

**PART I**

---

# **INDUSTRY PRACTICES IN RISK MANAGEMENT**

COPYRIGHTED MATERIAL



# 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.<sup>1</sup> 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<sup>2</sup> 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

---

<sup>1</sup>Some also refer to ITRM as "information security risk management (ISRM)."

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

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

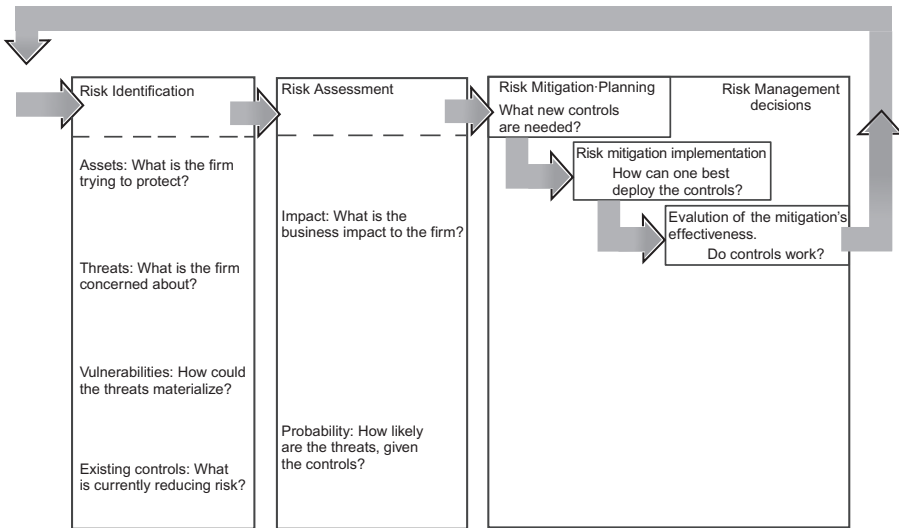


FIGURE 1.1. Risk management process as defined in this text.

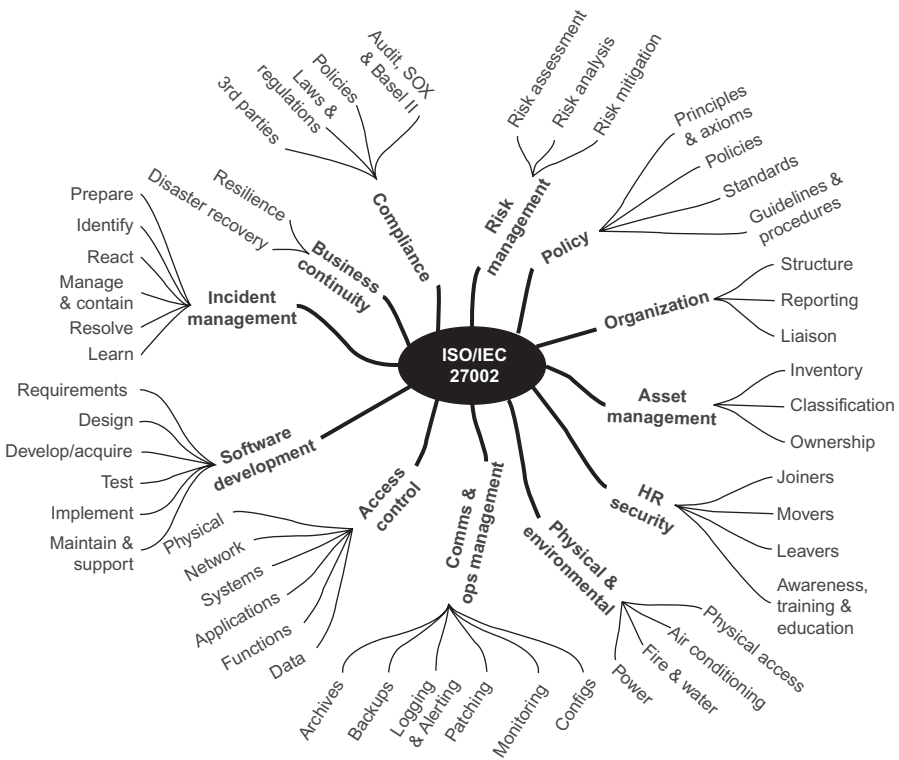


FIGURE 1.2. A view of information security management, as HR conceived in ISO 27002.

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*<sup>3</sup> have shown that the primary business and financial liabilities from the use of IT are directly related to how well, or poorly,

<sup>3</sup>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](http://www.itpolicycompliance.com) for the benefit of members.

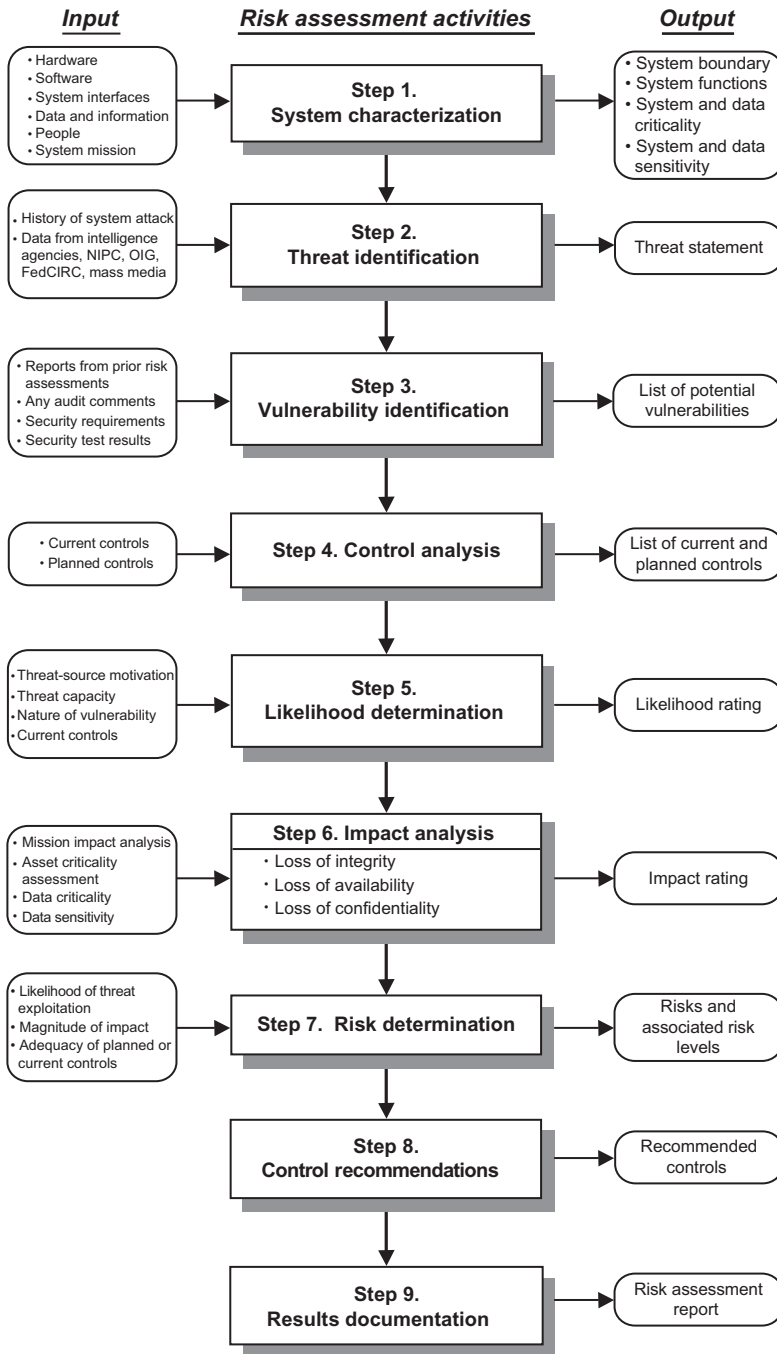
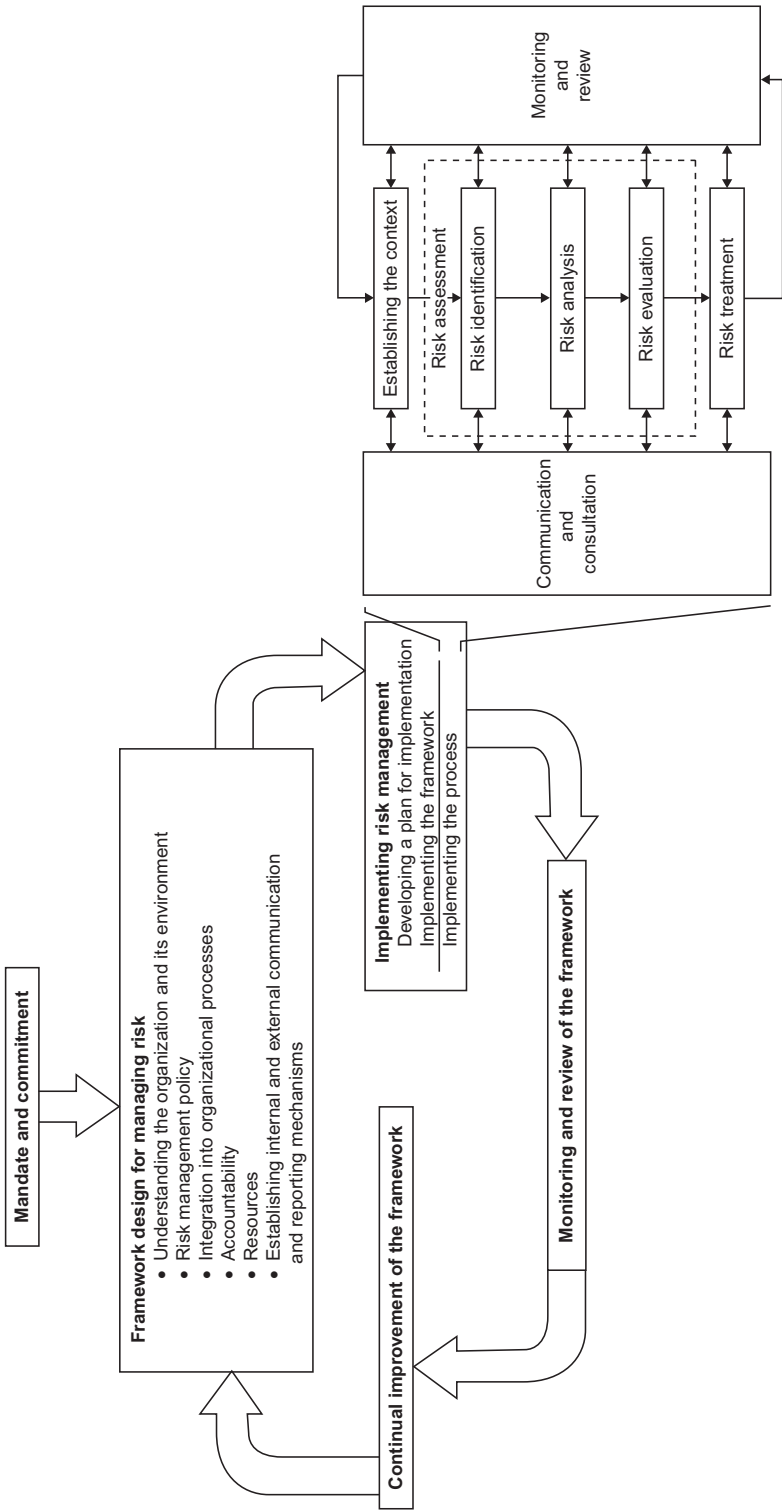
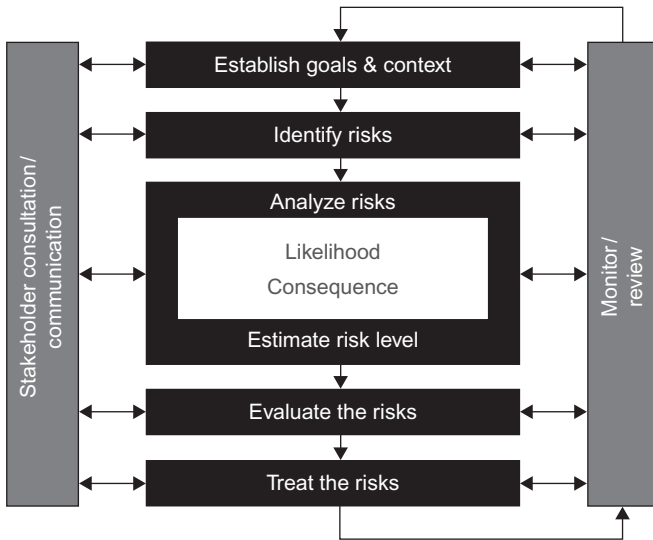


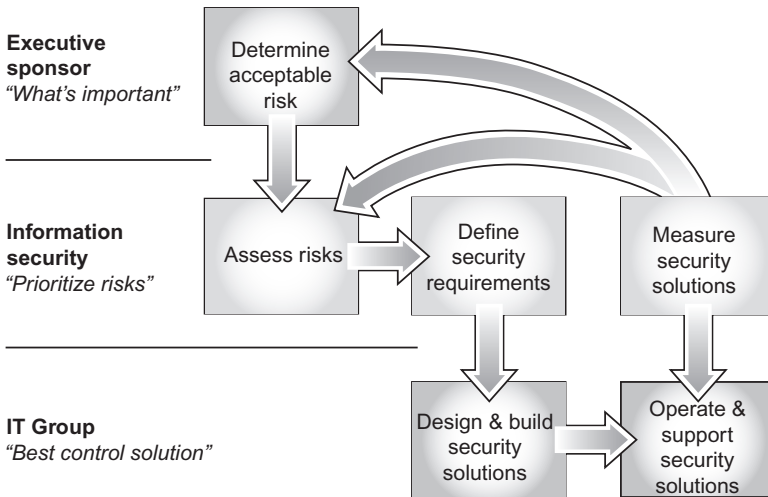
FIGURE 1.3. A graphical view of risk assessment, as conceived in NIST SP 800-30.



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

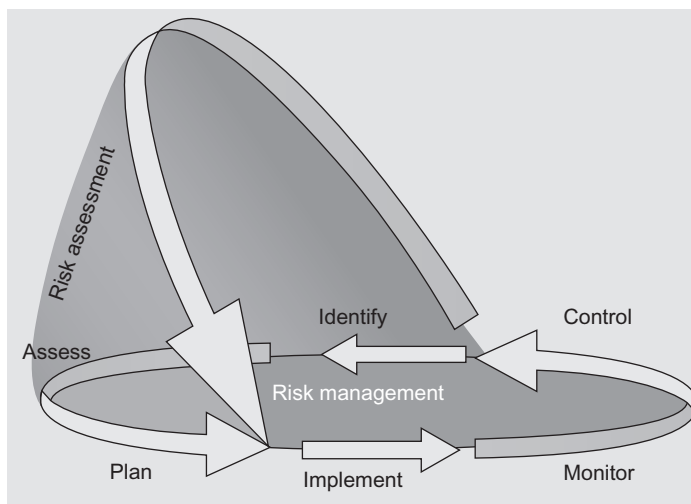


**FIGURE 1.5.** A view of the risk management process, as conceived in AS/NZS 4360:2004.



**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

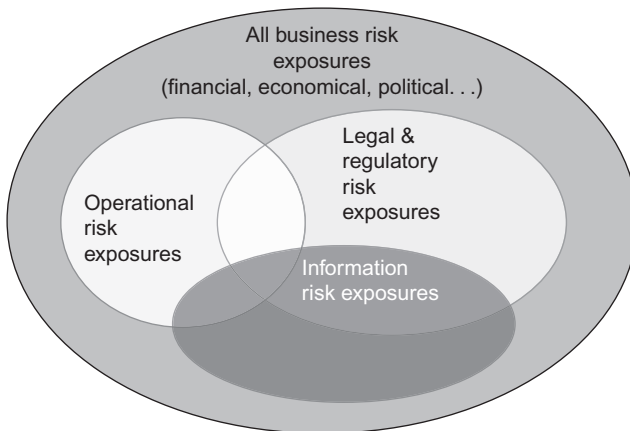
IT capabilities and information [ITP200901]. According to the Open Security Foundation's DataLossDB (<http://datalosssdb.org>), as of early 2009 over 358 million records have been exposed due to data loss incidents since January 2005.

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



**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.<sup>4-6</sup> 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  $\iota$ , block TCP port  $j$  used protocol  $\varphi$ , block TCP port  $k$  used protocol  $k$ , block TCP port  $l$  used protocol  $\lambda$ , block TCP port  $m$  used protocol  $\mu$ , 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

<sup>4</sup>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?

<sup>5</sup>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?

<sup>6</sup>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.<sup>7</sup> 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.

<sup>7</sup>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<sup>8</sup> (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<sup>9</sup> (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]:

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

<sup>9</sup>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 tsunamis 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<sup>SM</sup> 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](http://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. Sternecker, *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. Kadrach, *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: (b1) 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 I: 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 . . . .