3

Why Risk Assessment

With industry compliancy and information security laws and mandates being introduced in the past four years, the need for conducting a vulnerability and risk assessment is now paramount. These recent laws and mandates include the following:

- The Healthcare Information Privacy and Portability Act (HIPPA) is driving the need for vulnerability and risk assessments to be conducted within any health-care or health-care-related institution.
- The recent Gramm-Leach-Bliley Act (GLBA) is driving the need for vulnerability and risk assessments to be conducted within any banking or financial institution in the United States.
- The recent Federal Information Security Management Act (FISMA) is driving the need for vulnerability and risk assessments to be conducted for all United States federal government agencies.
- The recent Sarbanes-Oxley Act affects all publicly traded companies within the United States that have a market cap greater than $75 million; they are now subject to compliance with the Sarbanes-Oxley Act, Section 404, which also is driving the need for vulnerability and risk assessments to be conducted for publicly traded companies.
- The recent Canadian Management of Information Security Standard (MITS) requires regular security assessments for all Canadian federal government agencies.

The need to conduct vulnerability and risk assessments is being driven by these new laws and mandates. Organizations must now be information security conscious and must develop and implement proper security controls based on the results of their internal risk assessment and vulnerability assessment. By conducting a risk assessment and vulnerability assessment, an organization can uncover known weaknesses and vulnerabilities in its existing IT infrastructure, prioritize the impact of these vulnerabilities based on the value and importance of affected IT and data assets, and then implement the proper security controls and security countermeasures to mitigate those identified weaknesses. This risk

mitigation results in increased security and less probability of a threat or vulnerability impacting an organization's production environment.

Risk Terminology

With any new technology topic, terminology, semantics, and the use of terms within the context of the technology topic can be confusing, misused, and misrepresented. Risk itself encompasses the following three major areas: *risks*, *threats*, and *vulnerabilities*.

Risk is the probability or likelihood of the occurrence or realization of a threat. There are three basic elements of risk from an IT infrastructure perspective:

- **Asset**—An IT infrastructure component or an item of value to an organization, such as data assets.
- **Threat**—Any circumstance that could potentially cause loss or damage to an IT infrastructure asset.
- **Vulnerability**—A weakness in the IT infrastructure or IT components that may be exploited in order for a threat to destroy, damage, or compromise an IT asset.

An *IT asset* or *data asset* is an item or collection of items that has a quantitative or qualitative value to an organization. Examples of IT assets that organizations may put a dollar value or criticality value on include the following:

- **Workstations**—Hardware, software, and data assets stored at the end user's workstation location (PCs, PDAs, phones, and so on).
- **Operating systems software**—Operating system software, software updates, software patches, and their configuration and deployment on production services and workstations.
- **Application systems software**—Application software such as databases, client/server applications, software updates, software patches, and their configuration on production servers.
- **Local area network hardware and software**—Local area network infrastructure, TCP/IP, LAN switches, routers, hubs, operating system and application software within the LAN CPE equipment.
- **Wide area network hardware and software**—Wide area network infrastructure, TCP/IP, routers, operating system and application software within the WAN CPE equipment.
- **Network management hardware and software**—SNMP network management infrastructure, operating system and NMS application software, production NMS servers, data collection SNMP polling servers, network-monitoring CPE devices, SNMP MIB I and MIB II data collection and archiving.
- **Telecommunication systems**—Voice communication systems (PBX or IP Telephony), telephone CPE devices on desktops, operating system and application software (IP Telephony), voice-mail systems, automated attendants, and so on.

- **IT security hardware and software**—Operating system and security application software, production servers, DMZs, firewalls, intrusion detection monitoring systems, security monitoring, and alarm notification systems.
- **Systems and application servers, hardware, and software**—Operating systems, application software, client/server application software, production servers, and software code/intellectual property.
- **Intellectual property**—Customer data, customer databases, application data, application databases, information, and data assets. Intellectual property may have an intrinsic value to an organization depending on what the intellectual property is and whether the organization generates revenue from this intellectual property.
- **IT infrastructure documentation, configurations, and backup files and backup data**—Complete and accurate physical, logical, configuration, and setup documentation of the entire IT infrastructure, including backup files, backup data, disk storage units, and data archiving systems.

A *threat* is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset. From an IT infrastructure perspective, threats may be categorized as circumstances that can affect the confidentiality, integrity, or availability of the IT asset or data asset in terms of destruction, disclosure, modification, corruption of data, or denial of service. Examples of threats in an IT infrastructure environment include the following:

- **Unauthorized access**—The owner of the access rights, user ids, and passwords to the organization's IT systems and confidential information is compromised, and unauthorized access is granted to the unauthorized user who obtained the user ids and passwords.
- **Stolen/lost/damaged/modified data**—Loss or damage of an organization's data can be a critical threat if there are no backups or external archiving of the data as part of the organization's data recovery and business continuity plan. Also, if the data was of a confidential nature and is compromised, this can also be a critical threat to the organization, depending on the potential damage that can arise from this compromise.
- **Disclosure of confidential information**—Disclosure of confidential information can be a critical threat to an organization if that disclosure causes loss of revenue, potential liabilities, or provides a competitive advantage to an adversary.
- **Hacker attacks**—Unauthorized perpetrator who purposely and knowingly attacks an IT infrastructure and/or the components, systems, and data.
- **Cyber terrorism**—Because of the vulnerabilities that are commonplace in operating systems, software, and IT infrastructures, terrorists are now using computers, Internet communications, and tools to perpetrate critical national infrastructures such as water, electric, and gas plants, oil and gasoline refineries, nuclear power plants, waste management plants, and so on.

- **Viruses and malware**—*Malware* is short for malicious software, which is a general term used to categorize software such as a virus, worm, or Trojan horse that is developed to damage or destroy a system or data. *Viruses* are executable programs that replicate and attach to and infect other executable objects. Some viruses also perform destructive or discrete activities (payload) after replication and infection is accomplished.
- **Denial of service or distributed denial of service attacks**—An attack on a TCP/IP-based network that is designed to bring the network and/or access to a particular TCP/IP host/server to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, system administrators can install software fixes to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.
- **Acts of God, weather, or catastrophic damage**—Hurricanes, storms, weather outages, fires, floods, earthquakes, and total loss of IT infrastructures, data centers, systems, and data.

A *vulnerability* is a weakness in the system design, a weakness in the implementation of an operational procedure, or a weakness in how the software or code was developed (for example, bugs, back doors, vulnerabilities in code, and so on). Vulnerabilities may be eliminated or reduced by the correct implementation of safeguards and security countermeasures.

Vulnerabilities and weaknesses are common with software mainly because there isn't any software or code in existence that doesn't have bugs, weaknesses, or vulnerabilities. Many vulnerabilities are derived from the various kinds of software that is commonplace within the IT infrastructure. This type of software includes the following:

- **Firmware**—Software that is usually stored in ROM and loaded during system power up.
- **Operating system**—The operating system software that is loaded in workstations and servers.
- **Configuration files**—The configuration file and configuration setup for the device.
- **Application software**—The application or executable file `*.exe` that is run on a workstation or server.
- **Software Patch**—A small piece of software or code snippet that the vendor or developer of the software typically releases as software updates, software maintenance, and known software vulnerabilities or weaknesses.

Note

Why do software vendors and application software companies have Software Licensing Agreements (SLAs) that protect them from their own software vulnerabilities? Why do software companies have stringent Limited Warranty, Disclaimer of Warranties, Exclusion of Incidental, Consequential, and Certain Other Damages, and Limitations of Liability clauses in all their software products' SLAs?

The answer to these questions can be summarized quite simply: software vendors know they can't create and sell perfect code because of the human element. Software bugs and vulnerabilities are commonplace. Simply put, software vendors cannot guarantee that their software is bug-proof and free of vulnerabilities, so they must protect themselves from potential liability and damages that may be the result of a software vulnerability that is exploited by a hacker or unauthorized user.

Herein lies the fundamental problem—software has vulnerabilities, hackers and perpetrators know there are vulnerabilities, and organizations attempt to put the proper software patches and updates in place to combat this fundamental problem before being attacked. The key word here is *before* being attacked. Many organizations lack sufficient funds for securing their IT infrastructure by mandating a vulnerability window of 0 days or 0 hours, thus eliminating any software vulnerability potential threats. Achieving a vulnerability window of 0 days or 0 hours is virtually impossible given that software vendors cannot provide software patches fast enough to the general public after a vulnerability is exposed. In addition, the time required to deploy and install the software patch on production servers and workstations exposes an organization's IT infrastructure to potential threats from that vulnerability.

This gap in time is reality in IT infrastructures, especially because a majority of IT assets and devices have some kind of software loaded in them. Remember, vulnerabilities in software extend to firmware, operating systems, configuration files, and applications, and must be combated with a software maintenance, update, and patch maintenance plan. This encompasses the entire software, operating, and application software environment exposing potential vulnerabilities in any device that houses and runs this vulnerable software. In large organizations, combating the software vulnerability issue requires an enterprise, automated software patch-management solution.

The Computer Emergency Response Team (CERT) is an organization sponsored by Carnegie-Mellon University's Software Engineering Institute. Until 2003, CERT was the organizational body that was responsible for collecting, tracking, and monitoring vulnerability and incident reporting statistics. CERT can be found at www.cert.org. CERT publishes statistics for the following:

- **Vulnerabilities Reported**—This compilation is for vulnerabilities reported, not those that go unreported.
- **Vulnerability Notes Published**—These notes are published by CERT from data that is compiled from users and the vendor community describing known and documented vulnerabilities.

- **National Cyber Alert System Documents Published**—Information previously published in CERT advisories, incident notes, and summaries are now incorporated into National Cyber Alert System documents.
- **Security Alerts Published**—The total number of validated security alerts published by CERT.
- **Mail Messages Handled**—The total number of email messages handled by CERT.
- **Hotline Calls Received**—The total number of phone calls handled by CERT.
- **Incidents Reported**—Given the widespread use and availability of automated attack tools, attacks against Internet-connected organizations are common given the number of incidents reported.

As of 2004, CERT no longer publishes the number of incidents reported. Instead, CERT is working with others in the community to develop and report on more meaningful metrics for incident reporting, such as the 2004 E-Crime Watch Survey. Figure 3.1 shows the dramatic increase in known and documented vulnerabilities and the number of incidents that have occurred and have been recorded by www.cert.org during the past few years. Note that as the number of vulnerabilities increases, the number of incidents has also increased, but this value is misleading because the number of incidents that go unreported is unknown.

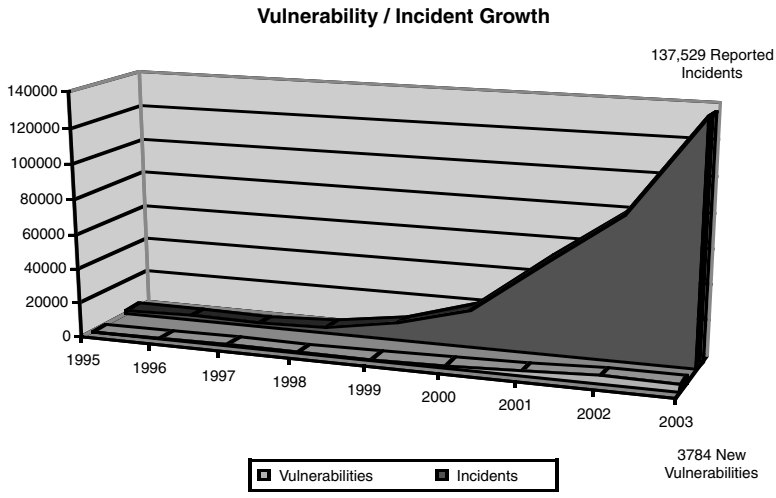

Figure 3.1 Rise in vulnerabilities and incidents.

Many of the security incidents indicated in 2003 on the www.cert.org website were the direct result of software vulnerabilities that were exploited by an attacker. These security incidents can be attributed to the "vulnerability window," which is the amount

of time that lapses between when a known vulnerability is identified and documented to when an organization implements the vulnerability fix or deploys the appropriate software patch.

Because of this vulnerability window issue, SQL Slammer, which was a known vulnerability posted by Microsoft in July 2002, affected nearly 90% of the world's SQL databases on Super Bowl Sunday, January 2003, six months after the vulnerability was exposed.

The stages of vulnerability in software are as follows:

1. Vendors release software and code with unknown vulnerabilities to the general public.
2. Vulnerability is discovered, communicated, documented, and published by the vendor. When the vulnerability is identified and communicated to the general public, this defines when the vulnerability window is open. This is referred to as VTopen.
3. A configuration-based software countermeasure (software patch) is created by the vendor and made available to the public.
4. The software patch is released and made available to the public.
5. The software patch is received, deployed, and installed on the affected devices. When the software patch is deployed and installed on the affected device, this defines when the vulnerability window is closed. This is referred to as VTclosed.

In Figure 3.2, the stages in vulnerabilities in software are defined. This gap in time between when a known vulnerability is identified and communicated to when that known vulnerability is mitigated through a software patch is referred to as the vulnerability window.

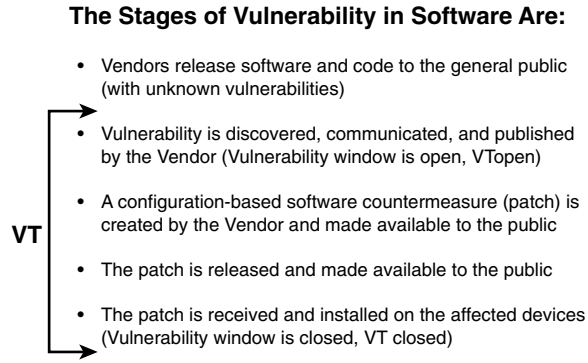

Figure 3.2 The vulnerability window.

From a vulnerability perspective, an IT asset or IT infrastructure is most vulnerable during the vulnerability window exposure time. This exposure time is referred to as vulnerability time:

Vulnerable Time (Vt) = Vt(open) - Vt(closed)

Most organizations, when they first conduct a vulnerability assessment on their IT infrastructure, servers, workstations, and systems, are shocked to realize that they are vulnerable because of software vulnerabilities inherent in the code. Upon realizing this, the ultimate goal for an organization is to prioritize those IT assets and IT infrastructure components to assess which IT assets should have their vulnerability time reduced. Reducing the vulnerability time will assist organizations in minimizing the potential risk and threats caused by software vulnerabilities. Many organizations create internal policies that state the maximum vulnerability time exposure for their mission critical IT assets and systems.

Organizations are now realizing that having an IT security architecture and framework consisting of policies, standards, procedures, and guidelines for their production IT systems, software, and applications is critical. Many organizations are apt to create a policy that defines the maximum acceptable vulnerability window for its mission-critical and production IT systems. This policy then drives the priorities for how funds are to be invested for risk mitigation via an enterprise patch-management solution.

Tip

When defining a policy for software vulnerability management, identifying and prioritizing mission-critical IT assets to prioritize the confidentiality, availability, and integrity of information assets is paramount.

Software vulnerabilities are documented and tracked by the U.S. Computer Emergency Readiness Team (US-CERT) in a public-accessible list called the Common Vulnerabilities and Exposures (CVEs) list. In 1999, the MITRE organization was contracted by the U.S. Computer Emergency Readiness Team to track, monitor, and update the CVE list. Today, the CVE list has grown to more than 7,000 unique documented vulnerability items, and approximately 100 new candidate names are added to the CVE list each month, based on newly discovered vulnerabilities. The CVE list can be found at `http://www.cve.mitre.org/`.

The CVE is merely a list or dictionary of publicly known information security vulnerabilities and exposures and is international in scope and free for public use. Each vulnerability or exposure included on the CVE list has one common, standardized CVE name. The CVE list is a community effort that encourages the support of hardware and software vendors. The CVE list is free and can be downloaded or accessed online at the previously mentioned website.

Tip

Use of the CVE list along with identifying IT and data assets are necessary first steps in conducting an internal risk assessment of an organization. The risk and vulnerability assessor should first identify all known IT assets and build an IT asset inventory using a spreadsheet or similar tool. Then, for each IT asset, the assessor should list the firmware, the operating system software, the application software, and the software patches and their version numbers currently loaded in that IT asset. Using the CVE list, a quick global search on known software vulnerabilities to the organization's IT asset list can be conducted, especially if the software version and software patch numbers from the software vendor can be obtained. This quick examination of known software vulnerabilities will help an organization uncover known software vulnerabilities. This information can be used to assess whether the value of the IT asset or the data asset requires remediation.

Prior to conducting an internal risk assessment, it is important to understand the new laws, mandates, and regulations that are driving organizations to create and implement information systems security plans and conduct vulnerability assessments. These new laws, mandates, and regulations are impacting IT infrastructures and their assets and are driving the need for conducting a thorough risk and vulnerability assessment on an IT infrastructure and its assets.

Laws, Mandates, and Regulations

The U.S. federal government has taken an active role in dealing with computer, Internet, privacy, and corporate threats, vulnerabilities, and exploits during the past five years. This is exemplified by the increase in new laws and mandates that were passed recently. These new laws and mandates encompass the following areas:

- **Cyber Laws and Crimes**—U.S. Code 1029 defines what a criminal activity is in regard to unauthorized access to devices and what the penalties for such crimes will be. U.S. Code 1030 defines what computer fraud is and other related activities in connection with computers.
- **Privacy**—New laws were enacted that protect an individual's confidentiality of personal information, such as social security number, passport number, driver's license number, ID numbers, and so on.
- **Financial Records Confidentiality**—New laws were enacted that protect an individual's confidential financial information, credit report, and any information pertaining to financial records such as user ids, passwords, bank account numbers, and financial data.
- **Corporate Integrity**—New laws were enacted to hold officers of publicly traded companies responsible and accountable for the accuracy and release of financial and annual reports as well as for documenting and ensuring that a proper information security architecture and framework with processes and controls are in place.

When dealing with risk assessment in an organization, there are now many new laws and mandates that impact the requirements and scope of the risk assessment.

Depending on the organization's vertical industry category, different laws and mandates will impact how that organization approaches its internal risk assessment and vulnerability assessment. Many of these new laws and mandates will assist in defining the scope of the risk assessment and vulnerability assessment, given the IT and data assets that must now have the proper security controls, procedures, and guidelines. The following new laws and mandates currently impact information security requirements and are briefly described in this chapter:

- **HIPAA**—Health Insurance Portability and Accountability Act, http://aspe.hhs.gov/admnsimp/pl104191.htm.
- **GLBA**—Gramm-Leach-Bliley Act, http://banking.senate.gov/conf/.

- **FISMA—Federal Information Security Management Act,** http://csrc.nist.gov/policies/FISMA-final.pdf.
- **SOX, Section 404**—Sarbanes-Oxley Act, Section 404, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 to address the lack of portability that individuals and their families had to deal with when changing jobs. HIPAA provides a way that individuals and their family members can have a continuity of health insurance even through job changes and perhaps even unemployment.

> **Note**
> It used to be people stayed in one or two jobs throughout a whole career. In those days people had no need for HIPAA. But today, in a time when jobs and even careers are constantly changing, HIPAA can make a big difference in your personal welfare or the welfare of your family.

Title I of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II requires the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

Under HIPAA law, the U.S. Department of Health and Human Services (DHHS) was required to publish a set of rules regarding privacy. The Privacy Rule was published on August 14, 2002, and the Security Rule was published in the Federal Register on February 20, 2003.

The privacy rule states three major purposes:

- To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information.
- To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care.
- To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

The security rule states the following:

"In addition to the need to ensure electronic health care information is secure and confidential, there is a potential need to associate signature capability with information being electronically stored or transmitted."

Today, there are numerous forms of electronic signatures, ranging from biometric devices to digital signature. To satisfy the legal and time-tested characteristics of a written signature, however, an electronic signature must do the following:

- Identify the signatory individual;
- Assure the integrity of a document's content; and
- Provide for nonrepudiation; that is, strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid. Currently, the only technically mature electronic signature meeting the above criteria is the digital signature."

Gramm-Leach-Bliley-Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) was signed into law in 1999 and resulted in the most sweeping overhaul of financial services regulation in the United States by eliminating the long-standing barriers between banking, investment banking, and insurance. Title V addresses financial institution privacy with two subtitles. Subtitle A addresses this by requiring financial institutions to make certain disclosures about their privacy policies and to give individuals an opt-out capability. Subtitle B criminalizes the practice known as pretexting, where someone will misrepresent themselves to collect information regarding a third party from a financial institution.

Various sections of the GLBA provide support to Title V in a variety of ways. For example:

- **Section 502**—Requires that a financial institution not disclose, directly or indirectly or through any affiliate, any personal information to a third party.
- **Section 503**—Requires the financial institution to disclose its policies annually during the institution's relationship with a given customer.
- **Section 504**—Requires that the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the Secretary of the Treasury, the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC), after consultation with representatives of state insurance authorities designated by the National Association of Insurance Commissioners, are to prescribe regulations to carry out subtitle A.

Under GLBA law, financial institutions are required to protect the confidentiality of individual privacy information. Under the GLBA definition, financial institutions may include banks, insurance companies, and other third-party organizations that have access to an individual's private and confidential financial, banking, or personal information. As specified in GLBA law, financial institutions are required to develop, implement, and maintain a comprehensive information security program with appropriate administrative,

technical, and physical safeguards. This information security program must include the following:

- Assigning a designated program manager for the organization's information security program
- Conducting periodic risk and vulnerability assessments
- Performing regular testing and monitoring
- Defining procedures for making changes in lieu of test results or changes in circumstance

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) was signed into law in 2002 as part of the E-Government Act of 2002, replacing the Government Information Security Reform Act (GISRA). FISMA was enacted to address the information security requirements for non-national-security government agencies. FISMA provides a statutory framework for securing government-owned and operated IT infrastructures and assets. FISMA requires the CIO to carry out the following responsibilities:

- Develop and maintain an agencywide information assurance (IA) program with an entire IT security architecture and framework.
- Ensure that information security training is conducted annually to keep staff properly trained and certified.
- Implement accountability for personnel with significant responsibilities for information security.
- Provide proper training and awareness to senior management such that proper security awareness programs can be deployed.

The FISMA law also requires the agency head, in this case the secretary of the Navy, to

- Develop and maintain an agencywide information assurance (IA) program with an entire IT security architecture and framework.
- Ensure each agency has a sufficient number of trained information security personnel to ensure agencywide IA.
- Require annual reports from the CIO regarding the effectiveness of the agency's IA programs and progress on any required remedial actions.

The FISMA law also requires each federal agency to develop, document, and implement an agencywide information security program that includes the following elements:

- Periodic risk assessments (at least annually).
- Risk-assessment policies and procedures that cost-effectively reduce the risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each agency information system, and ensure compliance with FISMA.

- Subordinate plans for networks, facilities, and groups of systems as appropriate.
- Security awareness training for agency personnel, including contractors and system users.
- Periodic (at least annually) testing and evaluation of the effectiveness of information security policies, procedures, and practices.
- Processes for planning, implementing, evaluating, and documenting remedial action to address deficiencies in agency information security policies, procedures, and practices.
- Procedures for detecting, reporting, and responding to security incidents.
- Plans and procedures to ensure continuity of operations for information systems that support agency operations and assets.

Finally, FISMA law requires each federal agency to report to Congress annually by March 1. The agency FISMA report must address the adequacy and effectiveness of information security policies, procedures, and practices.

In addition to the annual report, FISMA requires that each agency conduct an annual, independent evaluation of the IA program and practices to determine their effectiveness.

FISMA requirements brought about for the first time in U.S. federal government history a definition for agency information security and human accountability for the protection of federal government IT infrastructure and data assets.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) was signed into law in 2002 and named after its authors: Senator Paul Sarbanes (D-MD) and Representative Paul Oxley (R-Ohio). This act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

Corporate and accounting fraud became commonplace thanks to the Enron and MCI Worldcom fiascos, which were the driving force in the creation and adoption of the SOX law. This was the first law of this kind that requires U.S.-based corporations to abide by new anticrime laws, address a broad range of wrongdoings, and requires a set of comprehensive controls be put in place while holding the CEO and CFO accountable for the accuracy of the information.

SOX law applies to U.S.-based publicly traded companies with market capitalizations of $75 million or more. SOX compliancy commenced in fiscal year 2004, with fiscal year 2005 being the first full year of SOX compliancy. Many organizations are now assessing and eliminating identified gaps in defined control objectives and in particular, information-security-related control objectives.

The SOX structure and charter consists of the following organizational elements:

- **Public Company Accounting Oversight Board (PCAOB)**—The SOX law created and enacted the PCAOB to oversee and guide auditors in maintaining SOX compliancy.

- **PCAOB Was Charted with Creating Proposed Auditing Standards for SOX Compliancy**—PCAOB was tasked with creating consistent auditing standards for SOX compliancy.
- **PCAOB Selected Controls Frameworks from Committee of Sponsoring Organizations (COSO)**—The goal of the COSO was to develop a standardized control framework that provided structured guidelines for implementing internal controls.

To supplement the control framework structure created by the COSO, the PCAOB selected Information Systems Audit and Control Association's (ISACA) control objectives for information and related technology framework (COBIT). Assistance from the IT Governance Institute used COSO and COBIT frameworks to create specific IT control objectives for SOX. The IT Governance Institute Framework includes the following major areas:

- **Security Policies**—Policies are the most important control objectives to define because they encompass the entire organization and act as an element of that organization's overall IT security architecture and framework.
- **Security Standards**—Standards allow the entire organization to follow a consistent definition for how securing the IT infrastructure and assets will be implemented using hardware and software security tools and systems.
- **Access and Authentication**—Requires that the organization have a consistent definition for end user access control and how those users will be authenticated prior to access being granted to the systems and information.
- **User Account Management**—Requires that access control and management of access control be defined consistently across the organization with stringent controls put in place to track, monitor, and ensure system access is not compromised.
- **Network Security**—Requires that the network infrastructure (LAN, WAN, Internetworking, Egress Points, Internet Access, DMZ, and so on) be designed and configured according to the IT security architecture and framework that is defined for the organization.
- **Monitoring**—Requires that the organization have a plan to adequately monitor the security of the IT infrastructure and the various IT systems and assets. This plan undoubtedly requires IT security tools and systems to monitor, audit, and report on network activity and system access.
- **Segregation of Duties**—Requires that the IT organization and, in particular, the roles, responsibilities, and accountabilities for information security be defined and documented in a segregated manner given the layers of responsibilities that are typical in an IT infrastructure.
- **Physical Security**—Requires that physical access and physical security be defined that house and protect the IT infrastructure and assets (for example, data centers, computer rooms, server rooms).

Two sections indirectly and directly impact IT infrastructures and information security: Section 302 and Section 404.

Section 302 impacts information security indirectly in that the CEO and CFO must personally certify that their organization has the proper internal controls. Section 302 mandates that the CEO and CFO must personally certify that financial reports are accurate and complete and that the data they use for financial reporting is accurate and secure. In addition, the CEO and CFO must also report on effectiveness of internal controls around financial reporting.

Section 404 mandates that certain management structures, control objectives, and procedures be put into place. Compliance with Section 404 requires companies to establish an infrastructure that is actually designed to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse.

When developing management structures, control objectives, and procedures for SOX Section 404 to protect and preserve records and data from destruction, loss, unauthorized alteration or other misuse, five major areas must be addressed:

- **Control Environment**—The Control Environment defines the scope of the SOX Section 404 responsibility, which includes an organization's IT infrastructure and assets.
- **Risk Assessment**—As per SOX Section 404, a risk assessment for the Control Environment that includes an organization's IT infrastructure and assets is to be conducted.
- **Control Activities**—Specific control activities (for example, asset management, change control board/procedures, configuration management) must be defined and documented for the Control Environment, which usually includes the IT infrastructure and IT and data assets.
- **Information and Communications**—Documentation and communication of the findings and assessment for the Control Environment must be done such that management can take the appropriate steps to mitigate identified risks, threats, and vulnerabilities.
- **Monitoring**—Continuous monitoring, configuration change update tracking, and other internal and external influences to the Control Environment must be done to maintain compliancy with SOX Section 404 on an annual basis.

Organizations today are being forced to create IT security architectures and frameworks to properly address the requirements of these new laws, mandates, and regulations. After an IT security architecture and framework is in place, risk and vulnerability assessments are needed to identify weaknesses and gaps in the deployment of information security architectures and frameworks.

By conducting a risk and vulnerability assessment, an organization will be able to identify and get a baseline for their current level of information security. This baseline will form the foundation for how that organization needs to increase or enhance its current level of security based on the criticality or exposure to risk that is identified during

the risk and vulnerability assessment conducted on the IT infrastructure and assets. From here, it is important to understand risk assessment best practices and what the goal of a risk assessment should be for an organization.

Risk Assessment Best Practices

When you're conducting a risk assessment, it is important to define what the goals and objectives are for the risk assessment and what that organization would like to accomplish by conducting one.

Risk and vulnerability assessments provide the necessary information about an organization's IT infrastructure and its asset's current level of security. This level of security allows the assessor to provide recommendations for increasing or enhancing that IT asset's level of security based on the identified and known vulnerabilities that are inherent in the IT infrastructure and its assets.

There are many best practices or approaches to consider when conducting a risk and vulnerability assessment on an IT infrastructure and its assets. These best practices or approaches will vary depending on the scope of the IT infrastructure and its assets. To properly secure and protect an organization's IT infrastructure and assets, a significant amount of design, planning, and implementation expertise is required to ensure that the proper level of security is designed and implemented properly. While preparing and conducting a risk assessment, the following best practices or approaches should be considered:

- **Create a Risk Assessment Policy**—A risk assessment policy will define what the organization must do periodically (annually in many cases), how risk is to be addressed and mitigated (for example, a minimum acceptable vulnerability window), and how that organization must carry out a risk assessment for its IT infrastructure components and its assets. Creation of a risk assessment policy is usually done after the first risk assessment is conducted as a post-assessment activity. In some cases, organizations create a risk assessment policy and then implement the recommendations that the policy defines.
- **Inventory and Maintain a Database of IT Infrastructure Components and IT Assets**—One of the most tedious but important first steps in conducting a risk or vulnerability assessment is to identify and inventory all known IT infrastructure components and assets. Without a complete and accurate inventory of IT infrastructure components and IT assets, an asset valuation, criticality, or importance evaluation cannot be performed.
- **Define Risk Assessment Goals and Objectives in Line with Organizational Business Drivers**—Defining the risk assessment's goals and objectives is the second step in conducting a risk assessment for your IT infrastructure components and IT assets. Aligning these goals and objectives with the organization's business drivers will allow the organization to prioritize and focus on critical systems and assets first given the budget limitations that most organizations face.

- **Identify a Consistent Risk Assessment Methodology and Approach for Your Organization**—Defining and selecting the risk assessment methodology and approach for your organization will be dependent on the organization's ability to identify accurate IT infrastructure components and assets, the ability to identify asset value and/or asset importance/criticality to the organization, and how the organization makes business decisions. This will be further examined in Chapter 4, "Risk Assessment Methodologies."
- **Conduct an Asset Valuation or Asset Criticality Valuation as per a Defined Standard Definition for the Organization**—Depending on the accuracy and availability of inventory documentation and asset valuation data (for example, capital dollars spent on hardware, software, integration, maintenance, staff salaries, G&A overhead), the organization should conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine which IT infrastructure components and assets are most important to the organization (either in monetary value or importance value). This will be further examined in Chapter 4.
- **Define and/or Limit the Scope of the Risk Assessment Accordingly by Identifying and Categorizing IT Infrastructure Components and Assets as Critical, Major, and Minor**—Depending on the scope of the risk assessment, an organization may or may not be faced with a limited budget to conduct a thorough risk and vulnerability assessment. In many cases, organizations have limited budgets to conduct a risk and vulnerability assessment and must limit the scope on the mission-critical IT infrastructure components and assets only. Although this solution exposes the organization to potential risks, threats, and vulnerabilities, a defense-in-depth approach to assessing and mitigating risks, threats, and vulnerabilities can still be pursued.
- **Understand and Evaluate the Risks, Threats, and Vulnerabilities to Those Categorized IT Infrastructure Components and Assets**—After the IT infrastructure components and assets are identified and an asset valuation or asset criticality assessment is conducted, the next step in the risk assessment and vulnerability assessment is to assess the impact that potential risks, threats, and vulnerabilities have on the identified IT infrastructure components and assets. By aligning the potential risks, threats, and vulnerabilities to the prioritized IT infrastructure components and assets, management can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities that are known.
- **Define a Consistent Standard or Yardstick of Measurement for Securing the Organization's Critical, Major, and Minor IT Infrastructure Components and Assets**—To properly categorize IT infrastructure components and assets, a consistent standard definition or yardstick of measurement needs to be defined. This standard definition refers to how the organization will define and

categorize IT infrastructure components and assets to be Critical, Major, or Minor. This definition can be based on monetary value, requirement by law or mandate, or criticality or importance to the organization. The selection criteria or requirements for defining this standard definition should be defined by management and incorporated into the risk assessment policy when it is drafted and implemented.

- **Perform the Risk and Vulnerability Assessment as per the Defined Standard or Yardstick of Measurement for the Organization's IT Infrastructure Assets**—After the standard definition or yardstick of measurement is defined for IT asset categorization, the risk and vulnerability assessment can be aligned to the priorities as defined by the results of the standard definition for categorization of the organization's IT infrastructure components and assets. This is important given that most organizations have a limited budget for implementing information security countermeasures and must prioritize how they spend funds on information security, especially if they are under compliance requirements with new laws, mandates, and regulations that require them to do so or be subject to penalties.
- **Prepare a Risk and Vulnerability Assessment Final Report That Captures the Goals and Objectives Aligned with the Organization's Business Drivers, Provides a Detailed Summary of Findings, Provides an Objective Assessment and Gap Analysis of Those Assessment Findings to the Defined Standard, and Provides Tactical and Strategic Recommendations for Mitigating Identified Weaknesses**—The risk and vulnerability assessment final report is the primary document that presents all the findings, information, assessments, and recommendations for the organization. The final assessment report becomes the instrument for management to make sound business decisions pertaining to the organization's overall risk and vulnerability assessment and how that organization will mitigate the identified risks, threats, and vulnerabilities.
- **Prioritize, Budget, and Implement the Tactical and Strategic Recommendations Identified During the Risk and Vulnerability Assessment Analysis**—After the findings, assessment, and recommendations are presented to management, it is important to prioritize them, create a budget, and have a tactical and strategic plan for implementing the recommendations presented in the final report. These recommendations may impact the entire organization and may take months, if not years, to fully implement. This prioritization of tactical and strategic recommendations will enable the organization to make sound business decisions with the defined goals and objectives of the risk and vulnerability assessment.
- **Implement Organizational Change Through an Ongoing Security Awareness and Security Training Campaign to Maintain a Consistent Message and Standard Definition for Securing the Organization's IT**

Infrastructure and Assets—Implementing organizational change requires an education and security awareness training plan for all employees or authorized users of the organization's IT systems, resources, and data. Mitigating risk requires all employees and users within the organization to abide by security awareness training.

Defining and implementing these risk assessment best practices does not come easily and requires careful analysis and decision making unique to the organization's business drivers and priorities as an organization. For example, a bank or financial institution requires more stringent use of encryption technology to ensure confidentiality of privacy data, whereas an organization that is not subject to stringent confidentiality requirements may put less investment in encryption technology and more investment in other areas.

These risk assessment best practices allow an organization to consider the big picture of why that organization should conduct a risk and vulnerability assessment and how they should methodically approach the assessment. More importantly, these best practices align that organization's business drivers and defined standards to the risk and vulnerability assessment to assist management in making sound business decisions based on available budgets, minimum acceptable vulnerability windows, and importance and criticality of IT infrastructure components and assets.

Understanding the IT Security Process

As defined earlier in Chapter 2, "Foundations and Principles of Security," designing and implementing a sound IT security architecture and framework requires a thorough analysis and examination of how availability, integrity, and availability (A-I-C Triad) is designed and implemented on the IT infrastructure components and assets in the overall information security plan.

Attacks on an IT infrastructure and assets can disrupt availability of service resulting in the following:

- **Loss of Productivity**—Downtime equals lost productivity to organizations. Lost productivity can result in loss in dollars and time.
- **Violation of Service Level Agreements**—Service providers or outsourcing service organizations can be in violation of contractual service level agreements (SLAs) that may result in penalties and financial compensation.
- **Financial Loss**—Lost productivity and violation of SLAs all result in financial loss. Depending on the criticality of the financial loss, this may change the prioritization of how that organization funds and secures its IT infrastructure components and assets.
- **Loss of Life**—System downtime or even loss of data can impact IT infrastructures and systems that are used to maintain, support, and respond to human life issues.

Attacks on an IT infrastructure and assets can disrupt the integrity of information that organizations disseminate:

- **Attack Against the Integrity of a System**—A system's integrity requires sound access control processes and authentication that the user is authorized to access the system. Attacks against the integrity of the system start with access control and include the manipulation of information or data, including destruction of data.
- **Information or Data Can Be Modified, Altered, or Destroyed**—A system's integrity can be compromised if access is granted to a perpetrator and the organization's information or data is modified, altered, or destroyed.

Caution

Attacks on an IT infrastructure and assets can disrupt the confidentiality of information and data assets. Attacks can expose confidential information such as corporate or intellectual property secrets, financial information, and health records, which can result in identity theft. Maintaining the confidentiality of privacy records and financial data pertaining to individuals is now subject to laws, mandates, and regulations dictated by HIPAA and GLBA.

Unfortunately, implementing a robust IT security architecture and framework and conducting a risk and vulnerability assessment is not something that can be taken lightly by an organization. This is true given that many IT systems and applications were not designed with security in mind; many organizations are struggling to deal with the lack of security in their IT infrastructure components and applications that are currently in production. Security was always an afterthought and now for the first time, information security is in the forefront of system requirements definitions and system designs.

Security as a process would define an entire development life cycle that incorporates security requirements into the system or application design from the very beginning. By designing a system (hardware, software, or multiplatforms) or application (software code) from the ground up that includes security requirements for availability, integrity, and confidentiality, minimization of the risks, threats, and vulnerabilities can be designed into the system or application up front. Security as a process would have security requirements incorporated throughout all the steps of the system or application development and design life cycle. These steps include the following:

- **Risk/Threat/Vulnerability Analysis**—Ideally, this is done prior to any system requirements or application requirements being defined and documented. This initial risk, threat, and vulnerability analysis will attempt to identify and mitigate the exposure by incorporating appropriate security countermeasure requirements into the overall system or application design.

- **System Requirements Definition and Design**—After a risk, threat, and vulnerability analysis is conducted, the system's or application's requirements definition can incorporate the technical requirements along with embedded security and security countermeasures requirements to mitigate the identified and known exposures to that system or application.
- **Functional Design**—After the system's technical requirements definition and security requirements definition are complete, a comprehensive system or application functional design can be documented. The functional design will describe the functionality of the system or application and how security is embedded into the functionality of the system or application.
- **Security Design**—After the system requirements definition, technical design, and functional design are completed, the specific security design for the system and application can be conducted based on the security requirements that are identified as being needed. Depending on the criticality and importance of the security design, implementation of security elements into the system or application design will assist the system designers in ensuring the availability, integrity, and confidentiality of the system or application and its data.
- **System/Application Test Plan**—Like any new system or application, a thorough system or application test plan must be developed to ensure that all the technical, functional, and security design elements were developed properly and do not contain identifiable bugs, performance issues, or potential exposure to risks, threats, and vulnerabilities.
- **System Design Verification/Validation**—A thorough system design verification and validation assessment will come from the results of the system or application test plan. The results of the test plan will uncover whether the system design properly incorporated the technical, functional, and security requirements as defined in the system or application development life cycle.

As shown in Figure 3.3, step 4 in the System Development Life Cycle incorporates security design within the design and development phase of the life cycle. This is an important first step to ensure that the proper security controls, security objectives, and security goals are initiated properly.

This IT security process is what is currently missing from many organizations when it comes to designing and implementing new IT systems and applications throughout the organization. As organizations incorporate security requirements and design into the development life cycle, more IT systems and applications will have the inherent security controls to ensure that the availability, integrity, and confidentiality goals and objectives are achieved.

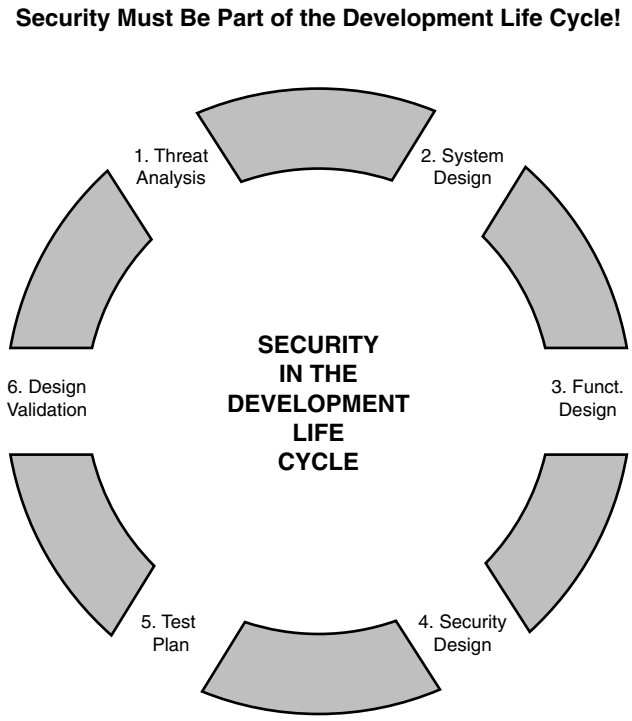

Figure 3.3 Security in the development life cycle.

When conducting a risk and vulnerability assessment on IT systems and applications, examination of the defined security goals and objectives can be done. This examination will include a review of the IT system's or applications' security requirements and how they were implemented in production. Understanding this void in the development life cycle will help IT organizations fill the void with proper security requirements and security design steps in the overall development effort. By implementing the proper security controls and requirements into the system and application design up front, minimization of exposure to risks, threats, and vulnerabilities can be achieved, thus eliminating costly security countermeasures and other security controls around the IT system or application that lacks the proper security controls.

The Goals and Objectives of a Risk Assessment

An organization may consider many goals and objectives prior to undergoing a risk and vulnerability assessment. Some of these goals and objectives may be the result of required compliancy to new laws, mandates, and regulations for information security. Security as a process for an IT infrastructure and assets is primarily concerned with prevention,

detection, and response. A sound and comprehensive security process coupled with a robust IT security architecture and framework will assist the organization in ensuring the security of the IT infrastructure and assets as per the organization's minimum acceptable risk or exposure level.

Security Process Definition

Security as a process typically includes three key elements: prevention, detection, and response.

Prevention deals with the implementation of security controls and countermeasures or safeguards during the initial security design phase of the development life cycle. By incorporating security requirements into the design phase of the development life cycle, prevention or protection is easier to implement because it is inherent in the system's or application's design up front. Prevention techniques and solutions should be designed and developed into the system or application to ensure that availability, integrity, and confidentiality for the system or application are implemented.

Detection or monitoring deals with monitoring the IT infrastructure and assets. This includes monitoring log files, audit trails, intrusion detection system reporting, and reviewing vulnerability assessments reports and CVE items that are installed within the production IT infrastructure. Continuous monitoring of the IT infrastructure and assets for newly discovered risks, threats, and vulnerabilities is an ongoing process and the responsibility of information security professionals who are responsible and accountable for securing the IT infrastructure and assets.

Response is the reaction that an IT organization takes in response to a security breach or incident from a known or unknown risk, threat, or vulnerability. Response usually encompasses the following four areas:

- **Business Continuity Plan (BCP)**—Organizations that have a significant amount of investment in the IT infrastructure and assets typically create, test, and validate an internal BCP plan to address how to maintain operations and functionality in the event of lost critical assets. A BCP plan typically includes a risk assessment, asset valuation or criticality assessment, and a vulnerability assessment in order for the organization to build the proper BCP plan in the event of risk, threat, or vulnerability incidents affecting the production IT infrastructure and assets.
- **Disaster Recovery Plan (DRP)**—Organizations that have a significant exposure to risks and threats, particularly weather related, act of God related, or war related, must have a plan for dealing with a disaster (for example, hurricane, flood, fire). A DRP plan typically requires an outsourcing solution and/or a hot site that replicates the main IT infrastructure and systems that the organization is fully dependent on to maintain its business operations.
- **Security Incident Response Team (SIRT) and Plan**—Many organizations have their own internal Security Incident Response Team (SIRT) that comprises a

cross-section of human resources, legal, IT, and departmental management personnel. The SIRT typically has authority to collect and conduct investigations pertaining to security breaches and/or security incidents. Because of the potential sensitivity and nature of a security breach or incident, confidentiality and maintaining the integrity of data and information used to investigate and collect the data and information must be conducted under certain rules and guidelines. This is critical if forensic data is to be used in a court of law as evidence if a criminal charge is put on the perpetrator or perpetrators for violation of access or unauthorized use of an organization's IT infrastructure and assets.

- **Forensic Analysis Plan**—Depending on the laws, mandates, regulations, and jurisdiction of the security breach and/or incident occurring, a carefully developed forensic analysis plan and computer forensic data and information collection must be followed for the data and information to be admissible in a court of law as evidence for a criminal case in the United States. The CIRT team must be properly trained and the IT security professionals who collect and retrieve data and information must abide by the forensic analysis plan where data and information collected during the security breach or incident investigation is pursued.

Depending on the organization's compliancy requirements to new laws, mandates, and regulations, the priorities, definition of criticality or importance, and the goals and objectives that are identified for conducting a risk and vulnerability assessment will be unique to that organization.

Goals and Objectives of a Risk and Vulnerability Assessment

Some of the more common goals and objectives of conducting a risk and vulnerability assessment are as follows:

- IT organizations can have an accurate inventory of IT assets and data assets.
- IT organizations can have prioritized IT assets and data assets based on different measurements criteria—asset value in dollars, the importance of assets to the organization, or the criticality to the organization.
- Risks, threats, and known vulnerabilities can be identified and documented for the IT organization's production, infrastructure, and assets.
- Risks, threats, and known vulnerabilities can be prioritized based on impact or criticality of the IT asset or data asset that it impacts.
- The vulnerability window can be identified and minimized according to the organization's minimum acceptable tolerance to being vulnerable.
- Remediation or mitigation of the identified risks, threats, and vulnerabilities can be properly budgeted and planned according to the prioritization or criticality of IT assets and data assets.
- Compliancy with new information security laws, mandates, and regulations can be achieved by first conducting a risk and vulnerability assessment.

- Identification of the gaps or voids in the organization's IT security architecture and framework can be found with specific recommendations for closing the gaps and voids.
- A risk and vulnerability assessment identifies the exposures, risks, threats, and vulnerabilities that the organization is subject to and assists the IT organization in justifying the cost of needed security countermeasures and solutions to mitigate the identified risks, threats, and vulnerabilities.
- A risk and vulnerability assessment provides an IT organization with an objective assessment and recommendations to the organization's defined goals and objectives for conducting the risk and vulnerability assessment.
- A risk and vulnerability assessment assists IT organizations with understanding the return on investment if funds are invested in IT security infrastructure.

Summary

Because of the increase in risks, threats, and vulnerabilities and other exploits in IT infrastructures, IT security professionals are not able to address known vulnerabilities in time before the next unknown vulnerability appears. This *catch-22* scenario requires IT security professionals and management to make prioritized decisions pertaining to which IT assets get funding for security controls and security countermeasures first. Many IT budgets are limited, especially for investments in securing the IT infrastructure. This limitation forces organizations to prioritize funding for securing their most critical IT and data assets first. In other organizations, new laws, mandates, and regulations are requiring organizations to invest in information security and IT security infrastructure.

Risk assessments allow the organization to assess from a criticality and importance factor which IT and data assets must be protected and secured more than others. In addition, a risk assessment will allow an organization to make tactical and strategic business decisions pertaining to securing its most valuable IT and data assets. Without a risk assessment, IT management would be guessing as to how best to spend its funds on security for its IT and data assets.

Finally, a risk and vulnerability assessment allows an organization to understand the roles, responsibilities, and accountabilities for the IT professionals and IT security professionals in an organization. Risk and vulnerability assessments typically find gaps and voids in the human responsibility and accountability for dealing with risks, threats, and vulnerabilities. Given the magnitude of the IT security responsibility, segregation of duties and dissemination of these duties to IT and IT security professionals is a critical follow-up step in many IT organizations to properly address the human responsibilities and accountabilities for ensuring that the availability, integrity, and confidentiality of IT infrastructure components and assets are met.

The dissemination of roles, responsibilities, and accountabilities throughout the IT infrastructure or areas of risk management can be clearly defined after the risks, threats, and vulnerabilities are identified within an organization's IT infrastructure.

Key Terms

The following acronyms and terms are used in this chapter. For the explanation and definition purpose of this chapter, these acronyms and terms are defined as follows:

Audit A term that typically accompanies an accounting or auditing firm that conforms to a specific and formal methodology and definition for how an investigation is to be conducted with specific reporting elements and metrics being examined (such as a financial audit according to Public Accounting and Auditing Guidelines and Procedures).

Assessment An evaluation and/or valuation of IT assets based on predefined measurement or evaluation criteria. This does not typically require an accounting or auditing firm to conduct an assessment such as a risk or vulnerability assessment.

Disclaimer of Warranties A legal term that denies or disavows the user's legal claim of warranty of the product, hardware, or software.

Exclusion of Incidental, Consequential, and Certain Other Damages A legal term that protects and indemnifies the organization from external incidents, consequences, or other certain damages that may arise from the use of the organization's hardware or software.

Hot Site A remote and secure data center that replicates the production IT infrastructure, systems, applications, and backup data of the production environment.

IT Information technology.

IT Asset Information technology asset such as hardware or software or data.

IT Asset Criticality The act of putting a criticality factor or importance value (Critical, Major, or Minor) in an IT asset.

IT Asset Valuation The act of putting a monetary value to an IT asset.

IT Infrastructure A general term to encompass all information technology assets (hardware, software, data), components, systems, applications, and resources.

IT Security Architecture and Framework A document that defines the policies, standards, procedures, and guidelines for information security.

Law A rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority (U.S. federal government, state government, and so on).

Limitation of Liability and Remedies A legal term that limits the organization from the amount of financial liability and the limitation of the remedies the organization is legally willing to take on.

Limited Warranty A legal term that defines but limits the written guarantee of the integrity of a product and of the maker's responsibility for the repair or replacement of defective parts.

Mandate A formal order from a superior court or official to an inferior one, such as a mandate from the U.S. federal government to state government.

Qualitative Analysis A weighted factor or nonmonetary evaluation and analysis that is based on a weighting or criticality factor valuation as part of the evaluation or analysis.

Quantitative Analysis A numerical evaluation and analysis that is based on monetary or dollar valuation as part of the evaluation or analysis.

Regulation How a law or mandate is implemented.
Risk The exposure or potential for loss or damage to IT assets within that IT infrastructure.
Risk Assessment A process for evaluating the exposure or potential loss or damage to the IT and data assets for an organization.
Risk Management The overall responsibility and management of risk within an organization. Risk management is the responsibility and dissemination of roles, responsibilities, and accountabilities for risk in an organization.
Threat Any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset.
Vulnerability A weakness in the IT infrastructure or IT components that may be exploited for a threat to destroy, damage, or compromise an IT asset.
Vulnerability Assessment A methodical evaluation of an organization's IT weaknesses of infrastructure components and assets and how those weaknesses can be mitigated through proper security controls and recommendations to remediate exposure to risks, threats, and vulnerabilities.
Vulnerability Management The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.