SECURITY PROGRAM AND POLICIES

PRINCIPLES AND PRACTICES

SARI STERN GREENE

Security Program and Policies: Principles and Practices

Second Edition

Sari Stern Greene

PEARSON
IT CERTIFICATION

800 East 96th Street, Indianapolis, Indiana 46240 USA

Security Program and Policies: Principles and Practices, Second Edition

Sari Stern Greene

ISBN-13: 978-0-7897-5167-6
ISBN-10: 0-7897-5167-4

Library of Congress Control Number: 2014932766

Printed in the United States of America

First Printing: March 2014

Editor-in-Chief
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Box Twelve, Inc.

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Bart Reed

Indexer
Heather McNeill

Proofreader
Anne Goebel

Technical Editors
Ronald Gonzales
Tatyana Zidarov

Publishing Coordinator
Vanessa Evans

Interior Designer
Gary Adair

Cover Designer
Mark Shirar

Compositor
Studio Galou, LLC

Contents at a Glance

Table of Contents

About the Author

Sari Stern Greene was at the forefront of the security battlefield when she founded Sage Data Security in 2002. Sage's award-winning portfolio of advisory, assessment, and assurance security services are designed to protect an organization's information assets and ensure regulatory compliance. An entrenched security practitioner, Sari has amassed thousands of hours in the field working with a spectrum of technical, operational, and management personnel, as well as boards of directors, regulators, and service providers.

Sari provided expert witness testimony in the groundbreaking PATCO v. Ocean National Bank case. From 2006 through 2010, she served as the managing director for the MEAPC, a coalition of 24 financial institutions that embrace a mission of preventing information theft and fraud through public education and awareness. Since 2010, she has served as the chair of the annual Cybercrime Symposium held in Portsmouth, New Hampshire.

A recognized leader in the field of information security, Sari's first book was *Tools and Techniques for Securing Microsoft Networks*, soon followed by the first edition of *Security Policies and Procedures: Principles and Practices*. She has published a number of articles related to information security and has been quoted in *The New York Times*, *Wall Street Journal*, CNN, and on CNBC. She speaks regularly at security conferences and workshops around the country and is a frequent guest lecturer.

Sari has an MBA from the University of New Hampshire system and has earned an array of government and industry certifications and accreditations, including ISACA Certification in Risk and Information Systems Control (CRISC), ISACA Certification in Security Management (CISM), ISC^2 Certification in Information Systems Security (CISSP), and Microsoft Certified Network Engineer (MCSE), and is certified by the National Security Agency to conduct NSA-IAM assessments for federal government agencies and contractors.

You can contact Sari at sari@sarigreene.com or follow her on Twitter @sari_greene.

Dedication

To all who honor the public trust.

Acknowledgments

Transforming raw material into a useful publication is a team effort. My colleagues at Sage Data Security generously and passionately shared their knowledge. Dr. Ron Gonzales of National University and Tatyana Zidarov of Kaplan University provided thoughtful feedback and recommendations. Senior Development Editor Chris Cleveland and Development Editor Jeff Riley expertly guided the process. The Fadiman family made available a wonderful workspace. The Captain, as always, waited patiently. To all, I am grateful.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

Chapter 4

Governance and Risk Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain the importance of strategic alignment.
- Know how to manage information security policies.
- Describe information security–related roles and responsibilities.
- Identify the components of risk management.
- Create polices related to information security policy, governance, and risk management.

Information Security Policies (ISO 27002:2013 Section 5) and Organization of Information Security (ISO 27002:2013 Section 6) are closely related, so we address both domains in this chapter. The Information Security Policies domain focuses on information security policy requirements and the need to align policy with organizational objectives. The Organization of Information Security domain focuses on the governance structure necessary to implement and manage information security policy operations, across and outside of the organization. Included in this chapter is a discussion of risk management because it is a fundamental aspect of governance, decision making, and policy. Risk management is important enough that it warrants two sets of standards: ISO/IEC 27005 and ISO/IEC 31000.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 5 of ISO 27002:2013 is titled "Information Security Policies." This domain addresses policy development and authorization. Section 6 of ISO 27002:2013 is titled "Organization of Information Security." This domain addresses information security governance as well as enterprise roles and responsibilities. Risk management principles, risk assessment techniques, and information security risk management systems are described in ISO 27005:2005 and the ISO 31000 series.

Corresponding NIST guidance is provided in the following documents:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-30: Risk Management Guide for Information Technology Systems
- SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- SP 800-100: Information Security Handbook: A Guide for Managers

Understanding Information Security Policies

Information security policies, standards, procedures, and plans exist for one reason—to protect the organization and, by extension, its constituents from harm. The lesson of the Information Security Policies domain is threefold:

- Information security directives should be codified in a written policy document.
- It is important that management participate in policy development and visibly support the policy.
- The necessity of strategically aligning information security with business requirements and relevant laws and regulations.

Internationally recognized standard security standards such as the ISO 27002:2013 can provide a framework, but ultimately each organization must construct its own security strategy and policy taking into consideration organizational objectives and regulatory requirements.

What Is Meant by Strategic Alignment?

The two approaches to information security are parallel and integrated. A ***parallel approach*** silos information security, assigns responsibility for *being secure* to the IT department, views compliance as discretionary, and has little or no organizational accountability. An ***integrated approach*** recognizes that security and success are intertwined. When strategically aligned, security functions as a business enabler that adds value. Security is an expected topic of discussion among decision makers and is given the same level of respect as other fundamental drivers and influencing elements of the business. This doesn't happen magically. It requires leadership that recognizes the value of information security, invests in people and processes, encourages discussion and debate, and treats security in the same fashion as every other business requirement. It also requires that information security professionals recognize that the true value of information security is protecting the business from harm and achieving organizational objectives. Visible management support coupled with written policy formalizes and communicates the organizational commitment to information security.

Regulatory Requirements

In an effort to protect the citizens of the United States, legislators recognized the importance of written information security policies. Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Family Educational Rights and Privacy Act (FERPA), and the Federal Information Systems Management Act (FISMA) all require covered entities to have in place written policies and procedures that protect their information assets. They also require the policies to be reviewed on a regular basis. Each of these legislative acts better secured each person's private information and the governance to reduce fraudulent reporting of corporate earnings.

Many organizations find that they are subject to more than one set of regulations. For example, publicly traded banks are subject to both GLBA and SOX requirements, whereas medical billing companies find themselves subject to both HIPAA and GLBA. Organizations that try to write their policies to match federal state regulations find the task daunting. Fortunately, the regulations published to date have enough in common that a well-written set of information security policies based on a framework such as the ISO 27002 can be mapped to multiple regulatory requirements. Policy administrative notations will often include a cross-reference to specific regulatory requirements.

User Versions of Information Security Policies

Information security policies are governance statements written with the intent of directing the organization. Correctly written, policies can also be used as teaching documents that influence behavior. An Acceptable Use Policy document and corresponding agreement should be developed specifically for distribution to the user community. The Acceptable Use Policy should include only pertinent information and, as appropriate, explanations and examples. The accompanying agreement requires users to acknowledge that they understand their responsibilities and affirm their individual commitment.

Vendor Versions of Information Security Policies

As we will discuss in Chapter 8, "Communications and Operations Security," companies can outsource work but not responsibility or liability. Vendors or business partners (often referred to as "third parties") that store, process, transmit, or access information assets should be required to have controls that meet or, in some cases, exceed organizational requirements. One of the most efficient ways to evaluate vendor security is to provide them with a vendor version of organizational security policies and require them to attest to their compliance. The vendor version should only contain policies that are applicable to third parties and should be sanitized as to not disclose any confidential information.

Client Synopsis of Information Security Policies

In this context, *client* refers to companies to which the organization provides services. A synopsis of the information security policy should be available upon request to clients. As applicable to the client base, the synopsis could be expanded to incorporate incident response and business continuity procedures, notifications, and regulatory cross-references. The synopsis should not disclose confidential business information unless the recipients are required to sign a non-disclosure agreement.

In Practice

Information Security Policy

Synopsis: The organization is required to have a written information security policy and supporting documents.

Policy Statement:

- The company must have written information security policies.
- Executive management is responsible for establishing the mandate and general objectives of the information security policy.
- The policies must support organizational objectives.
- The policies must comply with relevant statutory, regulatory, and contractual requirements.
- The policies must be communicated to all relevant parties both within and external to the company.
- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- For the purpose of educating the workforce, user-level documents will be derived from the information security policy including but not limited to Acceptable Use Policy, Acceptable Use Agreement, and Information Handling Instructions.
- Any information security policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.

FYI: Policy Hierarchy Refresher

- ***Guiding principles*** are the fundamental philosophy or beliefs of an organization and reflect the kind of company an organization seeks to be. The policy hierarchy represents the implementation of guiding principles.
- ***Policies*** are directives that codify organizational requirements.
- ***Standards*** are implementation specifications.
- ***Baselines*** are an aggregate of minimum implementation standards and security controls for a specific category or grouping.
- ***Guidelines*** are suggested actions or recommendations.
- ***Procedures*** are instructions.
- ***Plans*** are strategic and tactical guidance used to execute an initiative or respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.

Who Authorizes Information Security Policy?

A policy is a reflection of the organization's commitment, direction, and approach. Information security policies should be authorized by executive management. Depending on the size, legal structure, and/or regulatory requirements of the organization, executive management may be defined as owners, directors, or executive officers.

Because executive management is responsible for and can be held legally liable for the protection of information assets, it is incumbent upon those in leadership positions to remain invested in the proper execution of the policy as well as the activities of oversight that ensure it. The National Association of Corporate Directors (NACD), the leading membership organization for Boards and Directors in the U.S., recommends four essential practices:

- Place information security on the Board's agenda.
- Identify information security leaders, hold them accountable, and ensure support for them.
- Ensure the effectiveness of the corporation's information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee.

Policies should be reviewed at planned intervals to ensure their continuing suitability, adequacy, and effectiveness.

FYI: Director's Liability and Duty of Care

In tort law, duty of care is a legal standard applied to directors and officers of a corporation. In 1996, the shareholders of Caremark International, Inc., brought a derivative action, alleging that the Board of Directors breached their duty of care by failing to put in place adequate internal control systems. In response, the Delaware court defined a multifactor test designed to determine when duty of care is breached:

- The directors knew or should have known that violations of the law were occurring, and
- The directors took no steps in a good faith effort to prevent or remedy the situation, and
- Such failure proximately resulted in the losses complained of.

According to the firm of Orrick, Herrington and Sutcliffe, LLP, "in short, as long as a director acts in good faith, as long as she exercises proper due care and does not exhibit gross negligence, she cannot be held liable for failing to anticipate or prevent a cyber attack. However, if a plaintiff can show that a director failed to act in the face of a known duty to act, thereby demonstrating a conscious disregard for [her] responsibilities, it could give rise to a claim for breach of fiduciary duty."

Revising Information Security Policies: Change Drivers

Because organizations change over time, policies need to be revisited. ***Change drivers*** are events that modify how a company does business. Change drivers can be demographic, economic, technological, and regulatory or personnel related. Examples of change drivers include company acquisition, new products, services or technology, regulatory updates, entering into a contractual obligation, and entering a new market. Change can introduce new vulnerabilities and risks. Change drivers should trigger internal assessments and ultimately a review of policies. Policies should be updated accordingly and subject to reauthorization.

Evaluating Information Security Polices

Directors and executive management have a fiduciary obligation to manage the company in a responsible manner. It is important that they be able to accurately gauge adherence to policy directives, the effectiveness of information security policies, and the maturity of the information security program. Standardized methodologies such as audits and maturity models can be used as evaluation and reporting mechanisms. Organizations may choose to conduct these evaluations using in-house personnel or engage independent third parties. The decision criteria include the size and complexity of the organization, regulatory requirements, available expertise, and segregation of duties. To be considered ***independent***, assessors should not be responsible for, benefit from, or have in any way influenced the design, installation, maintenance, and operation of the target, or the policies and procedures that guide its operation.

Audit

An ***information security audit*** is a systematic, evidence-based evaluation of how well the organization conforms to established criteria such as Board-approved policies, regulatory requirements, and internationally recognized standards such as the ISO 27000 series. Audit procedures include interviews, observation, tracing documents to management policies, review of practices, review of documents, and tracing data to source documents. An ***audit report*** is a formal opinion (or disclaimer) of the audit team based on predefined scope and criteria. Audit reports generally include a description of the work performed, any inherent limitations of the work, detailed findings, and recommendations.

FYI: Certified Information Security Auditor (CISA)

The CISA certification is granted by ISACA (previously known as the Information Systems Audit and Control Association) to professionals who have demonstrated a high degree of audit-related knowledge and have verifiable work experience. The CISA certification is well respected across the globe, and the credibility of its continuing professional education (CPE) program ensures that CISA-certified professionals maintain their skill set. The American National Standards Institute (ANSI) accredited the CISA certification program under ISO/IEC 17024:2003: General Requirements for Bodies Operating Certification Systems of Persons. For more information about ISACA certification, visit www.isaca.org.

Capability Maturity Model (CMM)

A ***capability maturity model (CMM)*** is used to evaluate and document process maturity for a given area. The term *maturity* relates to the degree of formality and structure, ranging from ad hoc to optimized processes. Funded by the United States Air Force, the CMM was developed in the mid-1980s at the Carnegie Mellon University Software Engineering Institute. The objective was to create a model for the military to use to evaluate software development. It has since been adopted for subjects as diverse as information security, software engineering, systems engineering, project management, risk management, system acquisition, information technology (IT) services, and personnel management. It is sometimes combined with other methodologies such as ISO 9001, Six Sigma, Extreme Programming (XP), and DMAIC.

As documented in Table 4.1, a variation of the CMM can be used to evaluate enterprise information security maturity. Contributors to the application of the model should possess intimate knowledge of the organization and expertise in the subject area.

TABLE 4.1 Capability Maturity Model (CMM) Scale

Level	State	Description
0	Nonexistent	The organization is unaware of the need for policies or processes.
1	Ad-hoc	There are no documented policies or processes; there is sporadic activity.
2	Repeatable	Policies and processes are not fully documented; however, the activities occur on a regular basis.
3	Defined process	Policies and processes are documented and standardized; there is an active commitment to implementation.
4	Managed	Policies and processes are well defined, implemented, measured, and tested.
5	Optimized	Policies and process are well understood and have been fully integrated into the organizational culture.

As Figure 4.1 illustrates, the result is easily expressed in a graphic format and succinctly conveys the state of the information security program on a per-domain basis. The challenge with any scale-based model is that sometimes the assessment falls in between levels, in which case it is perfectly appropriate to use gradations (such as 3.5). This is an effective mechanism for reporting to those responsible for oversight, such as the Board of Directors or executive management. Process improvement objectives are a natural outcome of a CMM assessment.

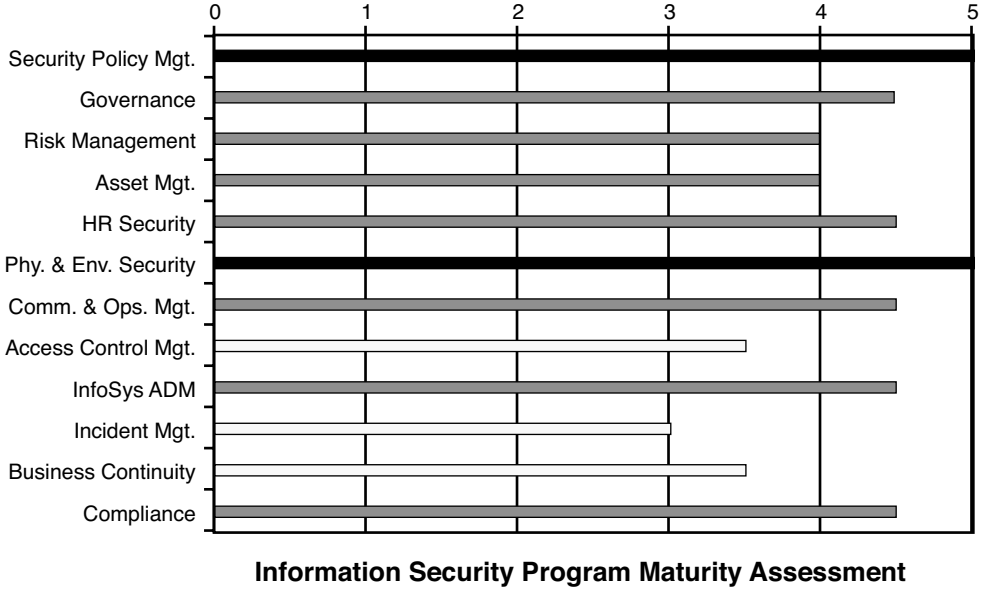

FIGURE 4.1 Capability maturity model (CMM) assessment.

In Practice

Information Security Policy Authorization and Oversight Policy

Synopsis: Information security policies must be authorized by the Board of Directors. The relevancy and the effectiveness of the policy must be reviewed annually.

Policy Statement:

- The Board of Directors must authorize the information security policy.
- An annual review of the information security policy must be conducted.
- The Chief Information Security Officer (CISO) is responsible for managing the review process.
- Changes to the policy must be presented to and approved by a majority of the Board of Directors.
- The Chief Operating Officer (COO) and the CISO will jointly present an annual report to the Board of Directors that provides them the information necessary to measure the organizations' adherence to the information security policy objectives and the maturity of the information security program.
- When in-house knowledge is not sufficient to review or audit aspects of the information security policy, or if circumstances dictate independence, third-party professionals must be engaged.

Information Security Governance

Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The ISO 27002:2013 Organization of Information Security domain objective is "to establish a management framework to initiate and control the implementation and operation of information security within the organization." This domain requires organizations to decide who is responsible for security management, the scope of their authority, and how and when it is appropriate to engage outside expertise. Julie Allen, in her seminal work "Governing for Enterprise Security," passionately articulated the importance of governance as applied to information security:

"Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance."

The Board of Directors (or organizational equivalent) is generally the authoritative policy-making body and responsible for overseeing the development, implementation, and maintenance of the information security program. The use of the term "oversee" is meant to convey the Board's conventional supervisory role, leaving day-to-day responsibilities to management. Executive management should be tasked with providing support and resources for proper program development, administration, and maintenance as well as ensuring strategic alignment with organizational objectives.

What Is a Distributed Governance Model?

It is time to bury the myth that "security is an IT issue." Security is not an isolated discipline and should not be siloed. Designing and maintaining a secure environment that supports the mission of the organization requires enterprise-wide input, decision making, and commitment. The foundation of a distributed governance model is the principle that stewardship is an organizational responsibility. Effective security requires the active involvement, cooperation, and collaboration of stakeholders, decision makers, and the user community. Security should be given the same level of respect as other fundamental drivers and influencing elements of the business.

Chief Information Security Officer (CISO)

Even in the most security-conscious organization, someone still needs to provide expert leadership. That is the role of the CISO. As a member of the executive team, the CISO is positioned to be a leader, teacher, and security champion. The CISO coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups. The most successful CISOs successfully balance security, productivity, and innovation. The CISO must be an advocate for security as a business enabler while being mindful of the need to protect the organizational from unrecognized harm. They must be willing to not be the most popular person in the room. This position generally reports directly to a senior functional executive (CEO, COO, CFO, General Counsel) and should have an unfiltered communication channel to the Board of Directors.

In smaller organizations, this function is often vested in the non-executive-level position of Information Security Officer (ISO). A source of conflict in many companies is whom the ISO should report to and if they should be a member of the IT team. It is not uncommon or completely out of the question for the position to report to the CIO. However, this chain of command can raise questions concerning adequate levels of independence. To ensure appropriate segregation of duties, the ISO should report directly to the Board or to a senior officer with sufficient independence to perform their assigned tasks. Security officers should not be assigned operational responsibilities within the IT department. They should have sufficient knowledge, background, and training, as well as a level of authority that enables them to adequately and effectively perform their assigned tasks. Security decision making should not be a singular task. Supporting the CISO or ISO should be a multidisciplinary committee that represents functional and business units.

In Practice

CISO Policy

Synopsis: To define the role of the CISO as well as the reporting structure and lines of communication.

Policy Statement:

- The COO will appoint the CISO.
- The CISO will report directly to the COO.
- At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
- The CISO is responsible for managing the information security program, ensuring compliance with applicable regulations and contractual obligations, and working with business units to align information security requirements and business initiatives.
- The CISO will function as an internal consulting resource on information security issues.
- The CISO will chair the Information Security Steering Committee.
- The CISO will be a standing member of the Incident Response Team and the Continuity of Operations Team.
- Quarterly, the CISO will report to the executive management team on the overall status of the information security program. The report should discuss material matters, including such issues as risk assessment, risk management, control decisions, service provider arrangements, results of testing, security breaches or violations, and recommendations for policy changes.

Information Security Steering Committee

Creating a culture of security requires positive influences at multiple levels within an organization. Having an Information Security Steering Committee provides a forum to communicate, discuss, and debate on security requirements and business integration. Typically, members represent a cross-section of business lines or departments, including operations, risk, compliance, marketing, audit, sales, HR, and legal. In addition to providing advice and counsel, their mission is to spread the gospel of security to their colleagues, coworkers, subordinates, and business partners.

In Practice

Information Security Steering Committee Policy

Synopsis: The Information Security Steering Committee (ISC) is tasked with supporting the information security program.

Policy Statement:

- The Information Security Steering Committee serves in an advisory capacity in regards to the implementation, support, and management of the information security program, alignment with business objectives, and compliance with all applicable state and federal laws and regulations.
- The Information Security Steering Committee provides an open forum to discuss business initiatives and security requirements. Security is expected to be given the same level of respect as other fundamental drivers and influencing elements of the business.
- Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives. Adjunct committee members may include but are not limited to representatives of HR, training, and marketing.
- The Information Security Steering Committee will meet on a monthly basis.

Organizational Roles and Responsibilities

In addition to the CISO and the Information Security Steering Committee, distributed throughout the organization are a variety of roles that have information security–related responsibilities. For example:

- **Compliance Officer**—Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.
- **Privacy Officer**—Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
- **Internal audit**—Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
- **Incident response team**—Responsible for responding to and managing security-related incidents.
- **Data owners**—Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards.

- **Data custodians**—Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.
- **Data users**—Are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.

Each of these responsibilities should be documented in policies, job descriptions, or employee manuals.

Regulatory Requirements

The necessity of formally assigning information security–related roles and responsibilities cannot be overstated. The requirement has been codified in numerous standards, regulations, and contractual obligations—most notably:

- **Gramm-Leach-Bliley (GLBA) Section 314.4**: "In order to develop, implement, and maintain your information security program, you shall (a) Designate an employee or employees to coordinate your information security program."
- **HIPAA/HITECH Security Rule Section 164.308(a)**: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."
- **Payment Card Industry Data Security Standard (PCI DDS) Section 12.5**: "Assign to an individual or team the following information security management responsibilities: establish, document, and distribute security policies and procedures; monitor and analyze security alerts and information, and distribute to appropriate personnel; establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; administer user accounts, including additions, deletions, and modifications; monitor and control all access to data."
- **201 CMR 17: Standards for the Protection of Personal Information of the Residents of the Commonwealth – Section 17.0.2:** "Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to: (a) Designating one or more employees to maintain the comprehensive information security program."

Creating a culture of security requires positive influences at multiple levels within an organization. Security champions reinforce by example the message that security policies and practices are important to the organization. The regulatory requirement to assign security responsibilities is a de facto mandate to create security champions.

Information Security Risk

Three factors influence information security decision making and policy development:

- Guiding principles
- Regulatory requirements
- Risks related to achieving their business objectives.

Risk is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction. The motivation for "taking a risk" is a favorable outcome. "Managing risk" implies that other actions are being taken to either mitigate the impact of the undesirable or unfavorable outcome and/or enhance the likelihood of a positive outcome.

For example, a venture capitalist (VC) decides to invest a million dollars in a startup company. The risk (undesirable outcome) in this case is that the company will fail and the VC will lose part or all of her investment. The motivation for taking this risk is that the company becomes wildly successful and the initial backers make a great deal of money. To influence the outcome, the VC may require a seat on the Board of Directors, demand frequent financial reports, and mentor the leadership team. Doing these things, however, does not guarantee success. ***Risk tolerance*** is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit—in this case, how much money the VC is willing to lose. Certainly, if the VC believed that the company was destined for failure, the investment would not be made. Conversely, if the VC determined that the likelihood of a three-million-dollar return on investment was high, she may be willing to accept the tradeoff of a potential $200,000 loss.

Is Risk Bad?

Inherently, risk is neither good nor bad. All human activity carries some risk, although the amount varies greatly. Consider this: Every time you get in a car you are risking injury or even death. You manage the risk by keeping your car in good working order, wearing a seat beat, obeying the rules of the road, not texting, not being impaired, and paying attention. Your risk tolerance is that the reward for reaching your destination outweighs the potential harm.

Risk taking can be beneficial and is often necessary for advancement. For example, entrepreneurial risk taking can pay off in innovation and progress. Ceasing to take risks would quickly wipe out experimentation, innovation, challenge, excitement, and motivation. Risk taking can, however, be detrimental when ill considered or motivated by ignorance, ideology, dysfunction, greed, or revenge. The key is to balance risk against rewards by making informed decisions and then managing the risk commensurate with organizational objectives. The process of managing risk requires organizations to assign risk-management responsibilities, establish the organizational risk appetite and tolerance, adopt a standard methodology for assessing risk, respond to risk levels, and monitor risk on an ongoing basis.

Risk Appetite and Tolerance

Risk appetite is a strategic construct and broadly defined as the amount of risk an entity is willing to accept in pursuit of its mission. Risk tolerance is tactical and specific to the target being evaluated. Risk tolerance levels can be qualitative (for example, low, elevated, severe) or quantitative (for example, dollar loss, number of customers impacted, hours of downtime). It is the responsibility of the Board of Directors and executive management to establish risk tolerance criteria, set standards for acceptable levels of risk, and disseminate this information to decision makers throughout the organization.

In Practice

Information Security Risk Management Oversight Policy

Synopsis: To assign organizational roles and responsibilities with respect to risk management activities.

Policy Statement:

- Executive management, in consultation with the Board of Directors, is responsible for determining the organizational risk appetite and risk tolerance levels.
- Executive management will communicate the above to decision makers throughout the company.
- The CISO, in consultation with the Chief Risk Officer, is responsible for determining the information security risk assessment schedule, managing the risk assessment process, certifying results, jointly preparing risk reduction recommendations with business process owners, and presenting the results to executive management.
- The Board of Directors will be apprised by the COO of risks that endanger the organization, stakeholders, employees, or customers.

What Is a Risk Assessment?

An objective of a risk assessment is to evaluate what could go wrong, the likelihood of such an event occurring, and the harm if it did. In information security, this objective is generally expressed as the process of (a) identifying the *inherent risk* based on relevant *threats*, *threat sources*, and related *vulnerabilities*; (b) determining the *impact* if the threat source was successful; and (c) calculating the *likelihood of occurrence*, taking into consideration the *control* environment in order to determine *residual* risk.

- ***Inherent risk*** is the level of risk before security measures are applied.
- A ***threat*** is a natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact. Information security focuses on the threats to confidentiality (unauthorized use or disclosure), integrity (unauthorized or accidental modification), and availability (damage or destruction).

- A ***threat source*** is either (1) intent and method targeted at the intentional exploitation of a vulnerability, such as criminal groups, terrorists, bot-net operators, and disgruntled employees, or (2) a situation and method that may accidentally trigger a vulnerability such as an undocumented process, severe storm, and accidental or unintentional behavior.
- A ***vulnerability*** is a weakness that could be exploited by a threat source. Vulnerabilities can be physical (for example, unlocked door, insufficient fire suppression), natural (for example, facility located in a flood zone or in a hurricane belt), technical (for example, misconfigured systems, poorly written code), or human (for example, untrained or distracted employee).
- ***Impact*** is the magnitude of harm.
- The ***likelihood of occurrence*** is a weighted factor or probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
- A ***control*** is a security measure designed to prevent, deter, detect, or respond to a threat source.
- ***Residual risk*** is the level of risk after security measures are applied. In its most simple form, residual risk can be defined as the likelihood of occurrence after controls are applied, multiplied by the expected loss. Residual risk is a reflection of the actual state. As such, the risk level can run the gamut from severe to nonexistent.

Let's consider the *threat* of obtaining unauthorized access to protected customer data. A *threat source* could be a cybercriminal. The *vulnerability* is that the information system that stores the data is Internet facing. We can safely assume that if no security measures were in place, the criminal would have unfettered access to the data (*inherent risk*). The resulting harm (*impact*) would be reputational damage, cost of responding to the breach, potential lost future revenue, and perhaps regulatory penalties. The security measures in place include data access controls, data encryption, ingress and egress filtering, an intrusion detection system, real-time activity monitoring, and log review. The *residual risk* calculation is based on the likelihood that the criminal (*threat source*) would be able to successfully penetrate the security measures, and if so what the resulting harm would be. In this example, because the stolen or accessed data are encrypted, one could assume that the residual risk would be low (unless, of course, they were also able to access the decryption key). However, depending on the type of business, there still might be an elevated reputation risk associated with a breach.

FYI: Business Risk Categories

In a business context, risk is further classified by category, including strategic, financial, operational, personnel, reputational, and regulatory/compliance risk:

- ***Strategic*** risk relates to adverse business decisions.
- ***Financial*** (or investment) risk relates to monetary loss.
- ***Reputational*** risk relates to negative public opinion.

- ***Operational*** risk relates to loss resulting from inadequate or failed processes or systems.
- ***Personnel*** risk relates to issues that affect morale, productivity, recruiting, and retention.
- ***Regulatory/compliance*** risk relates to violations of laws, rules, regulations, or policy.

Risk Assessment Methodologies

Components of a risk assessment methodology include a defined process, a risk model, an assessment approach, and standardized analysis. The benefit of consistently applying a risk assessment methodology is comparable and repeatable results. The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF). The NIST Risk Management Framework includes both risk assessment and risk management guidance.

NIST Risk Assessment Methodology

Federal regulators and examiners often refer to NIST SP 800-30 and SP 800-39 in their commentary and guidance. The NIST Risk Assessment methodology, as defined in SP 800-30: Guide to Conducting Risk Assessments, is divided into four steps: Prepare for the assessment, conduct the assessment, communicate the results, and maintain the assessment. It is unrealistic that a single methodology would be able to meet the diverse needs of private and public sector organizations. The expectation set forth in NIST SP 800-39 and 800-30 is that each organization will adapt and customize the methodology based on size, complexity, industry sector, regulatory requirements, and threat vector.

In Practice

Information Security Risk Assessment Policy

Synopsis: To assign responsibility for and set parameters for conducting information security risk assessments.

Policy Statement:

- The company must adopt an information security risk assessment methodology to ensure consistent, repeatable, and comparable results.
- Information security risk assessments must have a clearly defined and limited scope. Assessments with a broad scope become difficult and unwieldy in both their execution and the documentation of the results.
- The CISO is charged with developing an information security risk assessment schedule based on the information system's criticality and information classification level.

- In addition to scheduled assessments, information security risk assessments must be conducted prior to the implementation of any significant change in technology, process, or third-party agreement.
- The CISO and the business process owner are jointly required to respond to risk assessment results and develop risk reduction strategies and recommendations.
- Risk assessment results and recommendations must be presented to executive management.

What Is Risk Management?

Risk management is the process of determining an acceptable level of risk (risk appetite and tolerance), calculating the current level of risk (risk assessment), accepting the level of risk (risk acceptance), or taking steps to reduce risk to the acceptable level (risk mitigation). We discussed the first two components in the previous sections.

Risk Acceptance

Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Generally, but not always, this means that the outcome of the risk assessment is within tolerance. There may be times when the risk level is not within tolerance but the organization will still choose to accept the risk because all other alternatives are unacceptable. Exceptions should always be brought to the attention of management and authorized by either the executive management or the Board of Directors.

Risk Mitigation

Risk mitigation implies one of four actions—reducing the risk by implementing one or more countermeasures (risk reduction), sharing the risk with another entity (risk sharing), transferring the risk to another entity (risk transference), modifying or ceasing the risk-causing activity (risk avoidance), or a combination thereof.

Risk mitigation is a process of reducing, sharing, transferring, or avoiding risk. ***Risk reduction*** is accomplished by implementing one or more offensive or defensive controls in order to lower the residual risk. An ***offensive control*** is designed to reduce or eliminate vulnerability, such as enhanced training or applying a security patch. A ***defensive control*** is designed to respond to a threat source (for example, a sensor that sends an alert if an intruder is detected). Prior to implementation, risk reduction recommendations should be evaluated in terms of their effectiveness, resource requirements, complexity impact on productivity and performance, potential unintended consequences, and cost. Depending on the situation, risk reduction decisions may be made at the business unit level, by management or by the Board of Directors.

Risk transfer or risk sharing is undertaken when organizations desire and have the means to shift risk liability and responsibility to other organizations. ***Risk transfer*** shifts the entire risk responsibility or liability from one organization to another organization. This is often accomplished by purchasing insurance. ***Risk sharing*** shifts a portion of risk responsibility or liability to other organizations. The caveat to this option is that regulations such as GLBA (financial institutions) and HIPAA/HITECH (healthcare organizations) prohibit covered entities from shifting compliance liability.

Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk appetite and tolerance, and a determination has been made not to make an exception. ***Risk avoidance*** involves taking specific actions to eliminate or significantly modify the process or activities that are the basis for the risk. It is unusual to see this strategy applied to critical systems and processes because both prior investment and opportunity costs need to be considered. However, this strategy may be very appropriate when evaluating new processes, products, services, activities, and relationships.

In Practice

Information Security Risk Response Policy

Synopsis: To define information security risk response requirements and authority.

Policy Statement:

- The initial results of all risk assessments must be provided to executive management and business process owner within seven days of completion.
- Low risks can be accepted by business process owners.
- Elevated risks and severe risks (or comparable rating) must be responded to within 30 days. Response is the joint responsibility of the business process owner and the CISO. Risk reduction recommendations can include risk acceptance, risk mitigation, risk transfer, risk avoidance, or a combination thereof. Recommendations must be documented and include an applicable level of detail.
- Severe and elevated risks can be accepted by executive management.
- The Board of Directors must be informed of accepted severe risk. At their discretion, they can choose to overrule acceptance.

FYI: Cyber Insurance

Two general categories of risks and potential liabilities are covered by cyber-insurance: first-party risks and third-party risks:

- ***First-party risks*** are potential costs for loss or damage to the policyholder's own data, or lost income or business.
- ***Third-party risks*** include the policyholder's potential liability to clients or to various governmental or regulatory entities.
- A company's optimal cyber-security policy would contain coverage for both first- and third-party claims. A 2013 Ponemon Institute Study commissioned by Experian Data Breach Resolution found that of 683 surveys completed by risk management professionals across multiple business sectors that have considered or adopted cyber-insurance, 86% of policies covered notification costs, 73% covered legal defense costs, 64% covered forensics and investigative costs, and 48% covered replacement of lost or damaged equipment. Not everything was always covered, though, as companies said only 30% of policies covered third-party liability, 30% covered communications costs to regulators, and 8% covered brand damages.

FYI: Small Business Note

Policy, governance, and risk management are important regardless of the size of the organization. The challenge for small organizations is who is going to accomplish these tasks. A small (or even a mid-size) business may not have a Board of Directors, C-level officers, or directors. Instead, as illustrated in Table 4.2, tasks are assigned to owners, managers, and outsourced service providers. What does not change regardless of size is the responsibilities of data owners, data custodians, and data users.

TABLE 4.2 Organizational Roles and Responsibilities

Role	Small Business Equivalent
Board of Directors	Owner(s).
Executive management	Owner(s) and/or management.
Chief Security Officer	A member of the management team whose responsibilities include information security. If internal expertise does not exist, external advisors should be engaged.
Chief Risk Officer	A member of the management team whose responsibilities include evaluating risk. If internal expertise does not exist, external advisors should be engaged.
Compliance Officer	A member of the management team whose responsibilities include ensuring compliance with applicable laws and regulations. If internal expertise does not exist, external advisors should be engaged.
Director of IT	IT manager. If internal expertise does not exist, external service providers should be engaged.
Internal audit	If this position is required, it is generally outsourced.

Summary

Information security is not an end unto itself. Information security is a business discipline that exists to support business objectives, add value, and maintain compliance with externally imposed requirements. This type of relationship is known as *strategic alignment*. Organizational commitment to information security practices should be codified in a written policy. The information security policy is an authoritative document that informs decision making and practices. As such, it should be authorized by the Board of Directors or equivalent body. Derivative documents for specific audiences should be published and distributed. This includes an Acceptable Use Policy and Agreement for users, a third-party version for vendors and service providers, and a synopsis for business partners and clients.

It is essential that information security policies remain relevant and accurate. At a minimum, policies should be reviewed and reauthorized annually. Change drivers are events that modify how a company operates and are a trigger for policy review. Compliance with policy requirements should be assessed and reported to executive management.

An *information security audit* is a systematic evidence-based evaluation of how well the organization conforms to established criteria. Audits are generally conducted by independent auditors, which implies that the auditor is not responsible for, benefited from, or in any way influenced by the audit target. A *capability maturity model (CMM) assessment* is an evaluation of process maturity for a given area. In contrast to an audit, the application of a CMM is generally an internal process. Audits and maturity models are good indicators of policy acceptance and integration.

Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The Board of Directors is the authoritative policy making body. Executive management is tasked with providing support and resources. Endorsed by the Board of Directors and executive management, the CISO (or equivalent role) is vested with information security program management responsibility and accountability. The chain of command for the CISO should be devoid of conflict of interest. The CISO should have the authority to communicate directly with the Board of Directors.

Discussion, debate, and thoughtful deliberation result in good decision making. Supporting the CISO should be an Information Security Steering Committee, whose members represent a cross-section of the organization. The steering committee serves in an advisory capacity with particular focus on the alignment of business and security objectives. Distributed throughout the organization are a variety of roles that have information security–related responsibilities. Most notably, data owners are responsible for defining protection requirements, data custodians are responsible for managing the protection mechanisms, and data users are expected to act in accordance with the organization's requirements and to be stewards of the information in their care.

Three factors influence information security decision making and policy development: guiding principles, regulatory requirements, and risks related to achieving their business objectives. *Risk* is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or

inaction. *Risk tolerance* is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit. *Risk management* is the process of determining an acceptable level of risk, identifying the level of risk for a given situation, and determining if the risk should be accepted or mitigated. A *risk assessment* is used to calculate the level of risk. A number of publically available risk assessment methodologies are available for organizations to use and customize. Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Risk mitigation implies that one of four actions (or a combination of actions) will be undertaken: risk reduction, risk sharing, risk transference, or risk avoidance.

Risk management, governance, and information policy are the basis of an information program. Policies related to these domains include the following policies: Information Security Policy, Information Security Policy Authorization and Oversight, CISO, Information Security Steering Committee, Information Security Risk Management Oversight, Information Security Risk Assessment, and Information Security Risk Management.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. When an information security program is said to be "strategically aligned," this indicates that _____.

   A. It supports business objectives
   B. It adds value
   C. It maintains compliance with regulatory requirements
   D. All of the above

2. How often should information security policies be reviewed?

   A. Once a year
   B. Only when a change needs to be made
   C. At a minimum, once a year and whenever there is a change trigger
   D. Only as required by law

3. Information security policies should be authorized by _____.

   A. the Board of Directors (or equivalent)
   B. business unit managers
   C. legal counsel
   D. stockholders

4. Which of the following statements best describes policies?

   A. Policies are the implementation of specifications.
   B. Policies are suggested actions or recommendations.
   C. Policies are instructions.
   D. Policies are the directives that codify organizational requirements.

5. Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive information security policy?

   A. Sections of the comprehensive policy may not be applicable to all employees.
   B. The comprehensive policy may include unknown acronyms.
   C. The comprehensive document may contain confidential information.
   D. The more understandable and relevant a policy is, the more likely users will positively respond to it.

6. Which of the following is a common element of all federal information security regulations?

   A. Covered entities must have a written information security policy.
   B. Covered entities must use federally mandated technology.
   C. Covered entities must self-report compliance.
   D. Covered entities must notify law enforcement if there is a policy violation.

7. Organizations that choose to adopt the ISO 27002:2103 framework must _____.

   A. use every policy, standard, and guideline recommended
   B. create policies for every security domain
   C. evaluate the applicability and customize as appropriate
   D. register with the ISO

8. Evidence-based techniques used by information security auditors include which of the following elements?

   A. Structured interviews, observation, financial analysis, and documentation sampling
   B. Structured interviews, observation, review of practices, and documentation sampling
   C. Structured interviews, customer service surveys, review of practices, and documentation sampling
   D. Casual conversations, observation, review of practices, and documentation sampling

9. Which of the following statements best describes independence in the context of auditing?

   A. The auditor is not an employee of the company.
   B. The auditor is certified to conduct audits.
   C. The auditor is not responsible for, benefited from, or in any way influenced by the audit target.
   D. Each auditor presents his or her own opinion.

10. Which of the following states is *not* included in a CMM?

   A. Average
   B. Optimized
   C. Ad hoc
   D. Managed

11. Which of the following activities is not considered a governance activity?

   A. Managing
   B. Influencing
   C. Evaluating
   D. Purchasing

12. To avoid conflict of interest, the CISO could report to which of the following individuals?

   A. The Chief Information Officer (CIO)
   B. The Chief Technology Officer (CTO)
   C. The Chief Financial Officer (CFO)
   D. The Chief Compliance Officer (CCO)

13. Which of the following statements best describes the role of the Information Security Steering Committee?

   A. The committee authorizes policy.
   B. The committee serves in an advisory capacity.
   C. The committee approves the InfoSec budget.
   D. None of the above.

14. Defining protection requirements is the responsibility of _____.

   A. the ISO
   B. the data custodian
   C. data owners
   D. the Compliance Officer

15. Designating an individual or team to coordinate or manage information security is required by _____.

    A. GLBA
    B. MA CMR 17 301
    C. PCI DSS
    D. All of the above

16. Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?

    A. Threat
    B. Risk
    C. Vulnerability
    D. Impact

17. Inherent risk is the state before _____.

    A. an assessment has been conducted
    B. security measures have been implemented
    C. the risk has been accepted
    D. None of the above

18. Which of the following terms best describes the natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

19. Which of the following terms best describes a disgruntled employee with intent to do harm?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

20. Which if the following activities is *not* considered an element of risk management?

    A. The process of determining an acceptable level of risk
    B. Assessing the current level of risk for a given situation
    C. Accepting the risk
    D. Installing risk-mitigation safeguards

21. How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as _____.

    A. risk acceptance
    B. risk tolerance
    C. risk mitigation
    D. risk avoidance

22. Which of the following statements best describes a vulnerability?

    A. A vulnerability is a weakness that could be exploited by a threat source.
    B. A vulnerability is a weakness that can never be fixed.
    C. A vulnerability is a weakness that can only be identified by testing.
    D. A vulnerability is a weakness that must be addressed regardless of the cost.

23. A control is a security measure that is designed to _____ a threat source.

    A. detect
    B. deter
    C. prevent
    D. All of the above

24. Which of the following is not a risk-mitigation action?

    A. Risk acceptance
    B. Risk sharing or transference
    C. Risk reduction
    D. Risk avoidance

25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?

    A. Inherent risk
    B. Expected risk
    C. Residual risk
    D. Accepted risk

26. Which of the following risk types best describes an example of insurance?

- **A.** Risk avoidance
- **B.** Risk transfer
- **C.** Risk acknowledgement
- **D.** Risk acceptance

27. Which of the following risk types relates to negative public opinion?

- **A.** Operational risk
- **B.** Financial risk
- **C.** Reputation risk
- **D.** Strategic risk

28. Compliance risk as it relates to federal and state regulations can never be _____.

- **A.** avoided
- **B.** transferred
- **C.** accepted
- **D.** None of the above

29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?

- **A.** They must have different policies for each regulation.
- **B.** They must have multiple ISOs.
- **C.** They must ensure that their information security program includes all applicable requirements.
- **D.** They must choose the one regulation that takes precedence.

30. Which of the following terms best describes "duty of care" as applied to corporate directors and executive officers?

- **A.** It's a legal obligation.
- **B.** It's an outdated requirement.
- **C.** It's ignored by most organizations.
- **D.** It's a factor only when there is a loss greater than $1,000.

EXERCISES

EXERCISE 4.1: Understanding ISO 27002:2005

The introduction to ISO 27002:2005 includes this statement: "This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required."

1. Explain how this statement relates to the concept of strategic alignment.
2. The risk assessment domain was included in the ISO 27002:2005 edition and then removed in ISO 27002:2013. Why do you think they made this change?
3. What are the major topics of ISO 27005?

EXERCISE 4.2: Understanding Policy Development and Authorization

Three entrepreneurs got together and created a website design hosting company. They will be creating websites and social media sites for their customers, from simple "Hello World" pages to full-fledged e-commerce solutions. One entrepreneur is the technical guru, the second is the marketing genius, and the third is in charge of finances. They are equal partners. The entrepreneurs also have five web developers working for them as independent contractors on a per-project basis. Customers are requesting a copy of their security policies.

1. Explain the criteria they should use to develop their policies. Who should authorize the policies?
2. Should the policies apply to the independent contractors? Why or why not?
3. What type of documentation should they provide their customers?

EXERCISE 4.3: Understanding Information Security Officers

1. ISOs are in high demand. Using online job hunting sites (such as Monster.com, Dice.com, and TheLadders.com), research available positions in your geographic area.
2. Is there a common theme in the job descriptions?
3. What type of certifications, education, and experience are employers seeking?

EXERCISE 4.4: Understanding Risk Terms and Definitions

1. Define each of the following terms: inherent risk, threat, threat source, vulnerability, likelihood, impact, and residual risk.
2. Provide examples of security measures designed to (a) deter a threat source, (b) prevent a threat source from being successful, and (c) detect a threat source.
3. Explain risk avoidance and why that option is generally not chosen.

EXERCISE 4.5: Understanding Insurance

1. What is cyber-insurance and what does it generally cover?
2. Why would an organization purchase cyber-insurance?
3. What is the difference between first-party coverage and third-party coverage?

PROJECTS

PROJECT 4.1: Analyzing a Written Policy

1. Many organizations rely on institutional knowledge rather than written policy. Why do you think all major information security regulations require a written information security policy? Do you agree? Explain your opinion.
2. We are going to test the conventional wisdom that policy should be documented conducting an experiment.
   a. Write down or print out these three simple policy statements. Or, if you would prefer, create your own policy statements.

      The Board of Directors must authorize the Information Security Policy.

      An annual review of the Information Security Policy must be conducted.

      The CISO is responsible for managing the review process.

   b. Enlist four subjects for your experiment.

      Give two of the subjects the written policy. Ask them to read document. Have them keep the paper.

      Read the policy to the two other subjects. Do not give them a written copy.

   c. Within 24 hours, contact each subject and ask them to recall as much of the policy as possible. If they ask, let the first two subjects know that they can consult the document you gave them. Document your findings. Does the outcome support your answer to Question 1?

PROJECT 4.2: Analyzing Information Security Management

1. Does your school or workplace have a CISO or an equivalent position? Who does the CISO (or equivalent) report to? Does he or she have any direct reports? Is this person viewed as a security champion? Is he or she accessible to the user community?
2. It is important that CISOs stay current with security best practices, regulations, and peer experiences. Research and recommend (at least three) networking and educational resources.
3. If you were tasked with selecting an Information Security Steering Committee at your school or workplace to advise the CISO (or equivalent), who would you choose and why?

PROJECT 4.3: Using Risk Assessment Methodologies

The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF).

1. Research and write a description of each (including pros and cons).
2. Are they in the public domain, or is there a licensing cost?
3. Is training available?

Case Study

Determining the Likelihood and Impact of Occurrence

One of the most challenging aspects of a risk assessment is determining the likelihood of occurrence and impact. NIST SP 800-30 defines the likelihood of occurrence as follows: A weighted risk factor based on an analysis of the probability that a given threat source is capable of exploiting a given vulnerability (or set of vulnerabilities). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. Organizations typically employ a three-step process to determine the overall likelihood of threat events:

- Organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events).
- Organizations assess the likelihood that the threat events, once initiated or occurring, will result in adverse impacts or harm to organizational operations and assets, individuals, other organizations, or the nation.
- Organizations assess the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact.

Identify two threat sources—one adversarial and one non-adversarial—that could exploit a vulnerability at your school or workplace and would result in disruption of service. An adversarial event is the *intentional* exploitation of a vulnerability by criminal groups, terrorists, bot-net operators, or disgruntled employees. A non-adversarial event is the *accidental* exploit of a vulnerability, such as an undocumented process, a severe storm, or accidental or unintentional behavior.

1. For each (using your best judgment), answer the following questions:

   a) What is the threat?

   b) What is the threat source?

   c) Is the source adversarial or non-adversarial?

d) What vulnerability could be exploited?

e) How likely is the threat source to be successful and why?

f) If the threat source is successful, what is the extent of the damage caused?

2. Risk assessments are rarely conducted by one individual working alone. If you were hosting a workshop to answer the preceding questions, who would you invite and why?

References

Regulations Cited

"Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards," accessed on 08/2013, www.fdic.gov/regulations/laws/rules/2000-8660.html.

"201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth," official website of the Office of Consumer Affairs & Business Regulation (OCABR), accessed on 05/06/2013, www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

"Family Educational Rights and Privacy Act (FERPA)," official website of the US Department of Education, accessed on 05/2013, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"HIPAA Security Rule," official website of the Department of Health and Human Services, accessed on 05/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Other References

Allen, Julia, "Governing for Enterprise Security: CMU/SEI-2005-TN-023 2005," Carnegie Mellon University, June 2005.

Bejtlich, Richard, "Risk, Threat, and Vulnerability 101," accessed on 10/2013, http://taosecurity.blogspot.com/2005/05/risk-threat-and-vulnerability-101-in.html.

"Capability Maturity Model," accessed on 10/2013, http://en.wikipedia.org/wiki/Capability_Maturity_Model.

DeMauro, John, "Filling the Information Security Officer Role within Community Banks," accessed on 10/2013, www.practicalsecuritysolutions.com/articles/.

"Duty of Care," Legal Information Institute, Cornell University Law School, accessed on 10/2013, www.law.cornell.edu/wex/duty_of_care.

Godes, Scott, Esq., and Kristi Singleton, Esq. "Top Ten Tips for Companies Buying Cyber Security Insurance Coverage," accessed on 10/2013, www.acc.com/legalresources/publications/topten/tttfcbcsic.cfm.

"Information Security Governance: Guidance for Boards of Directors and Executive Management, Second Edition," IT Governance Institute, 2006.

"In re Caremark International Inc. Derivative Litigation," accessed on 10/2013, http://en.wikipedia.org/wiki/In_re_Caremark_International_Inc._Derivative_Litigation.

Matthews, Chris, "Cybersecurity Insurance Picks Up Steam," *Wall Street Journal/Risk & Compliance Journal*, August 7, 2013, accessed on 10/2013, http://blogs.wsj.com/riskandcompliance/2013/08/07/cybersecurity-insurance-picks-up-steam-study-finds/.

"PCI DDS Requirements and Security Assessment Procedures, Version 2.0," PCI Security Standards Council LLC, October 2010.

"Process & Performance Improvement," Carnegie Mellon Software Engineering Institute, accessed on 10/2013, www.sei.cmu.edu/process/.

"Risk Management," accessed on 10/2013, http://en.wikipedia.org/wiki/Risk_management#Potential_risk_treatments.

Scott, Todd, Alex Talarides, and Jim Kramer. "Do directors face potential liability for not preventing cyber attacks?" June 24, 2013, accessed on 10/2013, www.lexology.com/library.

Swenson, David, Ph.D., "Change Drivers," accessed on 10/2013, http://faculty.css.edu/dswenson/web/Chandriv.htm.

"The Security Risk Management Guide," Microsoft, 2006.

"What Is the Capability Maturity Model (CMM)?" accessed on 10/2013, www.selectbs.com/process-maturity/what-is-the-capability-maturity-model.

Index

Symbols

A

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q – R

S

T

U

V

W

Y – Z