to as risk management.[1] Concerns about the possibility of compromise and/or the loss of proprietary information have reached critical levels in many organizations in recent years as a barrage of news bulletins reporting on infractions and product defects, staff's shortfalls and shortcomings, functions' outsourcings and offshorings, political instabilities in a number of countries and in wider regions, and management's emphasis on short-term financial breakeven has become all too frequent. Cyber attacks continue to be a source of significant exposure to organizations of all types, and, as a consequence, potential damage, potential impairment, and/or potential incapacitation of IT assets have become fundamental business viability/continuity issues.

Information Security[2] is recognized at this juncture to be a key area of IT management by a majority of government, commercial, and industrial organizations. Information Security is defined as the set of mechanisms, techniques, measures, and administrative processes employed to protect IT assets from unauthorized access, (mis)appropriation, manipulation, modification, loss, or (mis)use and from unintentional disclosure of data and information embedded in these assets. Some organizations have individuals on staff with a plethora of security certifications, yet these organizations continue to be afflicted with security

[1] Some also refer to ITRM as "information security risk management (ISRM)."

[2] Some also use the terms "infosecurity," and/or "INFOSEC," and/or "information systems security (ISS)," and/or "information security management (ISM)."

Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practial Guide to Risk Management Teams, by Jake Kouns and Daniel Minoli

breaches on a fairly routine basis and continue to be exposed to risk; this implies that perhaps other approaches to information security are needed. Practitioners of information security are all well aware that exposure to risk is ever-changing and that it is also hard to assess; therefore, what is needed to manage and minimize risk in organizations is a diversified, versatile, and experienced IT/networking staff along with a solid set of policies, processes, and procedures that create a reliable information security program. This approach is typically much more successful as compared to the case where an organization just attempts to rely on ultra-narrow staffers with cookbooks of perishable memorized software commands specific to a given version of a given program of a given vendor to produce results, where the organization seems to be assuming that the real-life information security issues are similar to an academic pre-canned rapid-fire test for abstract scholastic grades, and simply believes that an alphabet soup of tags following one's name is sufficient (or necessary) to address incessant IT security threats.

Risk is a quantitative measure of the potential damage caused by a threat, by a vulnerability, or by an event (malicious or nonmalicious) that affects the set of IT assets owned by the organization. Risk exposure (that is, being subjected to risk-generating events) leads to potential losses, and risk is a measure of the "average" (typical) loss that may be expected from that exposure. Risk, therefore, is a quantitative measure of the damage that can incur to a given asset even after (a number of) information security measures have been deployed by the organization. Obviously, when the risk is high, an enhanced set of information security controls, specific to the situation at hand, needs to be deployed fairly rapidly in the IT environment of the organization. See Table 1.1 for some risk-related definitions, loosely modeled after [HUB200701]. The term "information asset" refers here to actual data elements, records, files, software systems (applications), and so on, while the term "IT asset" refers to the broader set of assets including the hardware, the media, the communications elements, and the actual IT environment of the enterprise; the general term "asset," refers to either "information asset" or "IT asset;" or both, depending on context. Typical corporate IT assets in a commercial enterprise environment include, but are not limited to, the following:

- Desktops PCs and laptops
- Mobile devices and wireless networks (e.g., PDAs, Wi-Fi/Bluetooth devices)
- Application servers, mainframes
- Mail servers
- Web servers
- Database servers (data warehouses, storage) as well as the entire universe of corporate data, records, memos, reports, etc.
- Network elements (switches, routers, firewalls, appliances, etc.)
- PBXs, IP-PBXs, VRUs, ACDs, voicemail systems, etc.
- Mobility (support) systems (Virtual Private Network nodes, wireless e-mail servers, etc.)

TABLE 1.1. Uncertainty, Probability, and Risk

Uncertainty	The lack of complete certainty, that is, the existence of more than one possibility for the outcome. The "true" outcome/state/result/value is not known.
Measurement of uncertainty	A set of probabilities assigned to a set of possibilities (specifically for risk events, threats, and/or vulnerabilities).
Risk exposure (also, liability)	A state of uncertainty where some of the possibilities (also colloquially called "risks") involve a loss, catastrophe, or other undesirable outcome. An environment exposed to risk events, threats, and/or vulnerabilities. Each new risk event, threat, and/or vulnerability gives rise to new risk exposure.
Measurement of risk	A set of possibilities, each with quantified probabilities and quantified losses.
Risk (singular)	The expected loss. Namely, the aggregation (summation) of the possibilities, their probabilities, and the loss associated with each possibility.
Risks (plural) (colloquial)	Individual possibilities (risk events) that are encountered with risk exposures.
Risk-exposing event (also called risk event)	Any changes in the state of the environment that have the potential of creating a new state where there is nonzero risk.

- Power sources
- Systems deployed in remote/branch locations (including international locations)
- Key organizational business processes (e.g., order processing, billing, procurement, customer relationship management, and so on)

Continuing with some definitions, a security threat is an occurrence, situation, or activity that has the potential to cause harm to the IT assets. A vulnerability (or weakness) is a lack of a safeguard that may be exploited by a threat, causing harm to the IT assets; specifically, it can be a software flaw that permits an exogenous agent to use a computer system without authorization or use it with an authorization level in excess of that which the system owner specifically granted to said agent. Risk-exposing events (also called risk events) are any changes in the state of the environment that have the potential of creating a new state where there is nonzero risk. Risk events and vulnerabilities are implicitly related in the context of this discussion in the sense that a vulnerability is ultimately given an opportunity for harm by some subtending event, malicious or nonmalicious. For example, in a so-called "nonmalicious event," a flaw may be inadvertently introduced in some software release by its designers; the event of having the IT group load and distribute that software throughout the enterprise creates a predicament where risk ensues. A "malicious" event may be a direct attack on the organization's firewalls, routers, website(s), or data warehouse.

> **Note:** Some people use the term "risk" (singular) more loosely than defined above to mean a potential threat, vulnerability, or (risk) event; we endeavor to avoid this phraseology, and we use the term risk to formally describe the quantitative (numerical) measure of the underlying damage-causing issues, and not the issues themselves.
>
> We acknowledge that the term "risks" (plural) is used colloquially to describe the set of individual possibilities (risk events) that are encountered with risk exposures. We occasionally use this phraseology.

Information security spans the areas of *confidentiality, integrity, and availability*. Confidentiality is protection against unauthorized access, appropriation, or use of assets. Integrity is protection against unauthorized manipulation, modification, or loss of assets. Availability is protection against blockage, limitation, or diminution of benefit from an asset that is owed. The Computer Crime and Intellectual Property Section (CCIPS) Computer Intrusion Cases of the U.S. Department of Justice defines these terms (and considers respective infractions as crimes) as follows:

- *Confidentiality*. A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access. Confidentiality is compromised when a hacker views or copies proprietary or private information, such as a credit card number or trade secret.
- *Integrity*. A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization. For example, viruses and worms alter the source code in order to allow a hacker to gain unauthorized access to a computer system.
- *Availability*. A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system. An example of this is a denial of service (DoS) attack.

At this point in time, the practical challenges for enterprises are how to organize and run an efficient and effective information security program for persistent, high-grade protection and, in turn, how to actually (i) identify risk events, (ii) assess the risk, and (iii) mitigate ("manage") the environment to reduce risk. IT risk management (information security risk management) is the process of reducing IT risk (a process is a well-defined, repeatable sequences of activities.) Risk management is a continuous process. IT risk management encompasses five processes (also see Table 1.2 and Figure 1.1):

1. (Ongoing) identification of threats, vulnerabilities, or (risk) events impacting the set of IT assets owned by the organization

TABLE 1.2. Risk Management Processes

Risk identification	The process of identifying threats, vulnerabilities, or events (malicious or nonmalicious, deterministic/planned, or random) impacting the set of IT assets owned by the organization.
Risk assessment	The process of calculating quantitatively the potential damage and/or monetary cost caused by a threat, a vulnerability, or by an event impacting the set of IT assets owned by the organization. Identification of the potential damage to the IT assets and/or to the business processes based on previous internal and external events, input from subject matter experts, and audits. Specifically, this entails (a) quantifying the potential damage, and (b) quantifying the probability that damage will occur.
Risk mitigation planning	Process for controlling and mitigating IT risks. It typically includes cost–benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws [STO200201].
Risk mitigation implementation	Deploying and placing in service equipment and/or solution identified during the risk mitigation planning phase, or actuating new corrective processes.
Evaluation of the mitigation's effectiveness	Monitoring the environment for effectiveness against the previous set of threats, vulnerabilities, or events, as well as determining if new/different threats, vulnerabilities, or events results from the modifications made to the environment.

2. Risk assessment (also called risk analysis by some, especially when combined with Step 1)
3. Risk mitigation planning
4. Risk mitigation implementation
5. Evaluation of the mitigation's effectiveness

When the term risk management (or information security risk management) is used in this text, all five of these processes are implied. Risk management is a fundamental, yet complex, element of information security. Figure 1.2, contained in the International Organization for Standardization (ISO) 27002 standard, depicts the macrocosms of information security management (ISM), including risk management. The National Institute of Standards and Technology (NIST) defines risk management (in their recommendation NIST SP 800-30) as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their

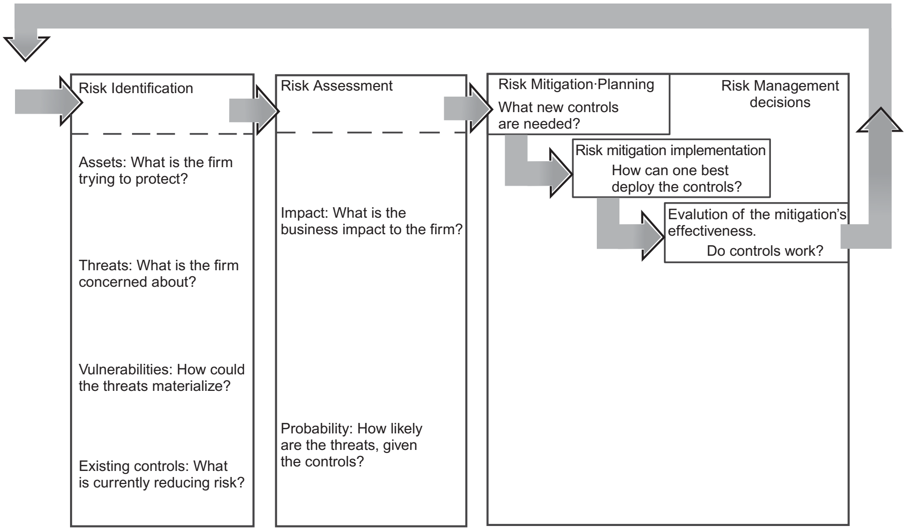

Risk Identification
Assets: What is the firm trying to protect?
Threats: What is the firm concerned about?
Vulnerabilities: How could the threats materialize?
Existing controls: What is currently reducing risk?
Risk Assessment
Impact: What is the business impact to the firm?
Probability: How likely are the threats, given the controls?
Risk Mitigation·Planning
What new controls are needed?
Risk Management decisions
Risk mitigation implementation
How can one best deploy the controls?
Evalution of the mitigation's effectiveness.
Do controls work?

FIGURE 1.1. Risk management process as defined in this text.

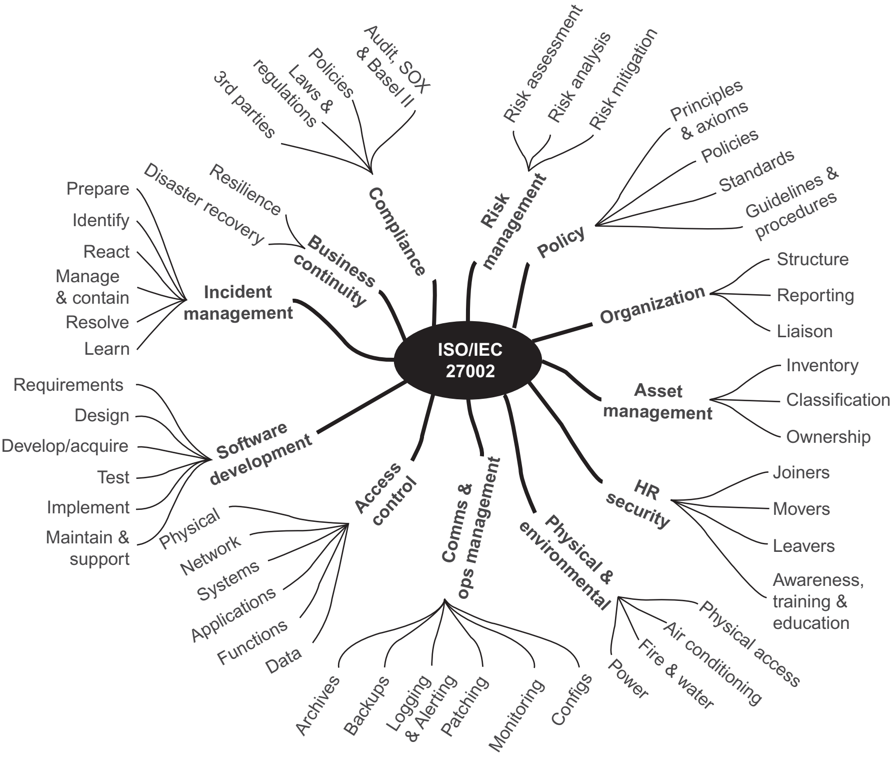


FIGURE 1.2. A view of information security management, as conceived in ISO 27002.

organizations' missions. Figure 1.3 provides a graphical view of the (assessment) process of NIST SP 800-30. Figure 1.4 depicts the ISO 31000 view of risk management. Figure 1.5 depicts the view in the Australian/New Zealand Standard AS/NZS 4360:2004. Figure 1.6 shows a vendor-based approach, specifically from Microsoft. Finally, Figure 1.7 depicts the view taken by OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), a risk-based strategic assessment and planning technique for security, developed by CERT (Carnegie Mellon University's Computer Emergency Response Team).

A recent confluence of technical and geopolitical factors has sensitized decision-makers about the business and legal consequences of cyber intrusions and risk exposures to an organization's IT assets, both at the corporate level as well as at the national security level. As a result of these developments, legislature has been introduced in a number of countries (e.g., Sarbanes–Oxley Act in the United States) that, in the final analysis, forces information security and privacy issues to be assessed rigorously and with fiduciary oversight by company executives and officials. In an effort to achieve business continuity and protect the enterprise from random, negligent, malicious, or planned security attacks, the organization must have a clear top-down understanding of its IT-supported business operations at a fundamental and comprehensive level. There must be an understanding of (a) what IT assets the company has deployed across its entire functional landscape, (b) how the resources are being used; and (c) who could attack these resources and the manner of such attacks.

IT security measures are intrinsically (and unfortunately) limited in their total effectiveness, therefore, organizations must equip themselves to manage risk. The following is an honest observation about the state of affairs from industry observers [MAR200601]:

> Even though serious responsibilities for complying with the organization's objectives have been placed in the hands of information systems, doubts about their security continue to arise. Those affected, often not technicians, wonder if they can place their trust on these systems. Each failure lowers the trust on information systems, especially when the investments made in defending the means of work do not rule out failures . . . The matter is not as much the absence of incidents, but the confidence that they are under control.

The convergence of IT networks and mobile communications (including "mobility solutions"), increases the number of potential threats, including unauthorized access, exploitable vulnerabilities, malicious attacks, viruses, worms, and DoS attacks to both wired and wireless corporate systems. Press time studies by the *IT Policy Compliance Group*[3] have shown that the primary business and financial liabilities from the use of IT are directly related to how well, or poorly,

[3] The IT Policy Compliance Group conducts benchmarks that are focused on delivering fact-based guidance on the steps that can be taken to improve results. Benchmark results are reported through www.itpolicycompliance.com for the benefit of members.

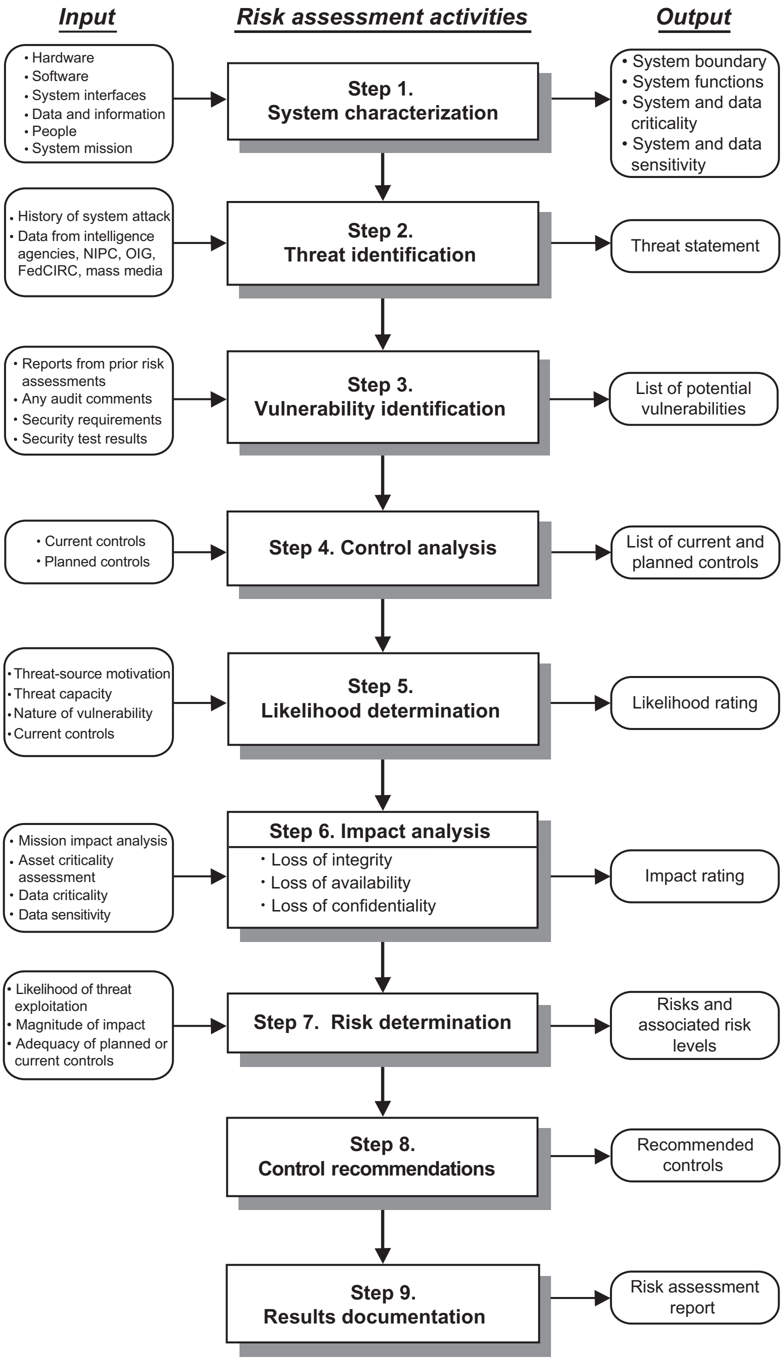


FIGURE 1.3. A graphical view of risk assessment, as conceived in NIST SP 800-30.

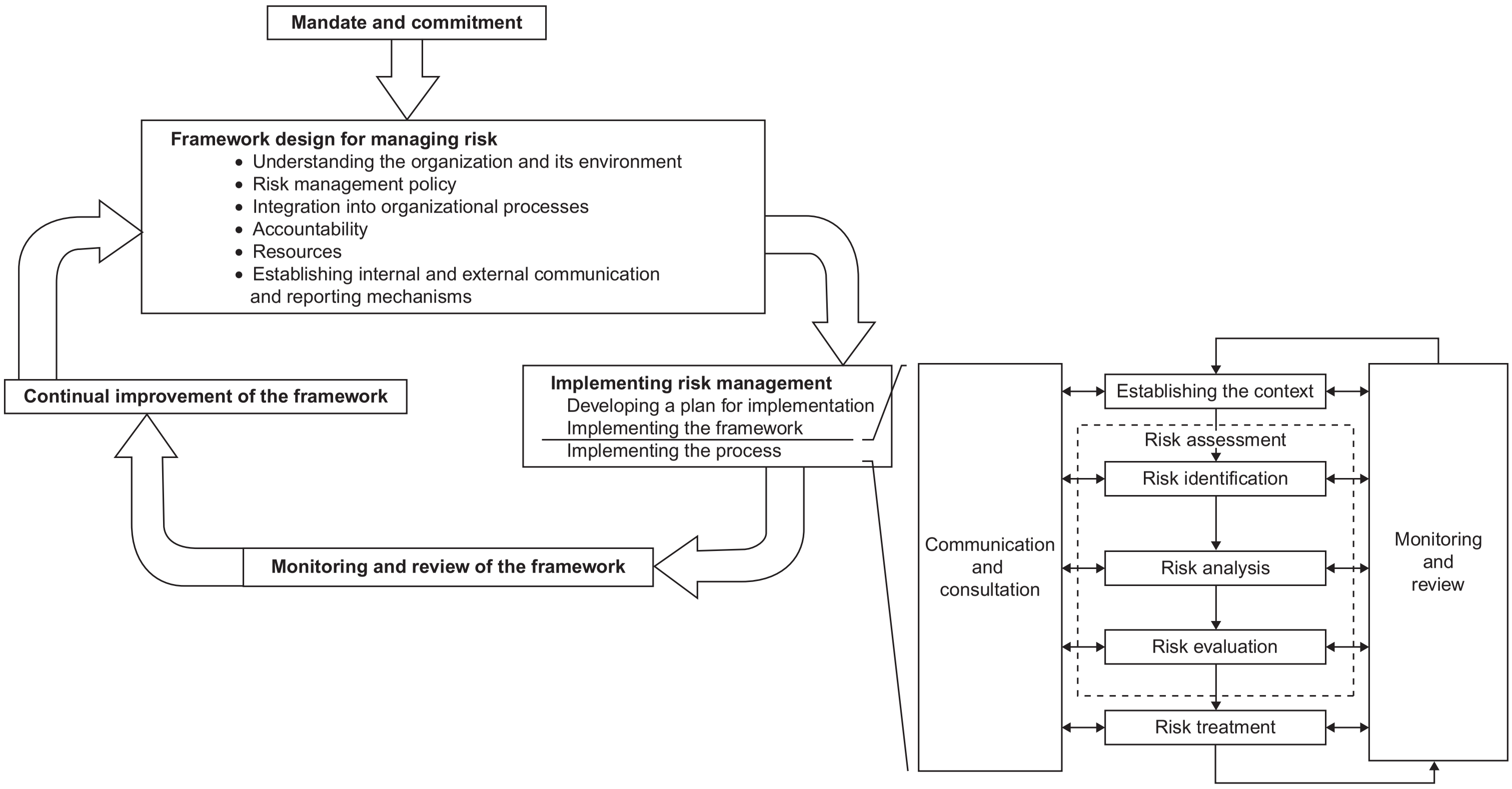

Mandate and commitment
Framework design for managing risk
• Understanding the organization and its environment
• Risk management policy
• Integration into organizational processes
• Accountability
• Resources
• Establishing internal and external communication and reporting mechanisms
Continual improvement of the framework
Implementing risk management
Developing a plan for implementation
Implementing the framework
Implementing the process
Monitoring and review of the framework
Communication and consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring and review

FIGURE 1.4. Framework for managing risk per (Draft International Standard) ISO/IEC 31000.

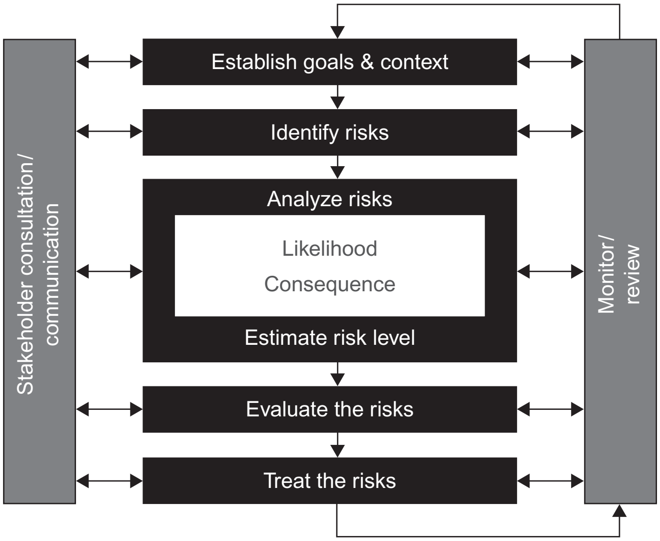


FIGURE 1.5. A view of the risk management process, as conceived in AS/NZS 4360:2004.

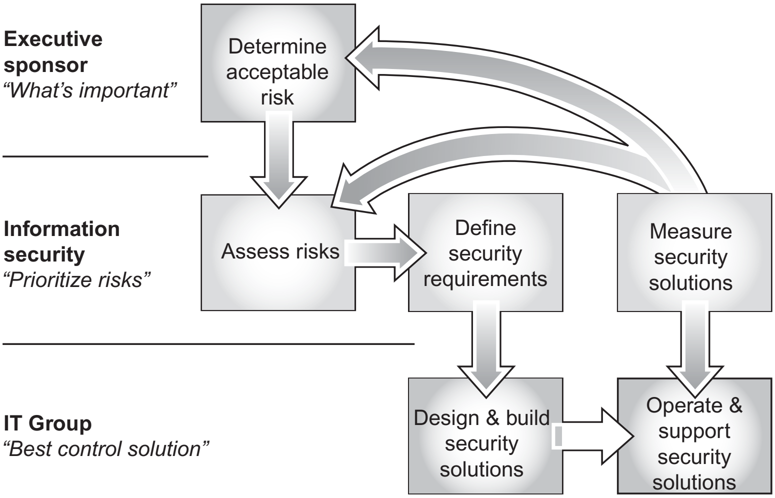


FIGURE 1.6. Microsoft risk management process.

organizations are managing the confidentiality, integrity, and availability of information and IT assets. These are, in turn, directly related to the controls and procedures implemented to protect sensitive information, maintain the integrity of information and audit controls, and the availability of IT services. The

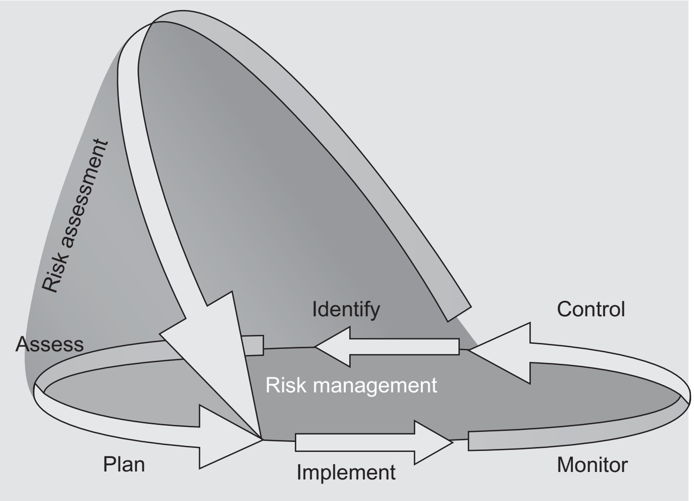


FIGURE 1.7. OCTAVE risk management/risk assessment.

primary business and financial liabilities are due to losses, or lapses that are occurring in three areas [ITP200901]:

- Confidentiality, or protection, of sensitive information
- Integrity of information, assets, and controls in IT
- Availability of IT services

These three—the loss of confidentiality, integrity, and availability—are ranked as the top business liabilities by organizations, well ahead of other possible concerns, including those from outsourced IT projects, systems, and information; delays to critical IT projects; and shortages of IT skills. Measured across almost 500 organizations surveyed, the findings reveal that the top business liabilities include:

1. Loss or theft of customer data
2. Business disruptions from IT failures and disruptions
3. Loss of integrity for critical IT assets and information

Specifically, in this 2009 study, the theft or loss of customer data was rated as the highest business risk by more than 72% of organizations while business disruptions and the loss of integrity were rated as posing the most business risk by 64% and 61% of organization, respectively. After the top three, theft or fraud related to IT assets and information and Internet security threats pose similarly high business liabilities. These highest-ranked business liabilities are followed by shortages of critical IT skills, delays to IT projects, and outsourced

IT capabilities and information [ITP200901]. According to the Open Security Foundation's DataLossDB (http://datalossdb.org), as of early 2009 over 358 million records have been exposed due to data loss incidents since January 2005.

Information security risk management seeks to reduce and/or minimize risk. It is unlikely that the risk can be reduced to zero; however, proper intervention should aim at decreasing it, and such goals are achievable when risk management techniques (methods and tools) are properly applied. If an organization has any of the following, then it is highly advisable, if not critical, that a risk management capability must be put in place:

- Has IT assets
- Has data
- Has proprietary information
- Keeps customer credit card, financial data, personal information or medical data
- Requires formal documentation and policies
- Is required to adhere to legal requirements, Sarbanes–Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), ISO 27000, and so on or
- Has a fiduciary responsibilities to stockholders

Of course, information security risk management is part of an overall business risk management continuum, as depicted in Figure 1.8.

There is no doubt that security threats are an ever-moving target, and, therefore, no definitive formula-based-solution is in sight at this juncture. Many books have been written in the past quarter century on the issue of information security and on general mechanisms that, at face value, address the

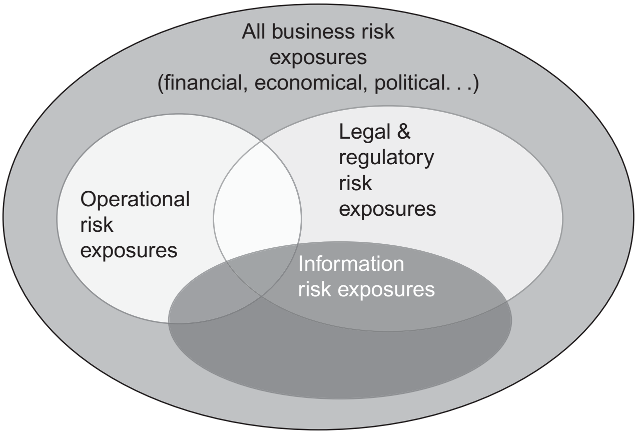

All business risk exposures (financial, economical, political. . .)
Operational risk exposures
Legal & regulatory risk exposures
Information risk exposures

FIGURE 1.8. Risk management continuum.

underlying technical issues. However, sadly, the complex issue of security and risk management is often reduced to a discussion about network security (in any event, when most people say "network security," they really mean "perimeter security" and not security of the network itself—that is, security of the network elements, transmission facilities, network management and/or provisioning system, and so on). It ought to be self-evident from recent history that for all intents and purposes, bookshelves of books that simply "blame" the network or hold it responsible for all sorts of security infractions to corporate IT assets is just a nonstarter for corporate officers under stringent regulatory mandates to demonstrate assured integrity.[4–6] It can be argued that there are clear benefits from implementing network or perimeter security, but it cannot be the only major control relied on as part of an information security program. A few years ago the concepts of "host security" and "network security" (perimeter security) were topics of "equal" treatment; today the concept of "host security" has almost exited the parlance even though some security vendors are now advocating endpoint security solutions, at least as documented by a book search on Google (see Appendix 2A, Section 2A.2). (There may be an "explanation" for this: After all, there is "something" that can be done for perimeter security: Having scripts to block Transmission Control Protocol (TCP) port i used by protocol ι, block TCP port j used protocol φ, block TCP port k used protocol k, block TCP port l used protocol λ, block TCP port m used protocol μ, and so on; the issue is that there may be rather scant science on the topic of host security for host A, or B, or C, even though these security measures would be of critical importance—focusing excessively on network/perimeter security obfuscates the critical fact that host security is of equal or even greater importance. The coming increased deployment of mobile devices and IPv6 will greatly increase this need for host/endpoint security in the near future.) Unfortunately, stories like the one that follows seem to be *a routine occurrence* at some U.S. organization: In February 2009, hackers broke into the Federal Aviation Administration's computer system, accessing the names and

[4] Perimeter and host security (including endsystems) need emphasis instead—networks are just "pipes." We do not blame the interstate highways, county roads, bridges, intercostals canals, airlines, railroads, pedestrian white stripes, or bicycle lanes when there is a physical break-in at a local bank or at someone's home, so why blame the network for the theft of a file of credit card accounts or for the disclosure of some memo on a server?

[5] We take encryption to be, optimally, a host's responsibility. For example if two polyglot individuals wanted to communicate in public but in a semi-secure manner in a place where the prevalent language might be A, then they could switch to language B; it would not be the responsibility of the "air" (the communication channel) to provide security—naturally these issues could be debated at infinitum, but we argue that perhaps one way to move the discourse along is to re-focus the security issue less on the network and more on the host/perimeter/bastion. We take perimeter security (including firewalls) to be a form of host-level security and not an intrinsic long-haul network issue per se. While the network could be enhanced to provide link-level encryption, why would the host be relieved of this responsibility?

[6] While the majority of the infractional code often arrives to the IT resource over the network, we take the position that the responsibility of blocking such threats lies with the perimeter defense mechanism and ultimately with the host/server and/or application.

Social Security numbers of 45,000 employees and retirees. "These government systems should be the best in the world and apparently they are able to be compromised," said an FAA contracts attorney. "*Our information technology systems people need to take a long hard look at themselves and their capabilities. This is malpractice in their world*" [LOW200901].

A more inclusive, systematic view of security is needed. Even then, what is required by organizations is more than just an intellectual recognition that security is a critical area of IT: What is needed is the establishment of a reliable and repeatable plan on how to reduce risk and how to comply with the regulatory mandates in a cost-effective manner. Risk management is a facet of regulatory compliance. Risk management encompasses the establishment of processes for risk assessment, processes for risk mitigation planning, processes for risk mitigation implementation, and processes for effectiveness evaluation and assessment. Furthermore, it must be recognized at the outset that given the fragmented state of the field of security, *people* are the key line of defense for managing exogenous and endogenous security events and to mitigate the ensuing risk exposures. As a point of reference, institutional spending on IS security was at $30 billion in 2005, yet, in spite of these investments, losses in excess of $15 billion were thought to occur because of security breaches. While the industry is seeing the emergence of new technologies for security control and compromise detection, there is, according to observers "a relative dearth of insights that help firms to understand the socio-organizational challenges of managing the deployment and use of these tools to prevent IS security compromises" [BEA200801]. Tools do not run themselves; therefore, experienced professionals operating in viable, well-supported teams are required. People are almost invariably the largest cost component over time of any IT initiative; hence, optimization of the human capital is the first precept for establishing an information security program that deals effectively and reliably with risk management. Our focus in this text, therefore, includes the people, teams, and human resources needed to carry out these tasks.

It is critical, therefore, for organizations and enterprises to develop

(i) Technological and procedural information security and risk management capabilities and
(ii) "Ready-to-go" human resources

to (a) address vulnerabilities and risk exposures that likely will impact the organization in the years to come and (b) be able to deal with information security and risk management in an effective manner. The fundamental goal of the risk management process, and of the team that owns this responsibility, is to protect the organization's ability to perform its mission, not just to protect its IT assets. It follows that the risk management process should not be treated primarily or exclusively as a technical function carried out by the IT or packet-level experts who operate and manage the IT system, or some perimeter firewall, but as an essential management function of the organization at senior levels [STO200201].

We show later in the book (Chapter 8) that some heuristic/empirical guidelines are as follows:

- For low probability of risk exposure the company revenue must be at around $4B/year, before one full time equivalent (FTE) dedicated to risk management is justified. For revenue of $16B/year, 2–3 FTEs are justified.
- For a relatively high probability of risk exposure the company revenue must be at around $1B/year, before one FTE dedicated to risk management is justified. For revenue of $16B/year, a team of 8–11 FTEs is justified.

These observations provide a rough order of magnitude (ROM) estimate for a risk management/assessment team that is sized to ‘‘pay for itself’’ in terms of remediated risk to the organization. Again, these are just guidelines, however, they provide some critical insight to the challenge an organization will face to justify the resources required to implement a risk management team. Many smaller companies will still need an employee serving in the risk assessment function even if the guidance does not quite add up. It is also important to note that many security practitioners in organizations often wear many hats and do not focus solely on risk management. The estimates provided are for FTE that are completely dedicated to fulfilling the risk management function.

1.1.2 Text Scope

With these observations as a backdrop, this book identifies risk management techniques and standards. It then discusses how to best assemble and maintain the *team of people* that will make effective, proactive, reliable, and on-target use of the available security framework mechanisms and tools to establish a risk-minimized IT environment. Some people have called these teams risk assessment teams (RATs); however, the term risk management team (RMT) or risk assessment and management team (RAMT) or even risk management and assessment team (RMAT) may be more appropriate and/or inclusive.[7] For the purposes of this text we will refer to the risk management team. The job function of a risk management team is to (a) assess the risk that ensues from vulnerabilities and/or from risk events and (b) identify and implement risk mitigation solutions. Some large organizations may have a team focused just on risk assessment and a separate team for risk mitigation. Smaller firms may have a small team of people (perhaps as small as one person) to handle the entire risk management function. The focus of this book is on deploying *risk management capabilities and the supportive team* within the organization.

[7] Just assessing a risk exposure may be of limited utility for an organization; preferably, one wants to assess and then correct/mitigate these risk exposures.

We observe yet again that risk management teams are much more than a collage of router-level specialists that have intimate familiarity with packet and state-machine formats for TCP, User Datagram Protocol (UDP), Real Time Protocol (RTP), Session Initiation Protocol (SIP), Hyper Text Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), IPsec, and so on, although this familiarity helps—they are part of teams that have a deep overall understanding of asset protection that encompasses a computer-, protocol-, financial-, organizational-, procedural-, probabilistic-, and game-theoretic view of the entire business of information security. Companies have known for many years (decades, in fact) how to assemble R&D teams, marketing teams, sales teams, engineering teams, operations teams, quality assurance (QA) teams, and HR teams, but IT risk management teams represent (by necessity) a new construct; unfortunately, there is limited established precedent for organizational dynamics in this arena. This is the issue under study in this book. While a search at an online bookseller with the keywords “computer security” identifies over 8000 items/books, a search with the keywords “information technology risk management” yields only a handful of relevant titles[8] (see Appendix 1.A for a compilation of some titles); finally, a press time search on keywords “security, HR, staffing, people, professionals” or variants yields even less relevant titles.

Punctuating the observations just made, to ultimately be successful, organizations have a requirement to develop “ready-to-go” technological and human resources to assess and address the universe of IT-related risk events, threats, and vulnerabilities; this is the case because IT liabilities cascade almost immediately into direct business liabilities. Studies show that automated system security vulnerability assessment tools by themselves are insufficient for complete risk analysis, not to say remediation: A team of effective practitioners is required to make customized use of the tools, correctly interpret findings, and apply appropriate, cost-effective remediation (also referred to as mitigation). This textbook takes a practical approach in its goal of describing how organizations can position themselves to properly handle the ever-increasing and perennially mutating risk exposures to their business-critical IT assets. There are many stakeholders involved in risk management, as shown in Table 1.3. Consequently, this book aims at assisting Chief Information Officers (CIOs), Chief Financial Officers (CFOs), Chief Technology Officers (CTOs), Chief Security Officers[9] (CSOs), and other technical officers, as well as *design, deploy, and run* an effective information security risk management program in their specific environments.

One useful perspective on security is the following [ENI200801]:

[8] A number of texts cover the concept of reducing project risk by proper Project Management techniques; this is not the topic of interest here.

[9] The term “Chief Information Security Office (CISO)” or “Information System Security Officers (ISSO)” is also used in the literature.

TABLE 1.3. Risk Management Stakeholders

Business and functional managers	Consumers (customers) of the IT development process
Chief Security Officer	Responsible for IT security (also known in some quarters as Chief Information Security Officer (CISO))
Commercial and federal Chief Information Officers	Senior managers that ensure the implementation of risk management for agency IT systems and the security provided for these IT systems
Corporate governance review board (a designated approving authority)	Responsible for the ultimate decision on whether to allow operation of an IT system (may also be known as a Steering Committee)
Information managers	Owners of data stored, processed, and transmitted by the IT systems
Information system auditors	Auditors of IT systems for financial, regulatory, and functional integrity
IT consultants	Professionals and contractors supporting clients in risk management
IT quality assurance personnel	Associates that test and ensure the integrity of the IT systems and data
IT security program managers	Managers that implement the security program
IT system and application developers (programmers)	Associates that develop and maintain software (e.g., applications, middleware, web services-based systems)
IT system managers	Owners of system software and/or hardware used to support IT functions
IT vendors	Develop (security) systems or packages that are used by organizations
Risk Management and Remediation Team	Responsible for comprehensive risk management (identification, assessment, containment) and security assurance
Senior management	Management individuals that make decisions about the IT security budget
Senior officers	Chief Information Officers (CIOs) and Chief Security Officers (CSOs) already mentioned above, along with Chief Financial Officers (CFOs), Chief Technology Officers (CTOs), and Chief Operating Officer (COO), all of whom make strategic decisions about the direction of the organization; the mission owners; the Chief Executive Officer (CEO) also bears responsibility
Technical security support personnel	Responsible for security architecture, security policies, security analysts
Technical support personnel	Manage and administer security for the IT systems (e.g., network, system, application, and database administrators)

- IT security administrators should expect to devote approximately one-third of their time addressing technical aspects; the remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk exposures, addressing contingency planning, and promoting security awareness.
- Security depends on people more than on technology.
- Employees are a far greater threat to information security than outsiders.
- Security is like a chain: It is as strong as its weakest link.
- The degree of security depends on three factors: the risk that one is willing to tolerate, the functionality of the system, and the costs that one is prepared to pay.
- Security is not a status or a snapshot but an ongoing process.

The goal of this text is to help corporate stakeholders and officers to understand what it takes to deploy the array of requisite security line-functions, human assets, functional processes, decision-making methods, and support tools/mechanisms/controls in order to effectively address risk management and in order to establish reliable remediation programs. The text surveys industry approaches, best practices, and standards for how an organization can position itself to properly handle the ever-increasing and constantly mutating tsunami of risks exposures. Overall, the discussion places emphasis on designing, implementing, and “feeding and caring” for a risk assessment function and the supporting team that can properly engage to foresee, prevent, and/or rapidly remediate potential business-disrupting infractions. The book has two major sections.

Part 1 reviews industry practices in the area of risk assessment methodologies and mitigation. It provides an overview of available security risk analysis standards. In particular, the ISO/IEC 27000 series (“ISO27k”) information security management standards are reviewed, along with numerous other standards such as AS/NZS 4360:2004, a risk management standard published jointly by Australia Standards and New Zealand Standards. This section also provides an overview of available security risk analysis methods. In particular, Control Objectives for Information and Related Technology (COBIT), which provides a comprehensive model guiding the implementation of IT governance processes/systems including information security controls, is reviewed, along with other methods such as OCTAVE, which, as noted, is a risk-based strategic assessment and planning technique for security published by CERT.

Part 2 focuses on developing “ready-to-go” technological and human resources within the organization, to effectively undertake the risk assessment and mitigation function. It looks at IT people issues, procedures, tools, and preparedness, and it places emphasis on implementing a risk assessment and management team that can properly foresee, prevent, and/or rapidly remediate potential infractions. It is then subdivided into two sections. The first section looks at the HR (organizational) factors related to the assembly, maintenance, expansion, and ongoing retraining of the staff that owns the information security program. It speaks to the IT/security "people issues," procedures, tools, and preparedness. Furthermore, because security is a "hot" industry, institutions need to establish the proper environment so that the staff's churning will be kept at a bare minimum and so that the security policy can be safeguarded. The second section then takes a more in-depth and real world approach as to the ongoing risk management process and builds off the material covered in the first section of the book.

There is a realization that effective leadership within the top levels of the organization and its related security functions are imperative: Organizational reputation, the uncompromised reliability of the technical infrastructure and normal business processes, protection of physical and financial assets, the safety of employees, and shareholder confidence all rely in various degrees upon the effectiveness of an accountable senior security executive [CSO200301]. What has generally been lacking, however, is a specific position at the senior governance level with the responsibility for developing, influencing, and directing an organization-wide protection strategy: In many organizations, accountability is diffused and is often shared among several managers in distinct departments, with ostensibly conflicting objectives. To address this issue, the establishment of a CSO function has proven useful. In turn, the risk assessment and remediation team discussed in this book would likely report into this focused organization. However, in some organizations a Chief Risk Officer (CRO) may oversee an entire organization that handles all risk management for the enterprise.

Security techniques have been around since the 1970s. Naturally, threats and vulnerabilities have evolved and mutated, and many new ones have emerged. Nonetheless, a sizeable number of the basic techniques remain the same; for example, sensitive data stored on removable media should be stored in an encrypted fashion (or at least the key data fields within that file), yet one continues to read stories of lost tapes, lost PCs, and lost memory sticks, all of which exposes critical data to a situation where there is a positive nonzero risk. According to the Open Security Foundation's DataLossDB, a project that documents known and reported data loss incidents worldwide, in 2008 alone there were approximately 246 incidents reported that could have most likely been avoided with a proper encryption solution deployed.

At this juncture, there is a broad understanding that the skills and competencies essential to achieving active protection and implementing measurably effective responses to the modern threat environment are far more critical than ever before [CSO200301]. Yet, few companies have a comprehensive, high-assurance company-wide mechanism in place. Furthermore, today more often than not, business continuity, security, and risk management are relegated to a handful of engineering-level individual(s). Surveys show that a majority of companies spend relatively little on security, even in the face of the avalanche of increased threats (caused by geopolitical events, higher penetration of Internet access to “rouge” countries, greater deployment of “weak” web-based software, etc.) Many Fortune 500 companies with thousands of IT professionals on staff may have no more than 6–12 security people on-board, and the majority of these people may only focus on implementing and maintaining perimeter defenses using packet-level firewalls. Some information-based companies have been in business for a decade or more and still do not have a security architecture in place. This is a mismatch between the potential risk and the resources allocated to counter the risk exposure.

The Information Security Forum’s biennial information security status survey leads to the conclusion that because information risk is not well understood or managed, on average a business-critical information resource [CIT200701]

- Suffers an information incident almost every working day (average of 225 incidents a year)
- Has a 58% chance of experiencing a major incident over the course of a year

By implementing risk management, an organization not only will be able to reduce the information risk exposure it faces (reducing the chance of suffering major incidents), but also can save monetarily by reducing risk (which is, as defined here, the expected losses incurred from exposures). Controls cut the number of minor incidents suffered day-to-day, along with the inefficiencies that go with them. Unfortunately, according to the European Network and Information Security Agency (ENISA), some “open” problems in the area of risk management include [ENI200801] the following:

- Low awareness of risk management activities within public and private sector organizations
- Absence of a “common language” in the area of risk management to facilitate communication among stakeholders
- Lack of surveys on existing methods, tools and good practices
- Limited or nonexistent interoperability of methods and integration with corporate governance

At the same time, it is important that organizations have a balanced and proportionate response to the risk exposures affecting them. Risk management should thus help avoid an overreaction to risk exposures that can unnecessarily prevent legitimate activity and/or seriously distort resource allocation [ISO31000].

Finally, with the ongoing focus on cost reduction, security professionals are being asked to quantify the benefit that security brings to the business. Return on security investment (ROSI) is one such measure being used. A number of definitions and methodologies for calculating ROSI have been advanced of late. Some methods follow traditional financial return on investment (ROI) theory—for example, total cost of ownership—while others use concepts from fields such as insurance.

Current approaches to information security risk management are seen by industry observers as being incomplete in the sense that they fail to include all components of risk (assets, threats, and vulnerabilities). In addition, many organizations outsource information security risk evaluations, leading to generalizations rather than a company-specific determination. Self-directed assessments (as discussed in the chapters that follow) provide the context to understand the risks and to make informed decisions and tradeoffs [CAR200101]. To undertake effective self-directed assessments, a well-functioning risk management team is needed.

Risk management practitioners have identified components that must be in place prior to the implementation of a successful security risk management process and that must remain in place once it is underway; these practitioners list the following [MIC200601]:

- Executive sponsorship
- A well-defined list of risk management stakeholders
- Organizational maturity in terms of risk management
- An atmosphere of open communication
- A spirit of teamwork
- A holistic view of the organization
- Authority throughout the process

This book addresses these issues and walks a security manager through the process of developing and implementing an organizational machinery that will be able to identify and handle risks for their company. It takes a look at the current state of the software vulnerabilities from a general perspective and how they are handled. Then it walks the reader through an analysis of how risks relate to their organization. It is critical to create policies, standards, guidelines, and procedures that enable an organization to identify and mitigate information security risks. An effective team, perhaps less steeped in an avalanche of acronyms in their daily parlance, is potentially best-suited to address these issues.

ISO/IEC 27002 notes that: “Information can exist in many forms: it can be printed or written on paper, stored electronically, transmitted by post using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected.” The IT organization typically manages the shared infrastructure of the enterprise, such as the servers, mainframes, data warehouses, networks, and intranets and, as such, operates as the custodian for a large portion of the corporate information content (including possibly information belonging to customers—e.g., credit card numbers, addresses, telephone numbers—and business partners.) However, with the trends to a mobile laptop/PDA-based workforce, not all an organization's information assets are managed by the IT organization. These information owners—including end users—need to strive to ensure that their information assets are protected; hence, in a microcosm, the techniques discussed here for IT are applicable to these users, as well.

REFERENCES

[BEA200801] J. Beachboard, A. Cole, et al. "Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda," *Issues in Informing Science and Information Technology*, Volume 5, 2008, Proceedings of Informing Science, Informing Science Institute.

[CAR200101] Carnegie Mellon, Software Engineering Institute, *OCTAVE^{SM} Method Implementation Guide Version 2.0, Volume 1: Introduction*, C. J. Alberts, and A. J. Dorofee, June 2001.

[CIT200701] Driving information risk down to an acceptable level, using FIRM and Citicus ONE, Whitepaper, 2007. Ref. A020-R231. Citicus Limited, Holborn Gate, 330 High Holborn, London WC1V 7QT, United Kingdom.

[CSO200301] *Chief Security Officer (CSO) Guidelines*, ASIS Commission on Guidelines, ASIS International, November 24, 2003, 1625 Prince Street, Alexandria, VA 22314–2818, USA, www.asisonline.org

[ENI200801] European Network and Information security Agency (ENISA), 2008.

[HUB200701] D. Hubbard, *How to Measure Anything: Finding the Value of Intangibles in Business*, p. 46, John Wiley & Sons, Hoboken, NJ, 2007.

[ISO31000] ISO/TMB WG on Risk management, ISO/CD 31000, *Risk Management—Guidelines on Principles and Implementation of Risk Management*, ISO 2007.

[ITP200901] IT Policy Compliance Group, Managing Spend on Information Security and Audit for Better Results, February 2009, Managing Director, Jim Hurley.

[LOW200901] J. Lowy, "*FAA says Hackers broke into agency computers*," Associated Press, Feb. 10, 2009.

[MAR200601] *MAGERIT, Version 2: Methodology for Information Systems Risk Analysis and Management. Book I—The Method*, Published by Ministerio de Administraciones Públicas, Madrid, 20 June 2006 (v 1.1), NIPO: 326-06-044-8.

[MIC200601] Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence, *The Security Risk Management Guide*, Microsoft Corporation, Redmond, WA, 2006.

[STO200201] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems—Recommendations of the National Institute of Standards and Technology", Special Publication 800–30, July 2002, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899–8930. [This document may be used by nongovernmental organizations on a voluntary basis. It is not subject to copyright.]

APPENDIX 1A: BIBLIOGRAPHY OF RELATED LITERATURE

1A.1 Scantiness of Risk Management Teams References

An assessment of the literature shows that there is little on the market for senior corporate planners and decision-makers to review that takes the perspective of *holistic corporate business continuity and security*, including proven approaches to IT risk management. Many of the guides on the market utilize a piecemeal formulation of the integrity, reliability, and survivability challenges of an organization; for example, they typically look *discretely* at firewalls, intrusion detection systems, security on Unix, Linux security, virus management, e-mail security, and so on. Furthermore, there is little on the topic of how to develop ready-to-go teams within the organization to proactively address and rapidly dispose of risks to the IT/networking infrastructure that will impact the organization in the years to come, which is the topic of the present text.

Some of the titles are shown below.

- A. Shoniregun, *Impacts and Risk Assessment of Technology for Internet Security: Enabled Information Small Medium Enterprises*, ISBN-13 9780387243436, Springer, New York, 2005.
- B. Schneier, *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, Hoboken, NJ, 2004.
- B. Sterneckert, *Critical Incident Management*, ISBN 084930010X, CRC Press, Boca Raton, FL, 2003.
- C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE(sm) Approach*; Addison-Wesley; Boston, MA; 2002.
- D. L. Anderson and G. V. Post, *Managing Information Systems: Using Cases within an Industry Context to Solve Business Problems with Information Technology*, ISBN 0201611767, Pearson Education, Upper Saddle River, NJ, 1999.
- E. Jordan and L. Silcock, *Beating IT Risks*, ISBN-13 9780470021903, John Wiley & Sons, Hoboken, NJ, 2005.
- G. E. Beroggi (editor) and W. A. Wallace (editor), *Computer Supported Risk Management*, ISBN-13 9780792333722, Springer, New York, 1995.
- G. E. Beroggi and W. A. Wallace, *Operational Risk Management: The Integration of Decision, Communications and Multimedia Technologies*, ISBN-13 9780792381785, Springer, New York, 1998.
- G. Hoffman, *Managing Operational Risk: 20 Firmwide Best Practice Strategies*, ISBN 0471412686, John Wiley & Sons, Hoboken, NJ, 2002.
- G. Stoneburner, A. Goguen, A. Feringa, *Risk Management Guide for Information Technology Systems and Underlying Technical Models for Information Technology Security*, ISBN 0756731909, Diane Publishing Company, Darby, PA, 2002.

- G. Stoneburner, *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, ISBN 0160674492, United States Government Printing Office, Washington, DC, 2002.
- G. Westerman and R. Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, ISBN-13 9781422106662, Harvard Business School Press, Boston, MA, 2007.
- I. Lim, *Information Security Cost Management*, ISBN-13 9780849392757, CRC Press, Boca Raton, FL, 2006.
- J. Armstrong, D. Dresner, and M. Rhys-Jones, *Managing Risk: Technology and Communications*, ISBN-13 9780754524687. Butterworth-Heinemann, Oxford, UK, 2004.
- J. Bryson, *Managing Information Services: A Transformational Approach*, ISBN-13 9780754646310, Ashgate Publishing, Aldershot, Hampshire, UK, 2006.
- J. F. Kuong (Editor), *Threats and Risks Compendium for Enterprise Risk Management: A Model to Reduce Your Organization's Exposure from All Types of Vulnerabilities*, Volume. 1: *Physical Access Perimeter*, ISBN 0940706628, Management Advisory Publications, Wellesley Hills, M. 2003.
- J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Auerbach, Boca Raton, FL, 2005.
- A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, ISBN-13 9780321349989, *Symantec Press Series*, Cupertino, CA, 2007.
- M. D. Lutchen, *Managing IT as a Business: A Survival Guide for CEO's*, ISBN 0471471046, John Wiley & Sons, Hoboken, NJ, 2003.
- M. E. Whitman and H. J. Mattord, *Principles of Information Security*, third edition, ISBN-13 9781423901778, Course Technology, Florence, KY, 2008.
- N. G. G. Carr, *Does IT Matter? Information Technology and the Corrosion of Competitive Advantage*, ISBN 1591394449, Harvard Business School Publishing, Boston, MA, 2004.
- R. Baskerville (Editor), J. Stageman, and J. I. DeGross (editor), *Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8.2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology*, June 9–11, 2000, Aalborg, Denmark, ISBN-13 9780792378365, Springer, New York, 2000.
- R. E. Susskind, *The Future of Law: Facing the Challenges of Information Technology*, ISBN-13 9780198764960, Oxford University Press, New York, 1998.
- T. R. Peltier, *Information Security Risk Analysis*, second edition, Auerbach, Boca Raton, FL, 2005.

1A.2 Scantiness of Host Security References

The literature on host security is rather scant. Below are the first 40 hits under a Google Book search with the exact expression "host security." Even 500-page books have just a few pages (if any) on the topic of host security. Most of the literature emphasis seems to be on the simpler issues of blocking TCP ports by a firewall, what people call "network security" (but should in fact be called fixed-network perimeter security, as contracted to mobile devices—such a employee PCs used at airports and coffee shops—simply entering the network and bypassing the firewall). With the increased penetration of mobile devices and the expected introduction of IPv6 in the next few years, the issue of host security needs to get renewed attention.

(*Note:* The title *Web Commerce Technology Handbook* in the Google list is by one of these authors.)

(*Note:* The term "endpoint security" is now also being used to refer to host-based security; however, a search on that term only yielded one text at press time: M. Kadrich, *Endpoint Security*, Addison Wesley Professional, Pub. Date: April 2007, ISBN-13: 9780321436955.)

Information Security Management Handbook, Page 267
by Harold F. Tipton, and Micki Krause, Business & Economics, 2005, 578 pages
CRM Host Security The security of the host and the network is often focused on by security professionals without a good understanding of the intricacies of . . . .

Web Security, Web Security, Privacy and Commerce, Page 396
by Simson Garfinkel, and Gene Spafford, Computers, 2001, 756 pages
CHAPTER 15 Host Security for Servers. In this chapter: • Current Host Security Problems Securing the Host Computer • Minimizing Risk by Minimizing Services . . . .

Firewalls and Internet Security: Repelling the Wily Hacker, Page 253
by William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, 1996
In some small companies, the developers might have a small collection of UNIX-based hosts with strong host security, but the sales and management teams may . . . .

A Practical Guide to Red Hat Linux 8: Fedora Core and Red Hat Enterprise Linux, Page 1416
by Mark G. Sobell, Computers, 2003, 1616 pages
. . . Host Security. Your host must be secure. Simple security steps include preventing remote logins and leaving the /etc/hosts. equiv and individual users' . . . .

LPI Linux Certification in a Nutshell, Page 445
by Steven Pritchard, Bruno Pessanha, Linux Professional Institute, Linux Professional Institute, Nicolai Langfeldt, Jeff Dean, and James Stanger, Computers, 2006, 961 pages

Objective 2: Set Up Host Security Once a Linux system is installed and working, you may need to do nothing more to it. However, if you have specific . . . .

Surviving Security: How to Integrate People, Process, and Technology, Page 241
by Amanda Andress, Computers, 2003, 502 pages

ATA In general, host security addresses weaknesses in default operating . . . . One of the biggest issues with host security is that it does not scale well. . . .

Linux and Windows: A Guide to Interoperability, Page 376
by Ed Bradford, and Lou Mauget, Computers, 2002, 430 pages

Host Security. Let us discuss physical access, local software system . . . . At the host security level, it would be as secure as the room, but quite useless. . . .

Building Internet Firewalls: Internet and Web Security, Page 19
by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, Computers, 2000, 869 pages

A host security model may be highly appropriate for small sites, ... Indeed, all sites should include some level of host security in their overall security . . .

Web-to-Host Connectivity - Page 116
by Anura Gurugé, Lisa Lindgren, and Computers, 2000, 566 pages

WEB-TO-HOST SECURITY Security is one of the most pressing concerns confronting IT managers, but one that has received scant attention in the emerging . . . .

Network Security Hacks: 100 Industrial-Strength Tips & Tools, Page 1
by Andrew Lockhart, Computers, 2004, 298 pages

CHAPTER ONE Unix Host Security Hacks-20 Networking is all about connecting computers together, so it follows that a computer network is no more secure . . . .

Information Security and Cryptology: ICISC 2000, Third International . . . , Page 256
by Dongho Won, Computers, 2000, 260 pages

It may exchange the host security information with other agents to find out . . . . Agent Report Manager generates the host security evaluation result report . . . .

Handbook of Information Security: Threats, Vulnerabilities, Prevention . . . , Page 153
by Hossein Bidgoli, Technology & Engineering, 2006, 3366 pages

Figure 3: (a) interagent security, (b) agent–host security, ... In agent–host security, we can distinguish two aspects: (bl) host security and (b2) agent . . . .

Apache Security: The Complete Guide to Securing Your Apache Web Server, Page 224
by Ivan Ristic, Computers, 2005, 396 pages

. . . host security . . .

Security Technologies for the World Wide Web, Page 50
by Rolf Oppliger, Computers, 2003, 416 pages

Host security is generally hard to achieve and does not scale well in the sense that as the number of hosts increases, the ability to ensure that security . . . .

Linux All-in-One Desk Reference for Dummies, Page 552
by Naba Barkakati, Computers, 2006, 840 pages

. . . to many vulnerabilities, such as denial of service, execution of arbitrary code, and root-level access to the system. Host security . . . .

Data Networks: Routing, Security, and Performance Optimization, Page 377
by Tony Kenyon, Computers, 2002, 807 pages

Example design l: simple end-to-end host security. As shown in Figure 5.20, two hosts are connected through the Internet (or an intranet) without any IPSec . . . .

Designing a Total Data Solution: Technology, Implementation and Deployment, Page 183
by Roxanne E. Burkey, and Charles V. Breakfield, Computers, 2000, 499 pages

GATEWAY-TO-HOST SECURITY Gateway security is often not considered until after the product is inhouse and already being used for development. . . .

Designing and Building Enterprise Dmzs, Page 617
by Ido Dubrawsky, Hal Flynn, and C. Tate Baumrucker, Computers, 2006, 714 pages

Testing Bastion Host Security. Whether you are implementing a bastion host from scratch or securing one that you inherited, the first step will be to test . . . .

SUSE Linux 10 For Dummies, Page 290
by Nabajyoti Barkakati, Computers, 2005, 356 pages

Understanding Linux Security. To secure a Linux system, you have to tackle two broad categories of security. issues: *<* Host security issues that relate to. . . .

Security + Certification: Exam Guide, Page 9
by Gregory B. White, Computer Networks, 558 pages

Security Principles There are three ways an organization can choose to address the protection of its networks: Ignore security issues, provide host security.

Master Data Management and Customer Data Integration for a Global Enterprise, Page 160

by Alex Berson, Larry Dubov, and Lawrence Dubov, Computers, 2007, 432 pages

Platform (Host) Security Platform or host security deals with the security threats that affect the actual device and make it vulnerable to outside or . . . .

Network Security Hacks, Second Edition, Page 58

by Andrew Lockhart

. . . CHAPTER TWO: Windows Host Security Hacks 23–36. This chapter shows some ways to keep your Windows system up-to-date and secure, thereby making your. . . .

Securing Ajax Applications: Ensuring the Safety of the Dynamic Web, Page 103

by Christopher Wells, Computers, 2007, 233 pages

Host Security Image your web server as a gladiator about to go into battle. If it's going to have any chance of survival, it must be battle ready. . . .

Red Hat Enterprise Linux 4 For Dummies, Page 147

by Terry Collings, Computers, 2005, 408 pages

Implementing Host Security After you have a basic understanding of system security (as explained in the first part of this chapter), look at specific . . . .

How to Cheat at Designing a Windows Server 2003 Active Directory . . . , Page 382

by Brian Barber, Melissa Craft, Melissa M. Meyer, Michael Cross, and Hal Kurz, Computers, 2006, 505 pages

. . . Host security . . .

Network Security Architectures: Expert Guidance on Designing Secure Networks, Page 142

by Sean Convery, Computers, 2004, 739 pages

Unlike identity technologies for which you wouldn't implement both OTP and PKI for the same application, host security options can be stacked together to . . . .

LPI Linux Certification in a Nutshell: A Desktop Quick Reference, Page 458

by Jeffrey Dean, Linux Professional Institute, Computers, 2001, 551 pages

Objective 2: Set Up Host Security Once a Linux system is installed and working, you may need to do nothing more to it. However, if you have specific . . . .

Building DMZs for Enterprise Networks, Page 121
by Robert Shimonski, Thomas W. Shinder, and Will Schmied, Computers, 2003, 744 pages

Host Security Software. Ensuring the reliability and integrity of the DMZ system means using host integrity- monitoring software to report activity that . . . .

Building Internet Firewalls, Page 15
by D. Brent Chapman and Elizabeth D. Zwicky, Computers, 1995, 517 pages

Even with all that work done correctly, host security still often fails due to bugs in . . . . Host security also relies on the good intentions and the skill of . . . .

MAC OS X Internals: A Systems Approach, Page 1050
by Amit Singh, Computers, 2006, 1641 pages

The host special ports are host port, host privileged port, and host security port. These ports are used for exporting different interfaces to the host . . . .

Multi-operating System Networking: Living with Unix, Netware, and NT
by Raj Rajagopal, Computers, 2000, 1360 pages

GATEWAY-TO-HOST SECURITY. Gateway security is often not considered until after the product is in-house and already being used for development. . . .

Smart Card Security and Applications, Page 141
by Mike Hendry, Computers, 2001, 305 pages

These devices, which are known as host security modules (HSMs), come to form an important part of host system security (see Figure 10.10). . . .

Web Security, Page 142
by Amrit Tiwana, Computers, 1999, 425 pages

Host Security Problems—Where Disaster Begins Servers commonly were based on UNIX platforms until a few years ago. NT now is becoming a dominant platform . . . .

Managing IP Networks with Cisco Routers, Page 266
by Scott M. Ballew, TCP/IP (Computer network protocol), 1997, 334 pages

When you consider these potential internal security threats, the answer to the question, "Is host security still necessary when I have a firewall? . . .

Encyclopedia of Computer Science and Technology: Volume 40, Supplement 25, Page 171
by Jack Belzer, Allen Kent, Albert G. Holzman, and James G. Williams, Computers, 1999, 500 pages

Looking at agent–host security, we can distinguish two aspects: host security . . . . The approach for achieving host security is to authenticate agents and to . . . .

RHCE Red Hat Certified Engineer Linux Study Guide: Linux Study Guide (exam . . . , Page 584

by Michael Jang, Syngress Media, Inc., Computers, 2002, 703 pages

CERTIFICATION OBJECTIVE 10.02 Basic Host Security. A network is only as secure as the most open system in that network. Although no system can be 1 00 . . . .

Web Commerce Technology Handbook, Page 124

by Daniel Minoli, and Emma Minoli, Business & Economics, 1997, 621 pages

This must be accomplished using host security mechanisms; the firewall comes into play if the . . . Host security is a discipline that goes back to the 1960s. . . .

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services . . . , Page 193

by Christopher Steel, Ramesh Nagappan, and Ray Lai, Computers, 2005, 1041 pages

. . . Host security . . .

Host Integrity Monitoring Using Osiris and Samhain: Using Osiris and Samhain, Page 103

by Brian Wotring, Bruce Potter, Marcus J. Ranum, and Rainer Wichmann, Computers, 2005, 421 pages

Table 4.1 Common Bank Security. Measures bank security, host security limited, entry/exit points (thick doors with locks), guards with guns, alarm system, . . .

Proceedings of the 1985 Symposium on Security and Privacy, April 22–24, 1985 . . . , Page 65

by IEEE Computer Society Technical Committee on Security and Privacy, Computers, 1985, 241 pages

Because host-security level information is very stable, updates of this host security table are easily accomplished by periodic manual table updates by the . . . .

CHAPTER 3

INFORMATION SECURITY RISK MANAGEMENT STANDARDS

As we have seen in the previous chapters, information security and, hence, risk management are universally applicable to all types of organizations, including commercial enterprises of various sizes (from small businesses to multinational companies), government agencies, government departments, not-for-profit institutions, academic institutions, medical institutions, media companies, banks, brokerage companies, and insurance companies—in fact applicable to any organization that creates, receives, stores, or transmits information vital to its operation. The specific information security requirements, risk exposure, and ensuing risk will be unique in each situation, but often a common approach and methodology can be employed. Risk management is the endeavor of balancing potential adverse impacts against the costs of deploying safeguards. We have already noted that IT risk management encompasses five major processes:

1. (Ongoing) identification of threats, vulnerabilities, or (risk) events impacting the set of IT assets owned by the organization
2. Risk assessment
3. Risk mitigation planning
4. Risk mitigation implementation
5. Evaluation of the mitigation's effectiveness

Fortunately, the stakeholders and risk management teams do not have to start from scratch when contemplating and/or undertaking these processes because a body of knowledge has emerged to support the risk management process. As early as 1989, the U.K. Department of Trade and Industry (DTI) established a working group that produced the User Code of Practice that was essentially a list of security controls considered good practice at the time. Figure 3.1 presents the development timeline leading to the ISO Code of Practice, ISO/IEC

Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practial Guide to Risk Management Teams, by Jake Kouns and Daniel Minoli

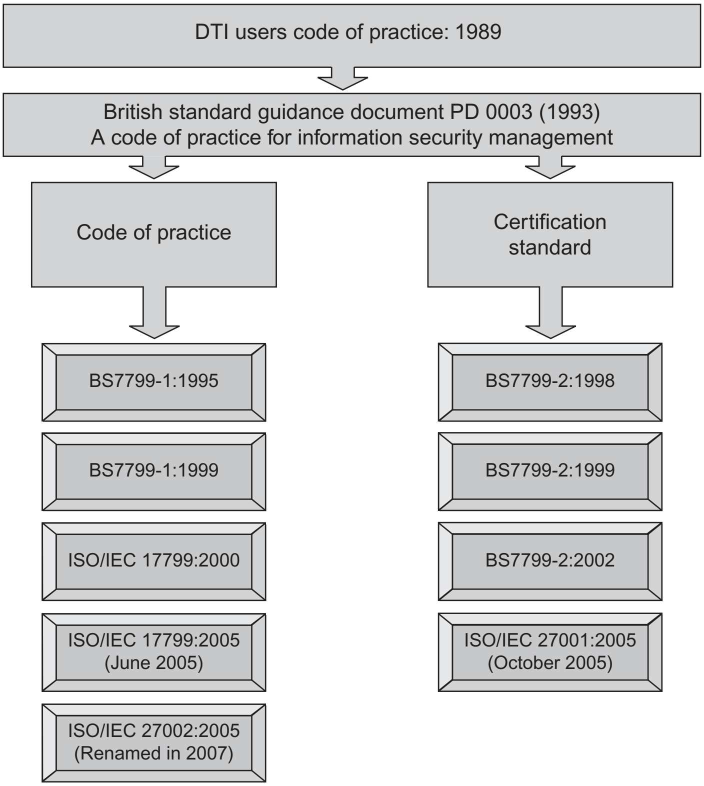

DTI users code of practice: 1989
British standard guidance document PD 0003 (1993)
A code of practice for information security management
Code of practice
Certification standard
BS7799-1:1995
BS7799-1:1999
ISO/IEC 17799:2000
ISO/IEC 17799:2005 (June 2005)
ISO/IEC 27002:2005 (Renamed in 2007)
BS7799-2:1998
BS7799-2:1999
BS7799-2:2002
ISO/IEC 27001:2005 (October 2005)

FIGURE 3.1. Timeline leading to the ISO Code of Practice, ISO/IEC 27002:2005, and the Information Security System Requirements standard ISO/IEC 27001:2005.

27002:2005 and the Information Security Systems Requirements standard, ISO/IEC 27001:2005. In addition, standards organizations in Canada, Australia/New Zealand, and Japan developed early versions of risk management standards in the mid-to-late 1990s. Beginning with the release of ISO/IEC 17799:2000, the International Organization for Standardization (ISO) got involved and has continued to expand the field of information security by producing a suite of standards.

This chapter provides a brief overview of the available information security, risk analysis standards. In particular, we will provide a general overview of ISO's[15] ISO/IEC 27000 series of information security management system standards. Table 3.1 provides a short list of the relevant information security and/or risk management standards.

[15] ISO cooperates with the International Electrotechnical Commission (IEC), hence the standards also have the IEC label

TABLE 3.1. Information Security Standards with Risk Management Relevance (Partial List)

British Standards Institute (BSI)	BS7799-1:1999, "Code of Practice for Information Security Management," was retired with the release of ISO/IEC 17799:2000. BS7799-2:2002 was the latest BSI specification for an information security management system certification. After the release of ISO/IEC 17799:2005, it was "fast tracked" by ISO to become ISO/IEC 27001:2005, the certification standard. BS7799-3:2006, "Information security management systems guidelines for information security risk management," the standard provides guidance and support for the implementation of a risk management process and is generic enough to be of use to small, medium, and large organizations. Clauses include: • Information security risks in the organizational context • Risk assessment • Risk treatment and management decision-making • Ongoing risk management activities • Examples of legal and regulatory compliance • Information security risks and organizational risks • Examples of assets, threats, vulnerabilities, and risk assessment methods • Risk management tools • Relationship between ISO/IEC 27001:2005 and BS7799-3:2006
International Organization for Standardization (ISO)	ISO/IEC 13335-1:2004, "Information technology—Security techniques—Management of information and communications technology security, Part 1: Concepts and models for information and communications technology security management." The standard contains generally accepted descriptions of concepts and models for information and communications technology security management. See text for other parts of the standard. The ISO/IEC 27000 family of information security management standards (also known as "ISO27k") ISO/IEC 27002:2005, "Code of Practice for Information Security Management." *Note*: ISO/IEC 27002:2005 was previously known as ISO/IEC 17799:2005 until renamed in 2007. The rename was initiated by the ISO, who wanted to align the information security standards under a common naming structure (the "ISO 27000 series"). ISO/IEC 27001:2005, "Information Security Management Systems—Requirements," "fast tracked" by ISO to become the certification standard paired with ISO/IEC 27002/17799:2005.

TABLE 3.1. (Continued)

	ISO/IEC 18028:2006, "Information technology—Security techniques—IT network security" Five-part standard (ISO/IEC 18028-1 to 18028-5) containing generally accepted guidelines on the security aspects of the management, operation, and use of information technology networks. The standard is an extension of the guidelines provided in ISO/IEC 13335 and ISO/IEC 17799 focusing on network security risks. ISO/IEC TR 18044:2004, "Information technology—Security techniques—Information security incident management." It provides, in part, information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used). It also provides a description of the information security incident management process. ISO DIS (Draft International Standard) 31000, "Risk Management Principles and Guidelines on Implementation" This draft standard (targeted for 2009) is based on AS/NZS 4360 and COSO-ERM and provides guidelines on the principles and implementation of risk management in general (not IT or information security specific).
National Institute of Standards and Technology (NIST)	SP 800-12, -16, -18, -23, -24, -25, -26, -30, -31, -32, -33, -34, -36, -37, -39, -41, -42, -43, -44, -45, -48, -50, -53, -55, -61, -64, -68 Computer Security Standards
Australian Standard/ New Zealand Standard (AS/NZS)	AS/NZS 4360:2004
Information Security Forum (ISF)	"The ISF Standard of Good Practice" A high-level standard promulgating a series of good practice standards related to information security. Consists of a comprehensive set of information security-specific controls: • Controls aimed at complying with legal and regulatory requirements, such as Sarbanes–Oxley Act 2002, the Payment Card Industry (PCI) Data Security Standard, Basel II 1998, and the EU Directive on Data Protection • Coverage of the main security controls in other major information security-related standards, such as ISO/IEC 27002 (17799) and COBIT The Standard of Good Practice is comprised of five parts: • Security management (enterprise-wide) • Critical business applications • Computer installations • Networks • Systems development

3.1 ISO/IEC 13335

ISO 13335 (originally a set of technical reports) embodies a set of guidelines for the management of IT security, focusing on technical security control measures. ISO/IEC 13335 is an assessor-led approach. The standard is comprised of four different parts, where the first part identifies the overall process and shows the different components necessary to complete a risk assessment.

- ISO/IEC 13335-1:2004, Information technology—Security techniques—Management of information and communications technology security, Part 1: Concepts and models for information and communications technology security management. It presents the concepts and models fundamental to a basic understanding of information and communication technology (ICT) security, and it addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. In this part of the standard the fundamental security concepts are explained; next the policy and strategy principles are explained, followed by a description of the necessary organizational structure for implementing security; and, finally, the management function, and in particular the process of risk management, is explained. This section of the standard is useful because it defines the principles that underpin an information security framework and explains in more detail the structures that support the framework [COL200701].
- ISO/IEC 13335-2, Management of information and communications technology security, Part 2: Information security risk management. This standard was intended to replace ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000. Part 2 of ISO/IEC 13335 (currently 2nd WD) provides operational guidance on ICT security.
- ISO TR 13335-3:1998 Information technologyy—Guidelines for the Management of IT Security, Part 3: Techniques for the management of IT Security. Covers techniques for the management of IT security. Has been included in ISO/IEC 27005:2008, Information security risk management (now an International Standard under publication). ISO TR 13335-3 provides guidance on implementing a risk assessment, together with a range of possible risk calculation models. It identifies four approaches to risk analysis, ranging from the baseline approach to a detailed risk assessment methodology. It identifies the process flow of risk assessment as follows [COL200701]:
  - Identification of assets to be included in the risk assessment
  - Valuation of assets and establishment of dependencies between assets
  - Threat and vulnerability assessment on the assets within the scope of the risk assessment
  - Identification of existing or planned safeguards
  - Assessment of risk exposures

- ISO TR 13335-4:2000 covers the selection of safeguards (countermeasures, meaning technical security controls). Has been included in ISO/IEC 27005:2008, Information security risk management (now a Published International Standard).

3.2 ISO/IEC 17799 (ISO/IEC 27002:2005)

ISO 17799 is used colloquially as a generic term to describe two distinct documents: ISO17799 (aka ISO 27002), which is a set of security controls (a code of practice), and ISO 27001 (formerly BS7799-2), which is a standard "specification" for an Information Security Management System (ISMS). The ISO 17799 standard has its genesis in the late 1980s in the Information Security "Code of Practice" from the UK's Department of Trade and Industry. The initial release of BS 7799 was based to a degree on an internal document by the Royal Dutch/Shell Group entitled Information Security Policy Manual. The manual's emphasis on mainframe security concepts and lack of explicit considerations related to the Internet suggests that it was based on material developed at an earlier point in time.

In 1995 the British Standards Institute (BSI) (now known as BSI British Standards[16]) released British Standard BS7799.[17] A second part, BS7799-2:1998, to be used for certification purposes, was added in February 1998. The first revision of the standard, BS7799:1999, followed a public consultation period and resulted in an extensive revision which was released with Part 1 and Part 2 in April 1999. BS7799-1:1999 was proposed as an ISO standard via the "Fast Track" mechanism in October 1999 and was published with minor amendments as ISO/IEC 17799:2000 in December 2000.

BS 7799-2:1999 was revised and officially launched in September 2002, as BS7799-2:2002 and was used for ISMS certification audits until the release of ISO/IEC 27001:2005 in October 2005. The latest revision of the ISO/IEC 17799 standard followed another consultation period and resulted in an extension that which was released in June 2005 as ISO/IEC 17799:2005. BS7799-2:2002 was revised and released in October 2005 as an ISO standard, ISO/IEC 27001:2005. The most recent change was in name only when ISO/IEC 17799:2005 was changed to ISO/IEC 27002:2005. More information on both standards is provided below.

The reader should focus on the 27000 series described next.

3.3 ISO/IEC 27000 SERIES

The ISO/IEC 27000 series of standards (also known as "ISO27k") provides a comprehensive introduction to information security, risk management,

[16] BSI British Standards is the National Standards Body of the UK.

[17] BS 7799:1995 is retired at this juncture, except for Part 3.

and management systems. The 27000 series is a family of information security management standards that provides, generally accepted best practices and guidance on establishing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS. An ISMS aims at protecting the confidentiality, integrity, and availability of the information and information processing facilities within an organization. The ISMS is in effect the information security governance/management processes that is and/or can be used by an organization to handle information security and risk management. These standards are intended to be used as a group to establish, operate, monitor, review maintain, improve, and gain certification for a documented ISMS. See Table 3.2 for a listing of standards in this family. As of press time, only ISO/IEC 27001, 27002, 27005, and 27006 were actually issued.

Note: Some material in this section is sourced to the ISO27k Implementers Forum (http://www.iso27001security.com) [IMP200801], a global community of nearly 1500 information security professionals who are actively using the ISO/IEC 27000 series standards.

3.3.1 ISO/IEC 27000, Information Technology—Security Techniques—Information Security Management Systems—Fundamentals and Vocabulary (Draft at Press Time)

ISO/IEC 27000 specifies the fundamental principles, concepts, and vocabulary for the ISO/IEC 27000 series of recommendations. ISO/IEC 27000 (under development at press time) aims at describing the fundamentals and vocabulary. It is a recognized fact that several key terms in information security (such as “risk”) have different meanings according to the context and the user or user community. In general, few people define terms precisely; this invariably creates confusion and impairs formal assessment—hence the value of a vocabulary (and this is also why we have defined the terms we use in Chapter 2). ISO/IEC 27000 was at Final Draft or Distribution International Standard (FDIS) stage at press time, with a 2009 publication target.

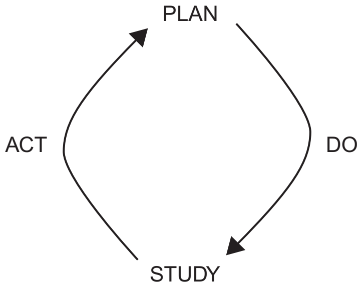
3.3.2 ISO/IEC 27001:2005, Information Technology—Security Techniques—Specification for an Information Security Management System

ISO/IEC 27001:2005 was published as an ISO standard in October 2005. The standard defines the requirements for an ISMS. An ISMS is a management system for dealing with information security risk exposures—namely, a framework of policies, procedures, physical, legal, and technical security controls forming part of the organization’s overall risk management processes. The standard specifies a set of requirements for the establishment, implementation, monitoring and review, maintenance, and improvement of an ISMS. ISO/IEC 27001 incorporates Deming’s Plan-Do-Check-Act

TABLE 3.2. ISO/IEC 27000 Series of Standards

ISO/IEC 27000	(under development) Standard will provide an overview/ introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.
ISO/IEC 27001:2005	ISMS requirements specification used for the certification of an organization's ISMS.
ISO/IEC 27002:2005	Standard that encompasses the code of practice for information security management describing a set of information security control objectives and a set of generally accepted best practice security controls.
ISO/IEC 27003	(under development) Standard will provide implementation guidance for ISO/IEC 27001.
ISO/IEC 27004	(under development) Standard will be an information security management measurement standard recommending metrics to facilitate an improvement in the effectiveness of an ISMS.
ISO/IEC 27005:2008	A key information security risk management standard that provides advice on information security risk management.
ISO/IEC 27006:2007	A guide to the certification or registration process for accredited ISMS certification or registration bodies.
ISO/IEC 27007	(under development) Standard will be a guideline for auditing ISMSs.
ISO/IEC TR 27008	(under development) Standard will provide guidance on auditing information security controls.
ISO/IEC 27009	(under development) Standard will provide guidance on information security governance.
ISO/IEC 27010	(under development) Standard will provide guidance on information security management for sector-to-sector communications.
ISO/IEC 27011	(under development) Standard (also known as X.1051) will provide information security management guidelines for telecommunications.
ISO/IEC 27012	(under development) Standard will provide information security management systems guidance for e-government applications
ISO/IEC 27013	(under development) Standard will provide information security management systems guidance for financial services organizations.
ISO/IEC 27031	(under development) Standard will be an information and communication technology (ICT)-focused standard on business continuity.
ISO/IEC 27032	(under development) Standard will provide guidelines for cybersecurity.
ISO/IEC 27033	(under development) Standard will replace the multi-part ISO/IEC 18028 standard on IT network security.
ISO/IEC 27034	(under development) Standard will provide guidelines for application security.
ISO/IEC 27035	(under development) Standard will replace ISO TR 18044 on security incident management.
ISO 27799	Recommendation that provides health sector specific ISMS implementation guidance.

Note: The titles, scope, and/or content of as-yet unpublished standards may change prior to their publication.



PLAN: Plan ahead for change. Analyze and predict the results.
DO: Execute the plan, taking small steps in controlled circumstances.
STUDY: CHECK, study the results.
ACT: Take action to standardize or improve the process.

FIGURE 3.2. The Deming (PDCA) cycle.

(PDCA) cycle.[18] ISO/IEC 27001 was being revised at press time; the revised standard is expected to be published by 2010. The ISMS is described in the standard using the PDCA process (see Figure 3.2), given that security controls have to be continually reviewed and adjusted to incorporate changes in the security threats, vulnerabilities and impacts of information security failures. In this case,

Plan = define requirements, assess risks, decide which controls are applicable;

Do = implement and operate the ISMS;

Check = monitor and review the ISMS;

Act = maintain and continuously improve the ISMS.

ISO/IEC 27001 is principally a *management system* standard, therefore, compliance requires the organization to have a defined set of management controls in place. Annex A of ISO/IEC 27001:2005 outlines 133 best practice security controls that should be considered by organizations to mitigate identified risks to their information assets. ISO/IEC 27002:2005 provides a more detailed description of each of the security controls along with implementation advice. ISO/IEC 27001:2005 does not mandate the implementation of specific information security controls. Organizations seeking compliance

[18] The Deming cycle, or PDCA cycle (also known as the Deming Wheel or the Continuous Improvement Spiral), is a continuous quality improvement model consisting of a logical sequence of four repetitive steps for continuous improvement and learning: "Plan, Do, Study (Check) and Act." The concept originated in the 1920s with Walter A. Shewhart, who introduced the "Plan, Do, and See" method. W. Edwards Deming, the Total Quality Management (TQM) practitioner, modified the Shewart cycle to become the PDSA. Deming was Japan as part of the occupation forces of the allies after World War II and taught Quality Improvement methods to the Japanese, including the use of statistics and the PDSA cycle.

and/or certification to ISO/IEC 27001:2005 are allowed to choose the information security controls from Annex A that are applicable to their environment along with other controls that are appropriate. ISO/IEC 27001:2005 is the formal standard against which organizations may seek certification of their ISMSs. ISO/IEC 27001:2005 describes the process for assessing risks and selecting, implementing and managing specific security controls. According to ISO/IEC, the standard allows the following:

- Use within organizations to formulate security requirements and objectives
- Use within organizations as a way to ensure that security risks are cost-effectively managed
- Use within organizations to ensure compliance with laws and regulations
- Use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met
- The definition of new information security management processes
- Identification and clarification of existing information security management processes
- Use by the management of organizations to determine the status of information security management activities
- Use by the internal and external auditors of organizations to demonstrate the information security policies, directives, and standards adopted by an organization and determine the degree of compliance with those policies, directives and standards
- Use by organizations to provide relevant information about information security policies, directives, standards, and procedures to trading partners and other organizations that they interact with for operational or commercial reasons
- Implementation of business enabling information security
- Use by organizations to provide relevant information about information security to customers

ISO/IEC 27001 has the following sections:

0. **Introduction.** Description of the process approach, which is based on the PDCA cycle.
1. **Scope.** Description of generic ISMS requirements suitable for various types of organizations.
2. **Normative References.** ISO/IEC 27002:2005 in particular.
3. **Terms and Definitions**
4. **Information Security Management System.** This section of the standard contains the “core” of the standard, based on the PDCA cycle. Also,

this section specifies documents that are required and must be controlled. The material explains that records must be generated and controlled to prove the operation of the ISMS (for example, certification audit purposes.)

5. **Management Responsibility.** This section of the standard advocates that management must demonstrate their commitment to the ISMS. Commitment is to be demonstrated by allocating adequate resources to implement and operate the ISMS.
6. **Internal ISMS Audits.** This section of the standard emphasizes the fact that the organization must conduct periodic internal audits to ensure that the ISMS incorporates adequate controls that operate effectively.
7. **Management Review of the ISMS.** This section of the standard makes the case that management must review the suitability, adequacy and effectiveness of the ISMS on a regular basis (for example, at least once a year), assessing opportunities for improvements.
8. **ISMS Improvements.** This section of the standard makes the case that the organization must continually improve the ISMS by assessing and implementing changes to ensure the ISMS' suitability and effectiveness, addressing nonconformance (noncompliance) and, where possible, preventing recurrent issues.

The appendices to the standard are as follows:

Annex A—Control Objectives and Controls. The annex contains a list of titles of the control sections in ISO/IEC 27002.

Annex B—OECD (Organization for Economic Co-operation and Development) Principles and the ISO/IEC 27002 International Standard. The annex contains a table showing which parts of the standard satisfy key principles laid out in the OECD Guidelines for the Security of Information Systems and Networks.

Annex C—Correspondence Between ISO 9001:2000, ISO 14001:2004 and the ISO/IEC 27002 International Standard. ISO/IEC 27001 shares the same basic structure of other management systems standards; as a consequence, an organization that implements any one of these management standards should already be familiar with concepts such as PDCA, records, and audits.

Certification against an accepted standard (e.g., ISO/IEC 27001:2005) is increasingly being demanded business partners, suppliers, and other entities that are concerned about information security. Independent assessment engenders rigor and formality to the implementation process; in turn, this typically implies improvements to information security and reduced risk. There are number of certification bodies worldwide that have been accredited by various national standards organizations that can perform certification audits in accordance with ISO/IEC 27001:2005 and issue certificates. The United Kingdom Accreditation Service or UKAS is the accreditation body in the United Kingdom and has accredited BSI along with about 18 other organizations as Certification Bodies (CBs). The ANSI-ASQ National Accreditation Board (ANAB) is the U.S. accreditation body for management system registrars or Certification Bodies.

The ANSI-ASQ National Accreditation Board and UKAS are members of the International Accreditation Forum (IAF) and are signatories of the IAF multilateral recognition arrangements. Through these arrangements, the ANSI-ASQ National Accreditation Board and UKAS cooperate with other accreditation bodies around the world to provide value to the organization it has accredited and their clients, ensuring that accredited certificates are recognized internationally. The global conformity assessment system ensures confidence and reduces risk for customers engaging in trade worldwide.

There are around 5000 ISO/IEC 27001:2005 certified organizations at press time. Considering an estimated 50 million corporations/institutions in the world, one can see that universal acceptance is far from complete. In addition, certifications are issued based on a specifically defined scope that may not cover the entire organization. One thing that certification to ISO/IEC 27001:2005 does ensure is that the organization has formally documented and implemented the mandatory management system elements of the standard as defined in clauses 4.0 through 8.0. In addition, organizations can seek certification based on a scope that they define, such as a portion of their critical business and not their entire organization.

3.3.3 ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management

ISO/IEC 27002:2005 is concerned with the security of information assets; in its view, this is well beyond just the IT systems. The standard takes the implicit view that the IT group is the custodian of a proportion of the organization's information assets and is charged with securing them; however, there is also a vast quantity of written information (embodying the knowledge and experience of employees) that resides outside IT.

ISO/IEC 27002 identifies a set of controls (133 to be exact, under 39 security objectives) to address information security risk exposures in the area of confidentiality, integrity, and availability. ISO/IEC 27002 is a code of practice, advisory document, not a formal specification: It provides a listing of best-practice information security control measures that organizations should consider to secure information assets. Information assets include (as covered in Chapters 1 and 2) IT equipment, networking equipment, storage equipment, data content, and so forth, at all layers of the architecture framework (for example, TOGAF) model. The control objectives listed in ISO/IEC 27002 can be interpreted as a generic functional specification for an organization's information security management controls architecture. ISO/IEC 27002 is widely used and is referenced by the ISMS certification standard ISO/IEC 27001. ISO/IEC JTC1/SC27 has started the process of revising ISO/IEC 27002, with possible re-publication in 2011.

As noted earlier, ISO/IEC 17799:2005 was renumbered ISO/IEC 27002:2005 in 2007 to bring it into the ISO/IEC 27000 family (the text remains word-for-word identical to ISO/IEC 17799:2005.)

Organizations that adopt ISO/IEC 27002 and seek to be certified compliant to ISO/IEC 27001 should assess their information security risks and apply appropriate controls, using the standard for guidance. As noted, ISO/IEC 27002 specifies 39 control objectives along with 133 security controls, but the standard does not make specific controls mandatory; the organization is free to select and implement controls that are appropriate to them and their environment. Some of the controls in the standard are not necessarily applicable in every instance; furthermore, the generic wording of the standard may not reflect an organization's exact requirements. Not making specific controls mandatory enables the standard to be broadly applicable and affords organizations implementation flexibility. There are no formal compliance certificates based on ISO/IEC 27002 itself (as stated above, organizations can get their information security governance/management processes—the information security management system—certified against ISO/IEC 27001).

The content of ISO/IEC 27002 is covered next.

0. **Introduction.** Describes how to make use of the standard.
1. **Scope.** Describes the scope that encompasses information security management recommendations for individuals responsible for initiating, implementing, or maintaining security.
2. **Terms and Definitions**
3. **Structure of this Standard.** This section of the standard explains that the crux of the standard consists of control objectives, suggested controls, and implementation guidance.
4. **Risk Assessment and Treatment.** This section of the standard provides a short discussion of risk management (a reference to ISO/IEC 27005 may be added in the 2011 revision, which provides guidance on selecting and using appropriate methods to analyze information security risk).

The following sections align with the security controls defined in Annex A of ISO/IEC 27001:2005:

5. **Security Policy.** This section of the standard contains one security objective and two security controls and advocates that (appropriate) management within organizations needs to define a policy to document their direction of, and support for, information security. There should be a high-level information security policy statement defining the key information security directives and mandates for the organization. The guiding policy naturally

needs to be supported by a comprehensive apparatus of specific corporate information security policies (an information security policy manual often describes the policies.) The apparatus of specific corporate information security policies is supported, in turn, by a set of institutional information security standards, procedures and guidelines.

Note: The ISMS policy required by ISO/IEC 27001:2005 is considered a superset of the information security policy described above.

6. **Organization of Information Security.** This section of the standard contains two security objectives and eleven security controls and makes the case that appropriate information security governance structure should be designed and implemented. Security considerations need to cover the internal organization and external parties. The (internal) organization is best served by a management framework for information security where senior management provides direction and commits support. Clearly, roles and responsibilities need to be defined for the information security function. Other guidance in this section includes, but is not limited to the following: Confidentiality agreements should reflect the organization's needs; contacts should be established with relevant authorities (e.g., law enforcement) and appropriate special interest groups; and, information security should be independently reviewed. In reference to external parties, it is axiomatic that information security should not be compromised by the introduction of third party products or services, and risk exposures should be assessed and mitigated when dealing with customers and other third parties.
7. **Asset Management.** This section of the standard contains two security objectives and five security controls and makes (the obvious) case that organizations need to be in a position to understand what information assets they hold, and to manage their security appropriately. All IT assets should be accounted for and have a defined owner. A comprehensive inventory of information assets should be maintained; as noted, IT assets include but are not limited to IT hardware, software, data, system documentation, storage media, supporting assets such as computer room air conditioners and UPSs, and ICT services. The inventory should record ownership and location of the assets, and owners should identify acceptable uses. The section of the standard also recommends that information assets (data) should be classified according to its need for security protection and labeled in such a manner.
8. **Human Resources Security.** This section of the standard contains three security objectives and nine security controls and punctuates that the organization should manage system access rights and IT assets for "joiners, movers, and leavers" and should undertake suitable security awareness, training, and educational activities. Section 8.1 of the standard focuses on "Prior to Employment" and notes that security responsibilities need to be taken into account when recruiting permanent employees,

contractors, and temporary staff (for example, by utilizing adequate job descriptions, preemployment screening, etc.) and included in contracts (for example, terms and conditions of employment and other signed agreements on security roles and responsibilities). Section 8.2 focuses on "During Employment" and calls attention to management responsibilities regarding information security. Specifically, employees and third-party IT users need to be educated and trained in security procedures. A formal disciplinary process is needs to be in place to handle security breaches. Section 8.3 focuses on "Termination or Change of Employment" and discusses security aspects of an employee's exit from the organization (including the return of corporate assets and removal of access rights). Applicable procedures also need to be codified for change of responsibilities within an organization—for example, a lateral move to a different group within the organization which has different (data access) privileges/responsibilities.

9. **Physical and Environmental Security.** This section of the standard contains two security objectives and 13 security controls and discusses how hardware assets should be physically protected against malicious or accidental damage or loss and also should be protected from overheating, radio-frequency interference, loss of electrical power, and so on. The need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access is discussed. IT equipment, communications equipment, and on-site/on-campus cabling should be protected against physical damage, fire, flood, damaging storms, sabotage, and other risk exposures.
10. **Communications and Operations Management.** This section of the standard contains 10 security objectives and 32 security controls that describe the security controls for systems and network management; it covers issues listed in Table 3.3.
11. **Access Control.** This section of the standard contains seven security objectives and 25 security controls and discusses logical access to IT systems, networks, and data and reinforces clearly that access must be suitably controlled to prevent unauthorized use. A number of issues are addressed in the section: (i) Business requirement for access control (requirements to control access to information assets should be clearly documented in an access control policy); (ii) user access management (allocation of access rights should be formally controlled through (a) user registration and administration procedures including special restrictions over the allocation of privileges and management of passwords and (b) periodic access rights reviews; (iii) user responsibilities (maintaining effective access controls such as choosing strong passwords and keeping them confidential); (iv) network access control (access to network services should be controlled and policy should be defined and remote users must be authenticated—also remote diagnostic ports should be securely controlled); (v) operating system access control (advocates use of operating

TABLE 3.3. Communications and Operations Management, ISO 27002

Topic	Description/Recommendation
Operational procedures and responsibilities	This subsection of the standard makes the case that IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people where relevant (for example, access to development and operational systems should be segregated).
Third-party service delivery management	This subsection of the standard makes the case that security requirements should be taken into account in third-party service delivery (for example, IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management.
System planning and acceptance	This subsection of the standard covers IT capacity planning and production acceptance processes.
Protection against malicious and mobile code	This subsection of the standard describes the need for anti-malware controls, including user awareness. Security controls for mobile code associated with a number of middleware services are also covered. Mobile code is code that can be transmitted across the network and executed on the far end; Java is one example of a language that supports such mode of operation.
Backup	This subsection of the standard covers routine data backups and rehearsed restoration.
Network security management	This subsection of the standard covers secure network management, network security monitoring and other controls. Additionally, it covers security of commercial network services such as private networks and managed firewalls and so on.
Media handling	This subsection of the standard makes the case that operating procedures should be defined to protect documents and computer media containing data, system information, and so on. Procedures should be defined for securely handling, transporting and storing backup media and system documentation. Also disposal of backup media, documents, and so on should be logged and controlled.
Exchange of information	This subsection of the standard makes the case that information exchanges between organizations should be controlled by using appropriate policies and procedures, and legal agreements. Security procedures and standards need to be in place to protect information and physical media in transit, including electronic messaging (for example, e-mail, EDI, and IM) and business information systems. Information exchanges must also comply with applicable legislation.
Electronic commerce services	This subsection of the standard makes the case that the security implications of e-commerce (online transaction systems)

(*Continued*)

TABLE 3.3. (Continued)

Topic	Description/Recommendation
	should be evaluated and suitable controls implemented. The integrity and availability of information published online (for example, on websites) should also be protected.
Monitoring	This subsection of the standard covers security event/audit/fault logging and system alarm/alert monitoring to detect unauthorized use. It also discusses the need to secure systems/network element logs.

system access control facilities and utilities, such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms); (vi) application and information access control (access to and within application systems should be controlled in accordance with a defined access control policy); and (vii) mobile computing and teleworking (formal policies covering the secure use of laptops, PDAs, cellphones, etc., and secure teleworking must be defined.)

12. **Information Systems Acquisition, Development, and Maintenance.** This section of the standard contains six security objectives and 16 security controls and emphasizes that information security must be taken into account during the process of specifying, building/acquiring, testing, implementing, and maintaining IT systems. Some of the issues discussed include: (i) security requirements of IT systems (automated and manual security control requirements must be identified during the requirements stage of the systems development or procurement process, and incorporated into business cases); (ii) correct processing in application systems (data entry, processing and dissemination validation controls and message authentication must be provided); (iii) cryptographic controls (policies should be defined, covering digital signatures, nonrepudiation, management of keys, and digital certificates); (iv) security of system files (access to system files—executable programs and source code—must be controlled; (v) security in development and support processes (application system managers must assume the responsibility for controlling access to the project environment and support environments—for example, formal change control processes should be applied, including technical reviews; checks should be made for information leakage via covert channels and Trojans); and (vi) technical vulnerability management (systems/applications vulnerabilities must be controlled by monitoring for the release of security alerts by observers including the vendor of the system/application, risk-assessing the situation, and then promptly applying relevant security patches.)
13. **Information Security Incident Management.** This section of the standard contains two security objectives and five security controls and highlights that information security events, incidents and weaknesses should be

promptly reported and properly managed by organizations. An incident reporting/alarm procedure must be put in place, along with the associated response and escalation procedures. Definition of responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence. Every employees, contractors, and business partner should be informed of their incident reporting responsibilities.

14. **Business Continuity Management.** This section of the standard contains one security objective and five security controls and describes the relationship between IT disaster recovery planning, business continuity management and contingency planning. At one end of the spectrum is the requisite analysis and creation of relevant documentation; at the other end of the spectrum is a process for periodic testing of the plans.
15. **Compliance.** This section of the standard contains two security objectives and ten security controls and addresses some of the compliance issues, including (i) compliance with legal requirements (for example applicable legislation such as copyright, data protection, protection of financial data); (ii) compliance with security policies and standards, and technical compliance (designated managers in the organization, along with system owners, must ensure compliance with security policies and standards); and (iii) Information systems audit considerations (even audit tools/facilities must also be protected against unauthorized use).

Note: There are a number of "27001 Toolkits" on the market that provide a collection of ISMS implementation guidelines and sample documents that may help during the implementation process.

3.3.4 ISO/IEC 27003 Information Technology—Security Techniques—Information Security Management System Implementation Guidance (Draft)

ISO/IEC 27003 (at Final Committee Draft stage at press time) seeks to provide implementation guidance for organizations implementing the ISO/IEC 27001 standard. Publication was expected in 2010. According to the ISO committee developing the standard, the scope of ISO/IEC 27003 is to provide practical guidance for establishing and implementing an information security management system in accordance with ISO/IEC 27001. It describes the implementation of an ISMS focusing on the part from the first approval for the ISMS implementation in an organization to the beginning of the ISMS operations that correspond to the plan and do phases of an ISMS PDCA cycle. The standard includes the explanations of the design activities related to operating, monitoring, reviewing, and improving an ISMS. The key sections of the Committee Draft are shown in Table 3.4.

TABLE 3.4. Key Sections of ISO/IEC 27003

Section	Subsection
Obtain management approval for implementation of ISMS	Overview on management approval for implementation
	Define objectives, information security needs, business requirements for ISMS
	Define initial ISMS scope
	Create the business case & project setup
	Obtain management approval and commitment to Implement an ISMS
Defining ISMS scope and ISMS policy	Overview on defining ISMS scope and ISMS policy
	Define organizational boundaries
	Define information communication technology boundaries
	Define physical boundaries
	Complete boundaries for ISMS scope
	Develop the ISMS policy
Conducting business analysis	Overview on conducting a business analysis
	Defining information security requirements supporting the ISMS
	Creating information assets inventory
	Generating an information security assessment
Conducting risk assessment	Overview on conducting a risk assessment
	Risk assessment description
	Conduct risk assessment
	Plan risk treatment and select controls
Designing the ISMS	Overview on designing an ISMS
	Designing organizational security
	Designing ICT and physical security
	Designing the Monitoring and Measuring
	Requirements for ISMS recording
	Produce the ISMS Implementation Plan
Implementing the ISMS	Overview on ISMS Implementation
	Carry out ISMS Implementation Projects
	Implementation of monitoring
	ISMS Procedures and Control Documentation
	ISMS Measurement Procedure Documentation

3.3.5 ISO/IEC 27004 Information Technology—Security Techniques—Information Security Management—Measurement (Second Final Committee Draft)

ISO/IEC 27004 aims at covering information security management measurements. Work on the standard started in the middle of the decade, and publication was expected by early 2010. The standard provides input on how organizations can measure and report the effectiveness of their ISMSs. It covers both the security management processes defined in ISO/IEC 27001 and the security controls defined in ISO/IEC 27002.

According to the ISO committee developing the standard, it provides guidance and advice on the development and use of measures and measurement in order to assess the effectiveness of an ISMS, including the ISMS policy and objectives and security controls as specified in ISO/IEC 27001. ISO/IEC 27004 also aims at providing guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. The standard is intended to be applicable to a wide range of organizations with a correspondingly wide range of information security management systems. It can be used to create a base for each organization to collect, analyze, and communicate data related to ISMS processes.

3.3.6 ISO/IEC 27005:2008 Information Technology—Security Techniques—Information Security Risk Management

ISO/IEC 27005:2008 provides guidelines for information security risk management. It supports the concepts specified in ISO/IEC 27001 and is designed to assist the implementation of information security based on a risk management approach. ISO/IEC 27005 offers general advice on choosing and using risk analysis or assessment methods without specifying any specific risk analysis method.

3.4 ISO/IEC 31000

There are a number of risk-related standards published by ISO and other standards bodies, as well as other standards that refer to risk management, as noted above, but until recently there was no central ISO document that provides a consistent approach to risk management. In 2005, ISO initiated a New Work Item Proposal (NWIP) to look at developing a guidance standard on risk management. Work started on the standard in 2006, and the document had progressed to a Draft International Standard by press time [NSA200701]. ISO 31000 Draft International Standard (DIS), "Risk management—Guidelines on principles and implementation of risk management," is intended to become the first international standard on risk management, upon approval. ISO 31000 provides generic guidelines for the principles involved in effective implementation of risk management. The standard also harmonizes risk management processes and definitions in existing and future standards. The standard can be applied to a wide range of activities, decisions, and operations of any public, private, or community enterprise, association, group, or individual. ISO 31000 provides guidelines on the principles and implementation of risk management in general (not IT or information security specific), namely it provides a general framework for managing risk exposures. It is not intended to be used for the purposes of certification.

In conjunction with developing ISO 31000, the ISO Risk Management Working Group is also looking at updating ISO/IEC Guide 73, "Risk Management—Vocabulary." This guide provides a basic vocabulary of the definitions of risk management generic terms. The guide aims to encourage a mutual and consistent understanding and a coherent approach to the description of activities relating to the management of risk [NSA200701]. The release of ISO/IEC Guide 73 CD2, which is a revision of the existing Guide 73 and provides a risk management vocabulary, is also expected in 2009 (ISO 31000 DIS refers to the definitions in Guide 73.)

ISO 31000 observes that to be most effective, an organization's risk management should adhere to the principles such as these [ISO31000]:

(a) Risk management should create value. Risk management should contribute to the demonstrable achievement of objectives and improvement of, for example, efficiency in operations, environmental protection, financial performance, corporate governance, human health and safety, product quality, legal and regulatory compliance, public acceptance, and reputation.

(b) Risk management should be an integral part of organizational processes. Risk management should be part of the responsibilities of management and an integral part of the normal organizational processes as well as of all project and change management processes. Risk management should not be a standalone activity or be separate from the main activities and processes of the organization.

(c) Risk management should be part of decision-making. Risk management can help prioritize actions and distinguish among alternative courses of action. Risk management helps decision makers make informed choices. Ultimately, risk management can help with decisions on whether a risk is unacceptable and whether risk controls will be adequate and effective.

(d) Risk management should explicitly address uncertainty. Risk management deals with those aspects of decision making that are uncertain, the nature of that uncertainty, and how it may be treated.

(e) Risk management should be systematic and structured. Risk management approaches should ensure where practicable that the results are consistent, comparable and reliable.

(f) Risk management should be based on the best available information. The inputs to the process of managing risk should be based on information sources such as experience, feedback, observation, forecasts, and expert judgment. However, decision makers should be informed of and may need to take into account any limitations of the data or modeling used or the possibility of divergence among experts.

(g) Risk management should be tailored. Risk management should be aligned with the organization's external and internal context and risk profile.

(h) Risk management should take into account human factors. The organization's risk management should recognize the capabilities, perceptions, and intentions of external and internal people that may facilitate or hinder attainment of the organization's objectives.

(i) Risk management should be transparent and inclusive. Appropriate and timely involvement and inclusion of stakeholders and, in particular, decision makers at all levels of the organization should ensure that risk management remains relevant and up to date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria, stakeholders' perceptions and levels of tolerable risk.

(j) Risk management should be dynamic, iterative, and responsive to change. As internal and external events occur, context and knowledge change, monitoring and review take place, new risks emerge, and others decrease. An organization should ensure that risk management continually senses and responds to change.

(k) Risk management should be capable of continual improvement and enhancement. Organizations should develop strategies to improve their risk management maturity alongside all other aspects of their organization.

Publication of the ISO 31000 Standard was underway at press time; by 2009 it had reached Final Draft International Standard (FDIS) status. AS/NZS 4360:2004 (see below) has been used as a point-of-departure in the formation of the ISO document. Figure 1.4 depicted the ISO 31000 process.

3.5 NIST STANDARDS

Table 3.5 identifies some of the applicable NIST standards; this is a comprehensive set of standards. In particular, NIST SP 800-16, NIST SP 800-24, NIST SP 800-30, and NIST SP 800-39 cover risk management. Subjects covered in the NIST standards include the following:

- Managing risk
  - Threats
  - Vulnerabilities
  - Risk
  - Relationships between threats, vulnerabilities, risks
- Threats from "authorized system users"
- Increased threats and vulnerabilities from connection to external systems and networks
  - "Hacker" threats
  - Malicious software programs and virus threats

TABLE 3.5. NIST Computer Security Standards (Partial List)

NIST	**SP (Special Publication) 800-12** An Introduction to Computer Security: The NIST Handbook
	SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model
	SP 800-18 Guide for Developing Security Plans for Information Technology Systems
	SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
	SP 800-24 PBX Vulnerability Assessment - Finding Holes in Your PBX Before Someone Else Does
	SP 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
	SP 800-26 Security Self-Assessment Guide for Information Technology Systems
	SP 800-30 Risk Management Guide for Information Technology Systems
	SP 800-31 Intrusion Detection Systems (IDS)
	SP 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure
	SP 800-33 Underlying Technical Models for Information Technology Security
	SP 800-34 Contingency Planning Guide for Information Technology Systems
	SP 800-36 Guide to Selecting Information Technology Security Products
	SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
	SP 800-39 Managing Risk from Information Systems—An Organizational Perspective” (draft published April 2008)
	SP 800-41 Guidelines on Firewalls and Firewall Policy
	SP 800-42 Guideline on Network Security Testing
	SP 800-43 Systems Administration Guidance for Windows 2000 Professional
	SP 800-44 Guidelines on Securing Public Web Servers
	DRAFT SP 800-53 Recommended Security Controls for Federal Information Systems
	SP 800-55 Security Metrics Guide for Information Technology Systems
	SP 800-61 Computer Security Incident Handling Guide
	SP 800-64 Security Considerations in the Information System Development Life Cycle
	SP 800-68 Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist

- Types of security controls (safeguards, countermeasures)
  - Management controls
  - Acquisition/development/installation/implementation controls
  - Operational controls

  - Security awareness and training controls
  - Technical controls
- How different categories of controls work together
- Examples of security controls for:
  - Confidentiality protection
  - Availability protection
  - Integrity protection
- Added security controls for connecting external systems and networks
- Protecting assets through IT security awareness and training programs
- Contingency-disaster recovery planning
  - Importance of plan to deal with unexpected problems
  - Importance of testing plan and applying lessons learned
- "Acceptable levels of risk" versus "absolute protection from risk"
- "Adequate" and "appropriate" controls
  - Unique protection requirements of IT systems and information
  - Severity, probability, and extent of potential harm
  - Cost effective/cost benefits
  - Reduction of risk versus elimination of risk
- Working together with other security disciplines
- Importance of internal and external audits, reviews, and evaluations in security decisions

Note: The material that follows in this subsection is based directly on NIST documentation.

3.5.1 NIST SP 800-16

NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," covers (among other topics) controls. Specifically, it covers Management Controls; Acquisition/Development/Installation/Implementation Controls; Operational Controls; and Technical Controls. Management Controls highlighted in NIST SP 800-16 include the following:

1. System/application-specific policies and procedures
2. Standard operating procedures
3. Personnel security
   a. Background investigations/security clearances
   b. Roles and responsibilities
   c. Separation of duties
   d. Role-based access controls

4. System rules of behavior contribute to an effective security environment
    a. Organization-specific user rules
    b. System-specific user rules
        i. Assignment and limitation of system privileges
        ii. Intellectual property/copyright issues
        iii. Remote access and work at home issues
        iv. Official versus unofficial system use
        v. Individual accountability
        vi. Sanctions or penalties for violations
5. Individual accountability contributes to system and information quality
    a. Individual acceptance of responsibilities
    b. Signed individual accountability agreements
6. IT security awareness and training
    a. Determining IT security training requirements for individuals
    b. Effect of IT security awareness and training programs on personal responsibility and positive behavioral changes
    c. "Computer ethics"
    d. System-specific user IT security training
7. User responsibilities for inappropriate actions of others

Acquisition/Development/Installation/Implementation Controls highlighted in NIST SP 800-16 include the following:

1. System life-cycle stages and functions
2. IT security requirements in system life-cycle stages
    a. Initiation stage
    b. Development stage
    c. Test and evaluation stage
    d. Implementation stage
    e. Operations stage
    f. Termination stage
3. Formal system security plan for management of a system
    a. Identification of system mission, purpose, and assets
    b. Definition of system protection needs
    c. Identification of responsible people
    d. Identification of system security controls in-place or planned and milestone dates for implementation of planned controls
4. Relationship of configuration and change management programs to IT security goals
5. Testing system security controls synergistically and certification
6. Senior manager approval (accredit) an IT system for operation

Operational Controls highlighted in NIST SP 800-16 include the following:

1. Physical and environmental protection
   a. Physical access controls
   b. Intrusion detection
   c. Fire/water/moisture/heat/electrical maintenance
   d. Mobile and portable systems
2. Marking, handling, shipping, storing, cleaning, and clearing
3. Contingency planning
   a. Importance of developing and testing contingency/disaster recovery plans
   b. Importance of users providing accurate information about processing needs, allowable downtime and applications that can wait
   c. Responsibility for backup copies of data files and software programs
   d. Simple user contingency planning steps

Technical Controls highlighted in NIST SP 800-16 include the following:

1. How technical (role-based access) controls support management (security rules) controls
   a. User identification and passwords/tokens
   b. User role-based access privileges
   c. Public access controls
2. How system controls can allow positive association of actions to individuals
   a. Audit trails
   b. System monitoring
3. Recognizing attacks by hackers, authorized or unauthorized users
   a. Effects of hacker attack on authorized users
   b. Unauthorized use or actions by authorized users
   c. Reporting incidents
4. User actions to prevent damage from malicious software or computer virus attacks
   a. Organization-specific procedures for reporting virus incidents
   b. Technical support and help from security incident response teams
   c. Software products to scan, detect, and remove computer viruses
5. Role of cryptography in protecting information

The standard also identifies some typical (but not necessarily all-inclusive) responsibilities of risk management personnel, based on practitioner's tier (junior, intermediate, and senior staff), as follows:

Junior Staff. Expected to

- Understand categories of risk and participate in the design and development of operational IT security program procedures
- Apply organization-specific IT security program elements to the implementation of the program and identify areas of weakness
- Participate in the review of an organization's IT security program and evaluate the extent to which the program is being managed effectively
- Identify general and system-specific IT security specifications that pertain to a particular system acquisition being planned.

Intermediate Staff. Expected to

- Establish acceptable levels of risk and translate the IT security program elements into operational procedures for providing adequate and appropriate protection of the organization's IT resources
- Analyze patterns of noncompliance and take appropriate administrative or programmatic actions to minimize security risks
- Develop compliance findings and recommendations, as well as security-related portions of acquisition documents

Advanced Staff. Expected to

- Design, develop, and direct the activities necessary to marshal the organizational structures, processes, and people for an effective IT security program implementation
- Direct the implementation of appropriate operational structures and processes to ensure an effective IT security program
- Direct the review of the management of an organization's IT security program, validate findings and recommendations, and establish follow-up monitoring for corrective actions
- Ensure that security-related portions of the system acquisition documents meet all identified security needs

3.5.2 NIST SP 800-30

NIST SP 800-30, ''Risk Management Guide for Information Technology Systems,'' provides an overview of risk management, how it fits into the system development life cycle (SDLC), and the roles of individuals who support and use this process. It also describes the risk assessment methodology and nine primary steps in conducting a risk assessment of an IT system. The document also describes the risk mitigation process, including risk mitigation options and strategy, approach for control implementation, control categories, cost–benefit analysis, and residual risk. Finally, the document also discusses the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program. NIST SP 800-30 is targeted to

- Senior management, the mission owners, who make decisions about the IT security budget
- (Federal) chief information officers, who ensure the implementation of risk management for (agency) IT systems and the security provided for these IT systems
- The Designated Approving Authority (DAA), who is responsible for the final decision on whether to allow operation of an IT system
- The IT security program manager, who implements the security program
- Information system security officers (ISSO), who are responsible for IT security
- IT system owners of system software and/or hardware used to support IT functions
- Information owners of data stored, processed, and transmitted by the IT systems
- Business or functional managers, who are responsible for the IT procurement process
- Technical support personnel (e.g., network, system, application, and database administrators; computer specialists; data security analysts), who manage and administer security for the IT systems
- IT system and application programmers, who develop and maintain code that could affect system and data integrity
- IT quality assurance personnel, who test and ensure the integrity of the IT systems and data
- Information system auditors, who audit IT systems
- IT consultants, who support clients in risk management

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

As we have noted in Chapter 2, risk is a function of (a) the likelihood that a given threat source will exercise a particular potential vulnerability and (b) the resulting impact of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described in detail in the document:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation.

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 1.2 in Chapter 1 depicts these steps and the inputs to and outputs from each step.

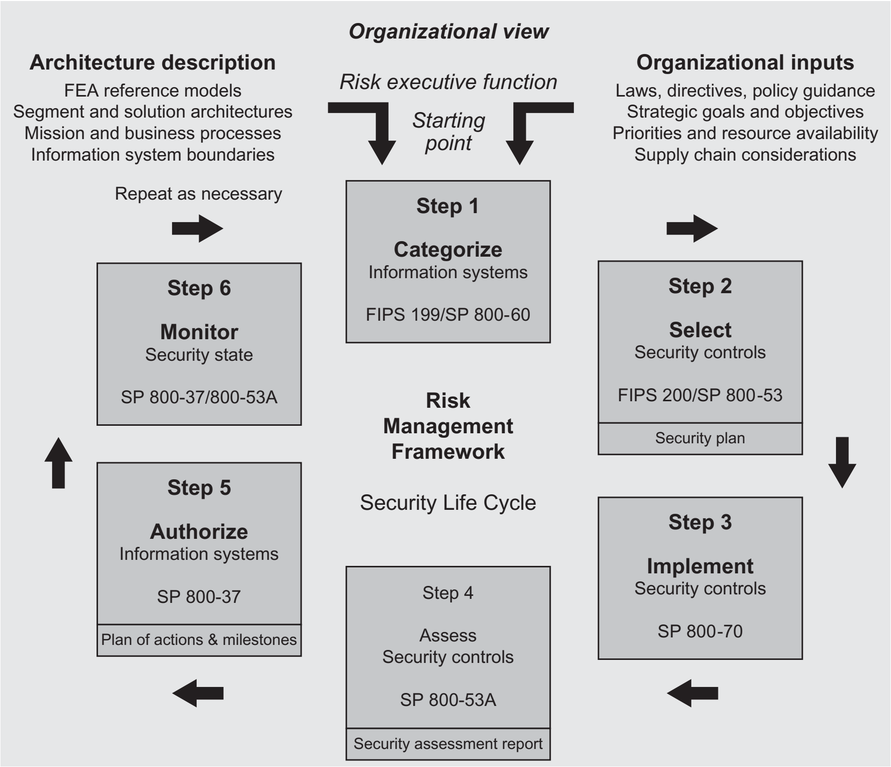
3.5.3 NIST SP 800-39

NIST SP 800-39, "Managing Risk from Information Systems—An Organizational Perspective" (draft published April 2008), describes a *Risk Management Framework (RMF)*. RMF provides organizations with a structured, yet flexible, process for managing risk related to the operation and use of information systems. The RMF can be used by organizations to determine the appropriate risk mitigation needed to protect the information systems and infrastructure supporting organizational mission/business processes. Figure 3.3 provides a graphical overview of the RMF along with the organization-wide inputs necessary for organizations to effectively apply the framework to the information systems supporting the organization's missions and business processes. There is a good degree of similarity between the NIST SP 800-39 approach and ISO/IEC 27001.

The RMF process includes (i) categorizing information and information systems with regard to mission and business impacts (FIPS 199 and Special Publication 800-60), (ii) selecting and documenting security controls needed for risk mitigation (FIPS 200 and Special Publication 800-53), (iii) implementing security controls in organizational information systems and supporting infrastructure (Special Publication 800-70), (iv) assessing security controls to determine effectiveness (Special Publication 800-53A), (v) authorizing information systems and supporting infrastructure and explicitly accepting mission/business risk (Special Publication 800-37), and (vi) monitoring of the security state of information systems and operational environments (Special Publications 800-53A and 800-37).

Stakeholders, as defined in NIST SP 800-39, include the following:

- Individuals with mission/business/information ownership responsibilities (e.g., agency heads, authorizing officials, information owners)



- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems;*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems;*
- NIST Special Publication 800-30, *Revision 1, Guide for Conducting Risk Assessments;*
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems;*
- NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems;*
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System;*
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories;*
- NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers;*
- NIST Special Publication 800-100, I*nformation Security Handbook, A Guide for Managers.*

FIGURE 3.3. NIST SP 800-39 Risk Management Framework (RMF).

- Individuals with information system/security management responsibilities (e.g., chief information officers, senior agency information security officers, security managers)
- Individuals with information system design and development responsibilities (e.g., program managers, enterprise architects, information technology product vendors, system integrators)
- Individuals with information system/security implementation and operational responsibilities (e.g., information system owners, system security officers)
- Individuals with information system/security assessment and monitoring responsibilities (e.g., auditors, assessors, Inspectors General, evaluators, validators, and certification agents)

Note: Authorizing officials are officials within an organization that have the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Authorizing officials are accountable for their authorization decisions.

NIST SP 800-39 makes the case that to help protect organizations from the adverse effects of ongoing, serious, and increasingly sophisticated *threats* to information systems, organizations should employ a risk-based protection strategy. Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate, and explicitly accepting the residual risks associated with the operation and use of information systems. Risk-based protection strategies require authorizing officials to

- Determine, with input from the risk executive function and senior agency information security officer, the appropriate balance between the risks from and the benefits of using information systems to carry out organizational mission/business processes
- Approve the selection of security controls for information systems and the supporting infrastructure necessary to achieve this balance
- Take responsibility for the information security solutions agreed upon and implemented within the information systems supporting the organization's mission/business processes
- Acknowledge, understand, and explicitly accept the risks to organizational operations and assets, individuals, other organizations, and the Nation that result from the operation and use of information systems
- Be accountable for the results of information security-related decisions
- Monitor the continued acceptability of organizational risk from information systems over time

Risk-based protection strategies, as described in NIST SP 800-39, focus on managing risks from information systems based on real-world conditions and making the management decisions explicit—an essential requirement for establishing and maintaining trust among organizations. A primary consideration of any risk-based protection strategy is to effectively integrate risks from the operation and use of information systems into existing organizational processes dealing with other types of organizational risks (e.g., program and investment risks). This integrated approach moves the management of information system-related risks from an isolated process to an integral part of an overall process for managing the totality of risks organization-wide. Risk-based protection strategies are necessary to help ensure that organizations are adequately protected against the growing sophistication of threats to information systems. The serious nature of the threats, along with the dynamic environment in which modern organizations operate, demand flexible, scalable, and mobile defenses that can be tailored to rapidly changing conditions including the emergence of new threats, vulnerabilities, and technologies. Risk-based protection strategies support the overall goals and objectives of organizations, can be tightly coupled to enterprise architectures, and can operate effectively within system development life cycles. By empowering senior leaders to make explicit risk management decisions, these strategies also provide the flexibility necessary for the selection and employment of appropriate security controls for organizational information systems to achieve common-sense, cost-effective information security solutions.

NIST SP 800-39 notes that organizations are becoming increasingly reliant on information system services and information provided by external providers as well as partnerships established to carry out important mission and business processes. The need for *trust relationships* among organizations arises both from the partnerships established to share information and conduct business and from an organization's use of external providers of information and information system services. In many cases, while external providers bring greater productivity and cost efficiencies to the organization, they may also bring greater risk. This risk must be appropriately managed given the mission and business goals and objectives. Relationships among cooperating organizations are established and maintained in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency and intra-agency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges (i.e., supply chain collaborations or partnerships). The growing dependence on external service providers and partnerships with domestic and international public and private sector participants presents new challenges for organizations, especially in the area of information security. These challenges include

- Defining the types of services/information to be provided to the organization or the types of information to be shared/exchanged in partnering arrangements

- Describing how the services/information are to be protected in accordance with the security requirements of the organization
- Obtaining the relevant information from external providers and from business partners needed to support and maintain trust (including visibility into risk decisions to understand the participating/cooperating organization's risk management strategies and risk tolerance)
- Determining if the risk to organizational operations and assets, individuals, other organizations, or the nation resulting from the use of the services or information or the participation in the partnership is at an acceptable level

NIST SP 800-39 also notes that organizations need to manage risk exposures from supply chains. A supply chain is a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Domestic and international supply chains are becoming increasingly important to the national and economic security interests of the United States because of the growing dependence on products and services produced or maintained in worldwide markets. Uncertainty in the supply chain and the growing sophistication and diversity of international cyber threats increase the potential for a range of adverse effects on organizational operations and assets, individuals, other organizations, and the nation. Global commercial supply chains provide adversaries with opportunities to manipulate information technology products that are routinely used by public and private sector organizations (e.g., federal agencies, contractors) in the information systems that support U.S. critical infrastructure applications. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those information systems. These risk exposures include

- The introduction of exploitable vulnerabilities into information systems when products containing malicious code and other malware are integrated into the systems
- Inability/difficulty in determining the trustworthiness of information systems that depend upon commercial information technology products to provide many of the security controls necessary to ensure adequate security
- Inability/difficulty in determining the trustworthiness of information systems service providers (e.g., installation, operations, and maintenance) that provide many of the security controls necessary to ensure adequate security

3.6 AS/NZS 4360

AS/NZS 4360:2004 is a risk management standard published jointly by Australia Standards and New Zealand Standards; the companion document

HB 436:2004, Risk Management Guidelines, expands on AS/NZS 4360 and is also a relevant reference. AS/NZS 4360 (originally published as AS/NZS 4360:1995, with second edition 1999 and third edition 2004) describes an approach to risk management process, but it is not a goal of the standard to create uniformity in risk management systems; the design and specific implementation of the risk management system is influenced by the detailed needs of an organization, its objectives, products and services. The standard provides a generic guide for establishing and implementing the risk management process involving identification, analysis, assessment, treatment, and continuous risk monitoring. The standard has broad applicability including commercial organizations, enterprises, and government entities.

In AS/NZS 4360:2004, ‘‘risk’’ is defined as ‘‘the chance of something happening that will have an impact on objectives’’ (recall that in this text, this chance is known as the probability of the risk exposure event.) Risk is ‘‘measured in terms of a combination of the consequences of an event and their likelihood’’ (in this text, risk is the measure of the expected loss). ‘‘Risk management’’ is defined as ‘‘the culture, processes, and structures that are directed toward realizing potential opportunities whilst managing adverse effects.’’ ‘‘Risk sharing’’ is defined as ‘‘sharing with another party the burden of loss, or benefit of gain from a particular risk.’’ ‘‘Stakeholders’’ are persons and organizations ‘‘who may affect, be affected by, or *perceive* themselves to be affected by a decision, activity or risk’’ [STA200401]. Controls aim at minimizing negative risk *and* enhancing positive opportunities.

The AS/NZS 4360 process has a first step that calls for the need to ‘‘communicate and consult.’’ It proposes a ‘‘dialogue with stakeholders . . . focused on consultation rather than a one-way flow of information from the decision maker to other stakeholders.’’ The standard acknowledges that stakeholder perceptions are as important as the estimates of experts and insiders. Other steps (seven in all) include ‘‘establish the context, identify risks, analyze risks, evaluate risks, treat risks, and monitor and review’’ [KLO200401]. Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance.

Figure 1.5 in Chapter 1 depicted pictorially the risk management steps embodied in the standard.

REFERENCES

[COL200701] L. Coles-Kemp, R. E. Overill, ‘‘On the role of the facilitator in information security, risk assessment,’’ Journal of Computer Virology (2007) 3:143–148, DOI 10.1007/s11416–007–0040–6, *EICAR 2007 Best Academic Papers*, Springer-Verlag, France, 2007.

[IMP200801] ISO27k Implementers Forum (http://www.iso27001security.com), 2008.

[KLO200401] H. F. Kloman, *Risk Management Reports*, November 2004, Volume 31, No. 11.

[NIS199801] NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler, and J. B. Ippolito, editors, NIST, April 1998.

[NSA200701] L. Hendy, ISO 31000 Risk Management Guidance Standard, NSAI, 1 Swift Square, Northwood, Santry Dublin 9, Ireland, July 2007.

[STA200401] Standards Australia, GPO Box 5420, Sydney, NSW 2001, Australia. Also, Standards New Zealand, Private Bag 2439, Wellington 6020, New Zealand. www.standards.com.au.

APPENDIX 3A: ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD) GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARD A CULTURE OF SECURITY

This appendix includes the OECD guidelines referenced in the ISO27k standards. The appendix is based directly on OECD documentation.

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organization for Economic Cooperation and Development (OECD) shall promote policies designed to

- Achieve the highest sustainable economic growth and employment and a rising standard of living in member countries, while maintaining financial stability, and thus to contribute to the development of the world economy
- Contribute to sound economic expansion in member as well as nonmember countries in the process of economic development
- Contribute to the expansion of world trade on a multilateral, nondiscriminatory basis in accordance with international obligations

The original member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. The following countries became Members subsequently through accession at the dates indicated: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996), and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer, and Communications Policy (ICCP), and accelerated in the aftermath of the September 11, 2001 tragedy. Drafting was undertaken by an Expert Group of the WPISP which met in Washington, DC, on 10–11 December 2001, Sydney on 12–13 February 2002, and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5–6 March 2002, 22–23 April 2002 and 25–26 June 2002. The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

1. **Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.** Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.
2. **Responsibility: All participants are responsible for the security of information systems and networks.** Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design, and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.
3. **Response: Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.** Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and cooperative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and cooperation.
4. **Ethics: Participants should respect the legitimate interests of others.** Given the pervasiveness of information systems and networks in our

societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial, and participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others.

5. **Democracy: The security of information systems and networks should be compatible with essential values of a democratic society.** Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.
6. **Risk assessment: Participants should conduct risk assessments.** Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies, and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.
7. **Security design and implementation: Participants should incorporate security as an essential element of information systems and networks.** Systems, networks, and policies need to be properly designed, implemented, and coordinated to optimize security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and nontechnical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems, and networks, as well as an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.
8. **Security management: Participants should adopt a comprehensive approach to security management.** Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection, and response to incidents, systems recovery, ongoing maintenance, review, and audit. Information system and network security policies, practices, measures, and procedures should be coordinated and

integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved, and system requirements.

9. **Reassessment: Participants should review and reassess the security of information systems and networks, and should make appropriate modifications to security policies, practices, measures, and procedures.** New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess, and modify all aspects of security to deal with these evolving risks.