STUDENT GUIDE

FACULTY OF INFORMATION TECHNOLOGY

CYBER-SECURITY 700

RICHFIELD

Registered with the Department of Higher Education as a Private Higher Education Institution under the Higher Education Act, 1997.
Registration Certificate No. 2000/HE07/008

LEARNER GUIDE

MODULE: CYBER SECURITY 700

PREPARED ON BEHALF OF

RICHFIELD Graduate Institute of Technology (PTY) LTD

RICHFIELD Graduate Institute of Technology (PTY) LTD
Registration Number: 2000/000757/07

Contents

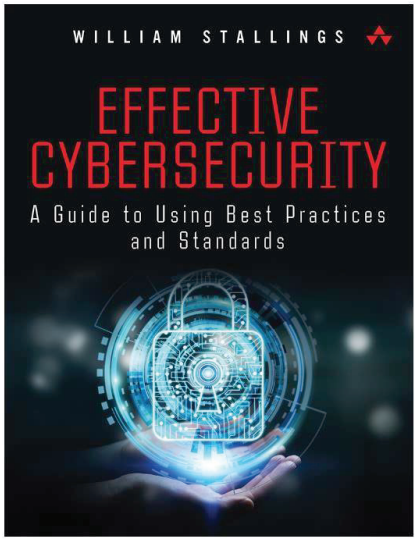
The Information Technology (IT) qualification at Richfield College is a dynamic and future-focused program designed to equip students with advanced technical, analytical, and problem-solving skills. At the core of the qualification is a commitment to academic excellence, industry alignment, and innovation, fostering graduates who are proficient in addressing modern technological challenges. This qualification strategically integrates theoretical knowledge with practical applications, preparing students for various roles in the IT sector. The IT program is structured to address the growing complexity of the evolving technological landscape.
The Higher certificate in Information Technology (HCIT) program is a foundational stepping-stone for students who wish to pursue further studies or enter the workforce. Graduates of this program are well-prepared to articulate to the Diploma in IT (DIT) or the Bachelor of Science in IT (BSc IT) qualifications, providing a seamless transition for those seeking to deepen their knowledge and skills in specialized IT areas. Additionally, the program equips students with the essential competencies for entry-level IT roles such as IT Support Technicians, Junior Web/ System Developers, IT Administrators, etc.

The Diploma in Information Technology (DIT) is a comprehensive and practical program designed to build a strong foundation in IT principles while equipping students with the hands-on skills required to meet industry demands. Focused on both theoretical knowledge and applied learning, this qualification prepares students for intermediate-level roles in IT and serves as a stepping-stone for further academic progression or specialization. Graduates of this program are well-prepared to articulate to the Bachelor of Science in IT (BSc IT) qualification. The curriculum covers programming, networking, database management, system analysis etc., ensuring graduates possess the competencies to solve real-world IT challenges effectively.

The Bachelor of Science in IT (BSc IT) program is structured to address the growing complexity of the evolving technological landscape. Through carefully curated modules, students gain a deep understanding of software development, database management, cloud computing, cybersecurity, IT management, artificial intelligence, machine learning, networking etc. Graduates of this program are well-prepared to articulate to the Bachelor of Science Honours in IT qualification. The curriculum is designed to bridge the gap between academic learning and real-world applications, thus fostering innovation and an entrepreneurial mindset. Students are encouraged to participate in research and practical learning.

Cyber-Security 700 introduces students to the concept of Cybersecurity - Security Governance, frameworks, Information Security. It also focuses on Security Management, Information Risk Assessment, Monitoring and best practices on improving security. Students will be equipped with the technical skills and knowledge required to manage organization’s network and protect them from security breaches and cyber threats.

PRESCRIBED OR RECOMMENDED BOOKS



PRESCRIBED

Stallings,W. (2019). **Effective Cybersecurity: A Guide to Using Best Practices and Standards**. United States: Pearson,
ISBN-13: 978-0-13-477280-6
ISBN-10: 0-13-477280-6

Chapter 1: Best Practices, Standards, and a Plan of Action

Chapter 2: Planning for Cybersecurity

Chapter 3: Security Management

Chapter 4: Managing the Cybersecurity Function- People & Information

Chapter 5: Managing the Cybersecurity Function- Networks and Communications

Chapter 6: Managing the Cybersecurity Function- Threat and Incident

Chapter 7: Security Assessment: Monitoring and Improvement

Chapter 1: Best Practices, Standards, and a Plan of Action

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Demonstrate the need for standards and best practices documents in cybersecurity.**
- **Explain the difference between ISO 27001 and ISO 27002.**
- **Discuss the role of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and how it differs from the objectives of ISO 27002.**
- **Explain the value of the Center for Internet Security (CIS) Critical Security Controls.**

1.1 Introduction, Cyberspace and Cybersecurity

This chapter begins with a definition of cybersecurity and a discussion of the importance of standards and best practices documents in cybersecurity. The sections that follow look at the most significant sources of these documents for effective cybersecurity management. Finally, this chapter provides a discussion of the effective use of standards and best practices documents.

Defining Cyberspace and Cybersecurity

It is useful, at the start of the book, to have working definitions of cyberspace and cybersecurity. A useful definition of cyberspace comes from the National Research Council's publication at the Nexus of Cybersecurity and Public Policy

Cyberspace consists of artifacts based on or dependent on computer and communications technology; the information that these artifacts use, store, handle, or process; and the interconnections among these various elements.

A reasonably comprehensive definition of cybersecurity is provided in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.1205 [Overview of Cybersecurity, 2014]:

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect the cyberspace environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the

cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.

Asset

Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (that is, a system component, such as hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Two related terms should be mentioned:

Information security: Preservation of confidentiality, integrity, and availability of information. In addition, other properties—such as authenticity, accountability, non-repudiation, and reliability—can also be involved.

Network security: Protection of networks and their services from unauthorized modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects.

Cybersecurity encompasses information security, with respect to electronic information, and network security. Information security also is concerned with physical (for example, paper-based) information. However, in practice, the terms cybersecurity and information security are often used interchangeably.

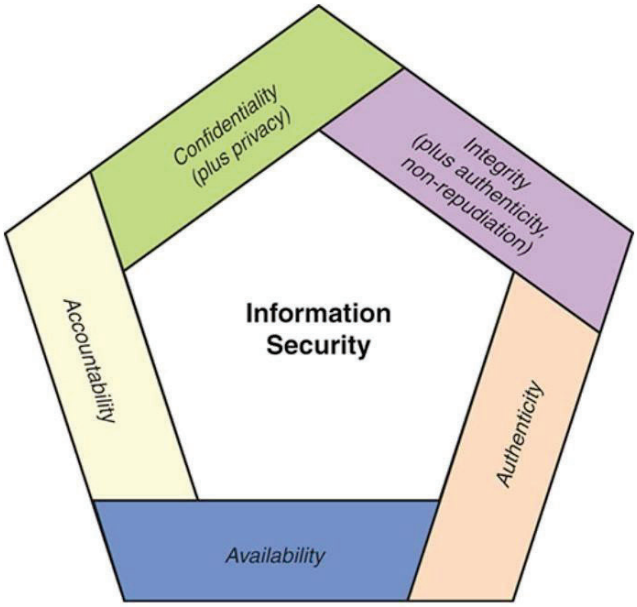


FIGURE 1.1 Essential Cybersecurity Objectives

Figure 1.1 illustrates essential cybersecurity objectives.

A more extensive list of cybersecurity objectives includes the following:

Availability: The property of a system or a system resource being accessible or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; that is, a system is available if it provides services according to the system design whenever users request them.

Integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Authenticity: The property of being genuine and being able to be verified and trusted. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Non-repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Confidentiality: The property that data is not disclosed to system entities unless they have been authorized to know the data.

Accountability: The property of a system or system resource ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

Cybersecurity Dilemmas: Technology, Policy, and Incentives [CICE14] summarizes the challenges in developing an effective cybersecurity system as follows:

Scale and complexity of cyberspace: The scale and complexity of cyberspace are massive. Cyberspace involves mobile devices, workstations, servers, massive data centers, cloud computing services, Internet of Things (IoT) deployments, and a wide variety of wired and wireless networks. The variety of individuals and applications requiring some level of access to these resources is also huge. Further, the challenges to achieving cybersecurity constantly change as technologies advance, new applications of information technologies emerge, and societal norms evolve.

Nature of the threat: Organizational assets in cyberspace are under constant and evolving threat from vandals, criminals, terrorists, hostile states, and other malevolent actors. In addition, a variety of legitimate actors, including businesses and governments, are interested in collecting, analyzing, and storing information from and about individuals and organizations, potentially creating security and privacy risks.

Threat

A potential for violation of security that exists when there is a circumstance, a capability, an action, or an event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

- **User needs versus security implementation:** Users want technology with the most modern and powerful features, that is convenient to use, that offers anonymity in certain circumstances, and that is secure. But there is an inherent conflict between greater ease of use and greater range of options on the one hand and robust security on the other. In general, the simpler the system, and the more its individual elements are isolated from one another, the easier it is to implement effective security. But over time, people demand more

functionality, and the greater complexity that results makes systems less secure. Users or groups within an organization that feel inconvenienced by security mechanisms will be tempted to find ways around those mechanisms or demand relaxation of the security requirements.

- **Difficulty estimating costs and benefits:** It is difficult to estimate the total cost of cybersecurity breaches and, therefore, the benefits of security policies and mechanisms. This complicates the need to achieve consensus on the allocation of resources to security.

Because of these challenges, there is an ongoing effort to develop best practices, documents, and standards that provide guidance to managers charged with making resource allocation decisions as well as those charged with implementing an effective cybersecurity framework. The focus of this book is on the broad consensus that has been reached, as expressed in such documents. The volume and variety of these documents is very broad, and the goal of this book is to consolidate that material and make it accessible.

1.2 The Value of Standards and Best Practices Documents

The development, implementation, and management of a cybersecurity system for an organization are extraordinarily complex and difficult. A wide variety of technical approaches are involved, including cryptography, network security protocols, operating system mechanisms, database security schemes, and malware identification. The areas of concern are broad, including stored data, data communications, human factors, physical asset and property security, and legal, regulatory, and contractual concerns. And there is an ongoing need to maintain high confidence in the cybersecurity capability in the face of evolving IT systems, relationships with outside parties, personnel turnover, changes to the physical plant, and the ever-evolving threat landscape.

Effective cybersecurity is very difficult, and any attempt to develop an ad hoc, grow-your-own approach to cybersecurity is an invitation to failure. The good news is that a great deal of thought, experimentation, and implementation experience have already gone into the development of policies, procedures, and overall guidance for cybersecurity system management teams. A number of organizations, based on wide professional input, have developed best practices types of documents as well as standards for implementing and evaluating cybersecurity. On the standards side, the most prominent player is the National Institute of Standards and Technology (NIST). NIST has a huge number of security publications, including nine Federal Information Processing Standards (FIPS) and well 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Other organization that have produced cybersecurity standards and guidelines include the ITU-T, International Organization for Standardization (ISO), and the Internet Society (ISOC).

In addition, a number of professional and industry groups have produced best practices documents and guidelines. The most important such document is the Standard of Good Practice for Information Security, produced by the Information Security Forum (ISF). This 300-plus-page document provides a wide range of best practices representing the consensus of industry and government organizations. Other respected organizations, including the Information Systems Audit and Control Association (ISACA) and the Payment Card Industry (PCI), have produced a number of similar documents.

Table 1.1 lists the most prominent best practices and standards documents that are discussed in this book.

TABLE 1.1 Important Best Practices and Standards Documents

Source	Title	Date
ISF	Standard of Good Practice for Information Security	2016
ISO	ISO 27002: Code of Practice for Information Security Controls	2013
NIST	Framework for Improving Critical Infrastructure Cybersecurity	2017
Center for Internet Security (CIS)	CIS Critical Security Controls for Effective Cyber Defense Version 7	2018
ISACA	COBIT 5 for Information Security	2012
PCI Security Standards Council	Data Security Standard v3.2: Requirements and Security Assessment Procedures	2016

1.3 The Standard of Good Practice for Information Security

The ISF is an independent, not-for-profit association of leading organizations from around the world. ISF members fund and cooperate in the development of a practical research program in information security. It is dedicated to investing, clarifying, and resolving key issues in cybersecurity, information security, and risk management and to developing best practice methodologies, processes, and solutions that meet the business needs of its members. ISF members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organizations and developed through an extensive research and work program.

Information Security Forum https://www.securityforum.org/tool/the-isfstandardrmationsecurity/

The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a business-focused, comprehensive guide to identifying and managing information security risks in organizations and their supply chains. The breadth of the consensus in developing the SGP is unmatched. The SGP is based on research projects and input from ISF members, as well as analysis of the leading standards on cybersecurity, information security, and risk management. In creating and updating the SGP, the goal of the ISF is the development of best practice methodologies, processes, and solutions that meet the needs of its members, including large and small business organizations, government agencies, and nonprofit organizations.

The SGP, first released in 1996, has gone through numerous revisions. The current version, as of this writing, is the 2016 version. The development of the standard is based on the results of four main groups of activities, shown in Figure 1.2.

- An extensive work program involving the expertise of a full-time ISF management team that performs comprehensive research into hot topics in information security; produces reports, tools, and methodologies; and maintains strategic projects such as the ISF's Information Risk Analysis Methodology (IRAM).
- Analysis and integration of information security–related standards (for example, ISO 27002, COBIT v5.1) and legal and regulatory requirements (for example, the Sarbanes-Oxley Act 2002, the PCI Data Security Standard, Basel II 1998, the EU Directive on Data Protection). All of the standards listed in Table 1.1 are incorporated into the SGP.

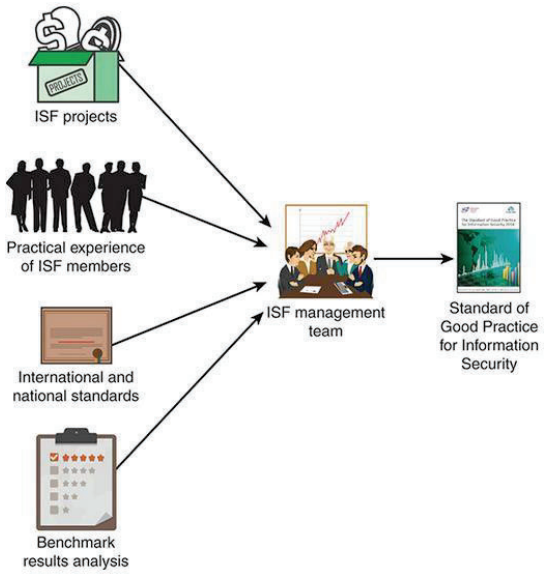


FIGURE 1.2 Basis for the ISF Standard of Good Practice for Information Security

- The involvement of ISF members, using techniques such as workshops, face-to-face meetings, and interviews to contribute their practical experience.
- The results of the ISF Benchmark, which provide valuable insights into how information security is applied in member organizations.

The SGP is of particular interest to the following individuals:

Chief information security officers (or equivalent): Responsible for developing policy and implementing sound information security governance and information security assurance.

Information security managers (as well as security architects, local security coordinators, and information protection champions): Responsible for promoting or implementing an information security assurance program

Business managers: Responsible for ensuring that critical business applications, processes, and local environments on which an organization's success depends are effectively managed and controlled

IT managers and technical staff: Responsible for designing, planning, developing, deploying, and maintaining key business applications, information systems, or facilities

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Internal and external auditors: Responsible for conducting security audits

IT service providers: Responsible for managing critical facilities (for example, computer installations, networks) on behalf of the organization

Procurement and vendor management teams: Responsible for defining appropriate information security requirements in contracts

The SGP is organized into 17 categories, each of which is broken down into 2 areas (see Table 1.2). Each area is further broken down into a number of topics, or business activities, for a total of 132 topics. Each of the 132 topics addresses good practice controls relevant to a particular activity from an information security perspective. Further, each topic is broken down into a number of subtopics, providing a substantial amount of detailed information and guidance. The SGP is consistent with the structure and flow of the ISO/IEC 27000 suite of standards (described in Section 1.4) and is suitable for organizations that want to use it in pursuing ISO compliance or certification or in implementing one or more information security management systems (ISMSs). The structure of the SGP reflects a broad consensus that has evolved and has been refined over more than 20 years.

TABLE 1.2 ISF Standard of Good Practice for Information Security: Categories and Areas

Category	Areas
Security Governance (SG)	Security Governance Approach Security Governance Components
Information Risk Assessment (IR)	Information Risk Assessment Framework Information Risk Assessment Process
Security Management (SM)	Security Policy Management Information Security Management
People Management (PM)	Human Resource Security Security Awareness/Education
Information Management (IM)	Information Classification and Privacy Information Protection
Physical Asset Management (PA)	Equipment Management Mobile Computing
System Development (SD)	System Development Management System Development Life Cycle
Business Application Management (BA)	Corporate Business Applications End User Developed Applications
System Access (SA)	Access Management Customer Access
System Management (SY)	System Configuration System Maintenance
Networks and Communications (NC)	Network Management Electronic Communication
Supply Chain Management (SC)	External Supplier Management Cloud Computing
Technical Security Management (TS)	Security Solutions Cryptography
Threat and Incident Management (TM)	Cybersecurity Resilience Security Incident Management
Local Environment Management (LE)	Local Environments Physical and Environmental Security
Business Continuity (BC)	Business Continuity Framework Business Continuity Process
Security Monitoring and Improvement (SI)	Security Audit Security Performance

It is informative to consider the 17 SGP categories as being organized into three principal activities (see Figure 1.3):

Planning for cybersecurity: Developing approaches for managing and controlling the cybersecurity function(s); defining the requirements specific to a given IT environment; and developing policies and procedures for managing the security function

Managing the cybersecurity function: Deploying and managing the security controls to satisfy the defined security requirements

Security assessment: Assuring that the security management function enables business continuity; monitoring, assessing, and improving the suite of cybersecurity controls

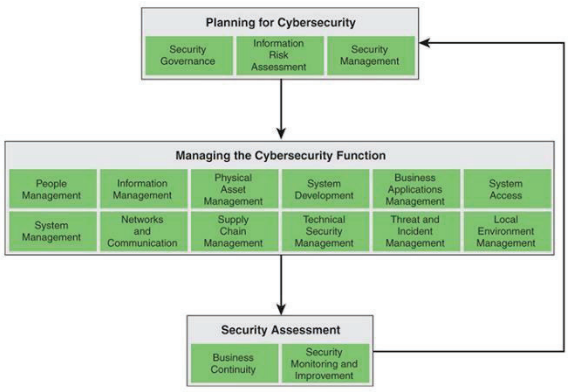


FIGURE 1.3 Categories in the Standard of Good Practice for Information Security

The arrows in Figure 1.3 suggest that these activities occur an ongoing process.

1.4 The ISO/IEC 27000 Suite of Information Security Standards

Perhaps the most important set of standards for cybersecurity is the ISO 27000 suite of information security standards. The ISO is an international agency for the development of standards on a wide range of subjects. It is a voluntary; nontreaty organization whose members are designated standards bodies of participating nations as well as nonvoting observer organizations. Although the ISO is not a government body, more than 70% of ISO member bodies are government standards institutions or organizations incorporated by public law. Most of the remainder have close links with the public

administrations in their own countries. The U.S. member body is the American National Standards Institute (ANSI).

International Organization for Standardization https://www.iso.org/home.html

The ISO, which was founded in 1946, has issued more than 12,000 standards in a broad range of areas. Its purpose is to promote the development of standardization and related activities to facilitate international exchange of goods and services and to develop cooperation in the sphere of intellectual, scientific, technological, and economic activity. It has issued standards covering everything from screw threads to solar energy. One important area of ISO standardization deals with the Open Systems Interconnection (OSI) communications architecture and the standards at each layer of this architecture.

In the areas of data communications, networking, and security, ISO standards are developed in a joint effort with another standards body, the International Electrotechnical Commission (IEC). The IEC is primarily concerned with electrical and electronic engineering standards. The interests of the two groups overlap in the area of information technology, with the IEC emphasizing hardware and the ISO focusing on software. In 1987, the two groups formed the Joint Technical Committee 1 (JTC 1). This committee has the responsibility of developing the documents that ultimately become ISO (and IEC) standards in the area of information technology.

In the area of information security, together the ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 series that deal with ISMSs.1 The ISO 27000 definition of ISMS substantially addresses the concerns of this book:

1. Throughout the rest of this book, for brevity, ISO/IEC standards are simply designated as ISO standards.

Information security management system consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

- awareness of the need for information security
- assignment of responsibility for information security;
- incorporating management commitment and the interests of stakeholders
- enhancing societal values
- risk assessments determining appropriate controls to reach acceptable levels of risk
- security incorporated as an essential element of information networks and systems
- active prevention and detection of information security incidents
- ensuring a comprehensive approach to information security management
- continual reassessment of information security and making of modifications as appropriate

The ISO 27000 series deals with all aspects of an ISMS. It helps small, medium, and large businesses in any sector keep information assets secure. This growing collection of standards falls into four categories (see Figure 1.4):

Overview and vocabulary: Provide an overview and relevant vocabulary for ISMS

Requirements: Discuss normative standards that define requirements for an ISMS and for those certifying such systems

Guidelines: Provide direct support and detailed guidance and/or interpretation for the overall process of establishing, implementing, maintaining, and improving an ISMS

Sector-specific guidelines: Address sector-specific guidelines for an ISMS

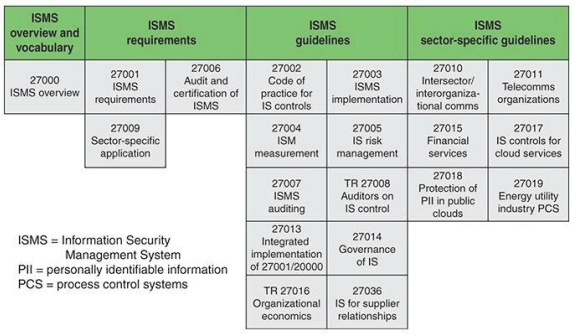


FIGURE 1.4 ISO 27000 ISMS Family of Standards

The most significant documents in the series are those that are cited in the ISF SGP:

ISO 27001: ISMS Requirements: Provides a mandatory set of steps—such as defining a target environment, assessing risks, and selecting appropriate controls—for creating an ISMS, against which an organization can certify its security arrangements.

ISO 27002: Code of Practice for Information Security Controls: Provides a framework of security controls that can be used to help select the controls required in an ISMS.

ISO 27005: Information Security Risk Management System Implementation Guidance: Provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk reporting, risk monitoring, and risk review. Examples of risk assessment methodologies are included as well.

ISO 27014: Governance of Information Security: Provides guidance on principles and processes for the governance of information security, by which organizations can evaluate, direct, and monitor the management of information security.

ISO 27036: Information Security for Supplier Relationships: Outlines information security for external parties for both the acquirers and suppliers. It supports organizations in implementing information security controls related to supplier relationships.

Security controls

The management, operational, and technical controls (that is, countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

ISO 27001

Although ISO 27001 is brief, it is an important document for organizational executives with security responsibility. It is used to define the requirements for an ISMS in such a way that it serves as a checklist for certification. Certification gives credibility to an organization, demonstrating that a product or service meets the expectations of the organization's customers. For example, security certification using ISO 27001 is a way for executives to be assured that the security capability was funded and implemented and meets the security requirements of the organization. For some industries, certification is a legal or contractual requirement. A number of independent certification bodies provide certification services.

certification

The provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements. Also known as third-party conformity assessment.

According to an article in ISSA Journal, ISO 27001 certification confers the following benefits

- Certification assures an organization that it is following practices that broad experience has shown reduce the risk of security breaches.
- Certification assures an organization that it is following practices that broad experience has shown reduce the impact of any breach that does occur.
- If an organization can attest that its security and record handling procedures have been certified, this should reduce the potential penalty for a security breach imposed by regulators. The certification indicates a good faith effort to following broadly accepted best practices and standards.
- Certification assures stakeholders that the organization has developed and implemented sound security policy.
- Certification provides independent third-party validation of an organization's ISMS.
- Certification to the ISO 27001 standard is the most comprehensive information security standard that is internationally accepted.

ISO 27001 is a management standard initially designed for the certification of organizations. The system works like this: An organization develops an ISMS, which consists of policies, procedures, people, technology, and so on, and then invites a certification body to determine that the ISMS is compliant with the standard; this is called a certification audit. Of course, there must be qualified individuals to develop and maintain the ISMS. Thus, various certification programs have been developed for individuals, the most common being for ISO 27001 Lead Implementer and ISO 27001 Lead Auditor programs. Obtaining such a certification enhances the value of an employee to an organization.

TABLE 1.3 ISO 27001 Requirements Topics

Requirement	Topics
4 Context of the Organization	**4.1** Understanding the Organization and Its Context **4.2** Understanding the Needs and Expectations of Interested Parties **4.3** Determining the Scope of the Information Security Management System **4.4** Information Security Management System
5 Leadership	**5.1** Leadership and Commitment **5.2** Policy **5.3** Organizational Roles, Responsibilities and Authorities
6 Planning	**6.1** Actions to Address Risks and Opportunities **6.2** Information Security Objectives and Planning to Achieve Them
7 Support	**7.1** Resources **7.2** Competence **7.3** Awareness **7.4** Communication **7.5** Documented Information
8 Operation	**8.1** Operational Planning and Control **8.2** Information Security Risk Assessment **8.3** Information Security Risk Treatment
9 Performance Evaluation	**9.1** Monitoring, Measurement, Analysis and Evaluation **9.2** Internal Audit **9.3** Management Review
10 Improvement	**10.1** Nonconformity and Corrective Action **10.2** Continual Improvement

Table 1.3 lists the requirements and topics covered by ISO 27001 (using the numbering scheme in the ISO document).

ISO 27002

Although ISO 27001 lays out the requirements for an ISMS, it is rather general, and the specification of the requirements is only nine pages long. Of equal importance is ISO 27002, Code of Practice for Information Security Controls, which provides the broadest treatment of ISMS topics in the ISO 27000 series and comprises 90 pages. The linkage between the ISMS requirements defined in ISO 27001 and the information security controls defined in ISO 27002 is provided by Section 6.1.3 of ISO 27001, Information Security Risk Treatment. In essence, this section requires that an organization develop a risk treatment process by determining what controls must be implemented for the risk treatment options chosen. The section then references the controls in ISO 27002 and indicates that the organization can pick and choose the controls that are needed to satisfy the ISMS requirements. But

ISO 27001 also states that the organization can select controls from any source, not solely or necessarily ISO 27002.

Table 1.4 lists the topics covered in ISO 27002 (using the numbering scheme in the ISO document). It should be mentioned that ISO 27001 and 27002 do not cover a number of important topics discussed in the ISF SGP, including threat intelligence and system decommissioning, and the ISF SGP is far more detailed

TABLE 1.4 ISO 27002 Control Topics

Control	Topics
5 Information Security Policies	**5.1** Management Direction for Information Security
6 Organization of Information Security	**6.1** Internal Organization **6.2** Mobile Devices and Teleworking
7 Human Resource Security	**7.1** Prior to Employment **7.2** During Employment **7.3** Termination and Change of Employment
8 Asset Management	**8.1** Responsibility for Assets **8.2** Information Classification **8.3** Media Handling
9 Access Control	**9.1** Business Requirements of Access Control **9.2** User Access Management **9.3** User Responsibilities **9.4** System and Application Access Control
10 Cryptography	**10.1** Cryptographic Controls
11 Physical and Environmental Security	**11.1** Secure Areas **11.2** Equipment
12 Operations Security	**12.1** Operational Procedures and Responsibilities **12.2** Protection from Malware **12.3** Backup **12.4** Logging and Monitoring **12.5** Control of Operational Software **12.6** Technical Vulnerability Management **12.7** Information Systems Audit Considerations
13 Communications Security	**13.1** Network Security Management **13.2** Information Transfer
14 System Acquisition, Development and Maintenance	**14.1** Security Requirements of Information Systems **14.2** Security in Development and Support Processes **14.3** Test Data
15 Supplier Relationships	**15.1** Information Security in Supplier Relationships
16 Information Security Incident Management	**16.1** Management of Information Security Incidents and Improvements
17 Information Security Aspects of Business Continuity Management	**17.1** Information Security Continuity **17.2** Redundancies
18 Compliance	**18.1** Compliance with Legal and Contractual Requirements **18.2** Information Security Reviews

1.5 Mapping the ISO 27000 Series to the ISF SGP

For an organization that relies on ISO 27001 for certification and ISO 27002 for a selection of controls to meet ISO 27001 requirements, the ISF SGP is an invaluable and perhaps essential tool. It provides a far more detailed description of the controls and represents the widest possible consensus among industry, government, and academic security experts and practitioners.

Table 1.5 shows maps the ISO 27001 requirements to the ISF SGP security controls. For each of the detailed requirements, this table indicates the controls that can be used to satisfy those requirements, as documented in the ISF SGP.

TABLE 1.5 Mapping ISO 27001 to the ISF SGP

ISO 27001 Topic	ISF SGP Category
4.1 Understanding the Organization and Its Context	Security Governance
4.2 Understanding the Needs and Expectations of Interested Parties	Security Governance
4.3 Determining the Scope of the Information Security Management System	Security Management
4.4 Information Security Management System	Security Management
5.1 Leadership and Commitment	Security Governance
5.2 Policy	Security Management
5.3 Organizational Roles, Responsibilities and Authorities	Security Governance
6.1 Actions to Address Risks and Opportunities	Information Risk Assessment
6.2 Information Security Objectives and Planning to Achieve Them	Security Management
7.1 Resources	Security Management
7.2 Competence	People Management
7.3 Awareness	People Management
7.4 Communication	People Management
7.5 Documented Information	Security Management
8.1 Operational Planning and Control	Security Management
8.2 Information Security Risk Assessment	Information Risk Assessment
8.3 Information Security Risk Treatment	Information Risk Assessment
9.1 Monitoring, Measurement, Analysis and Evaluation	Security Monitoring and Improvement
9.2 Internal Audit	Security Monitoring and Improvement
9.3 Management Review	Security Monitoring and Improvement
10.1 Non-conformity and Corrective Action	Security Monitoring and Improvement
10.2 Continual Improvement	Security Monitoring and Improvement

Similarly, Table 1.6 shows the mapping between the ISO 27002 security controls and the corresponding controls in ISF SGP. Even if an organization is using ISO 27002 as a checklist of controls to be chosen to meet security requirements, these selections should be augmented by the more detailed information available in the ISF SGP.

TABLE 1.6 Mapping ISO 27002 to the ISF SGP

ISO 27002 Topic	ISF SGP Category
5.1 Management Direction for Information Security	Security Monitoring and Improvement
6.1 Internal Organization	Security Governance
6.2 Mobile Devices and Teleworking	People Management
7.1 Prior to Employment	People Management
7.2 During Employment	People Management
7.3 Termination and Change of Employment	People Management
8.1 Responsibility for Assets	Physical Asset Management
8.2 Information Classification	Physical Asset Management
8.3 Media Handling	Physical Asset Management
9.1 Business Requirements of Access Control	System Access
9.2 User Access Management	System Access
9.3 User Responsibilities	System Access
9.4 System and Application Access Control	
10.1 Cryptographic Controls	Technical Security Management
11.1 Secure Areas	Local Environment Management
11.2 Equipment	Local Environment Management
12.1 Operational Procedures and Responsibilities	System Development
12.2 Protection from Malware	Technical Security Management
12.3 Backup	System Management
12.4 Logging and Monitoring	Threat and Incident Management
12.5 Control of Operational Software	XX
12.6 Technical Vulnerability Management	System Development
12.7 Information Systems Audit Considerations	Security Monitoring and Improvement
13.1 Network Security Management	Networks and Communications
13.2 Information Transfer	Networks and Communications
14.1 Security Requirements of Information Systems	Security Management
14.2 Security in Development and Support Processes	System Development
14.3 Test Data	System Development
15.1 Information Security in Supplier Relationships	Supply Chain Management
16.1 Management of Information Security Incidents and Improvements	Threat and Incident Management
17.1 Information Security Continuity	Business Continuity
17.2 Redundancies	Business Continuity
18.1 Compliance with Legal and Contractual Requirements	Security Management
18.2 Information Security Reviews	Security Monitoring and Improvement

As an example of the benefit of the ISF SGP, consider the category of threat and incident management. In ISO 27002, this category is defined in Section 16 in 4 pages and includes the following 7 subtopics:

16.1.1 Responsibilities and Procedures
16.1.2 Reporting Information Security Events
16.1.3 Reporting Information Security Weaknesses
16.1.4 Assessment of and Decision on Information Security Events
16.1.5 Response to Information Security Incidents

16.1.6 Learning from Information Security Incidents
16.1.7 Collection of Evidence

By contrast, the corresponding treatment in the ISF SGP is defined in 22 pages and consists of 9 topics and a total of 74 subtopics, as shown in Table 1.7. For additional guidance, each topic in Table 1.6 is labeled as fundamental or specialized; links to documents at the ISF website provide related background and technical tutorial information. An organization that makes use of all this information can have significant confidence that it is effectively deploying the security controls needed to meet the requirement.

TABLE 1.7 The SGP Threat and Incident Management Category

Area	Topic	Number of Subtopics	Type
Cyber Security Resilience	Technical Vulnerability Management	10	Fundamental
	Security Event Logging	7	Fundamental
	Security Event Management	11	Specialized
	Threat Intelligence	10	Specialized
	Cyber Attack Protection	8	Specialized
Security Incident Management	Security Incident Management Framework	7	Fundamental
	Security Incident Management Process	5	Fundamental
	Emergency Fixes	7	Fundamental
	Forensic Investigations	9	Specialized

1.6 NIST Cybersecurity Framework and Security Documents

NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to the U.S. government and to the promotion of U.S. private sector innovation. Despite their national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact. In the area of information security, the NIST Computer Security Resource Center (CSRC) is the source of a vast collection of documents that are widely used in the industry.

NIST Computer Security Resource Center (CSRC) http://csrc.nist.gov

NIST Cybersecurity Framework

In response to the growing number of cyber intrusions at U.S. federal agencies, Executive Order 13636, Improving Critical Infrastructure Cybersecurity [EO13], directed the NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The resulting NIST Cybersecurity Framework [NIST18] includes leading practices that a variety of standards bodies have deemed successful. Thus, the framework is a collection of best practices—practices that improve efficiency and protect constituents. Although provided for federal agencies, the document is of use for nongovernment organizations.

NIST Cybersecurity https://www.nist.gov/topics/cybersecurity

The NIST Cybersecurity Framework consists of three components (see Figure 1.5):

- **Core:** Provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
- **Implementation tiers:** Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
- **Profiles:** Represents the outcomes based on business needs that an organization has selected from the Framework Core categories and subcategories

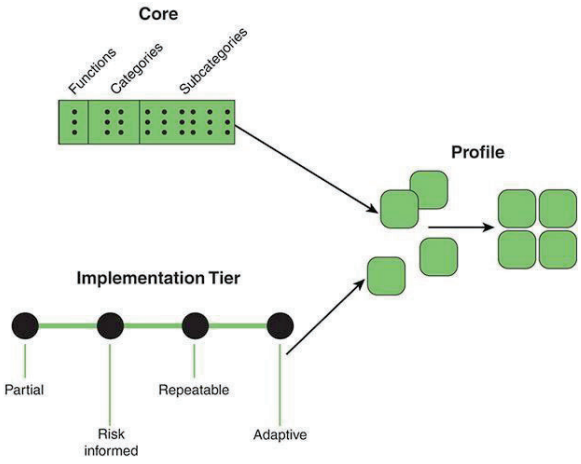


FIGURE 1.5 NIST Cybersecurity Framework Components

The Framework Core identifies five key functions that comprise an organization's cybersecurity risk management approach. As shown in Table 1.8, each function is divided into a number of specific categories, each of which in turn is divided into a number of more detailed subcategories, for a total of 23 categories and 106 subcategories. The five functions provide a high-level view of the elements that comprise risk management for an organization. The categories are groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Each category is divided into subcategories of specific outcomes of technical and/or management activities that provide a set of results that, while not exhaustive, help support achievement of the outcomes in each category. For each subcategory the NIST Cybersecurity Framework provides a list of informative references, which are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate methods of achieving the outcomes associated with each subcategory.

TABLE 1.8 NIST Cybersecurity Framework Functions and Categories

Function	Description	Category
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Response Planning Communications Analysis Mitigation Improvements
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event	Recovering Planning Improvements Communications

The Framework Core is intended not so much as a checklist of actions to be performed as a planning tool, enabling decision makers to more clearly appreciate what goes into effective risk management and to determine policies that emphasize the specific activities that are appropriate for the security goals of the organization.

The tiers defined in the Cybersecurity Framework help an organization define the priority that is to be given to cybersecurity and the level of commitment that the organization intends to make. The tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe increasing degrees of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and integrated into an organization's overall risk management practices (see Table 1.9).

TABLE 1.9 Cybersecurity Framework Implementation Tiers

Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1: Partial		
Risk management practices are not formalized but are, rather, ad hoc. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	Limited awareness of risk, no organization-wide approach to risk management or cybersecurity information to be shared within the organization.	Lack of coordination and collaboration with other entities.
Tier 2: Risk Informed		
Risk management practices are approved by management but not established as organizationwide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements	Processes and procedures are defined and implemented, and staff have adequate resources to perform their cybersecurity duties. No organizationwide approach to risk management.	No formal coordination and collaboration with other entities.
Tier 3: Repeatable		
Risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on changes in business/mission requirements and the threat and technology landscape.	Organizationwide approach to RM. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	Collaboration with partners enables risk management decisions in response to external events.
Tier 4: Adaptive		
Organization actively adapts to the changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	Organizationwide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.	Organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

Once an organization has clarity on the degree of commitment to risk management (tiers) and an understanding of the actions that can be taken to match that commitment, security policies and plans can be put in place, as reflected in a Framework profile. In essence, a profile is a selection of categories and subcategories from the Framework Core. A current profile reflects the cybersecurity posture of the organization. Based on a risk assessment, an organization can define a target profile and then categories and subcategories from the Framework Core to reach the target. This definition of current and target profiles enables management to determine what has been done and needs to be maintained and what new cybersecurity measures need to be implemented to manage risk. The referenced guidelines, standards, and practices for each subcategory provide concrete descriptions of the work needed to meet the target profile.

The NIST Cybersecurity Framework is an important resource for those involved in the planning, implementation, and evaluation of an organization's cybersecurity capability. It is concise and uses clearly defined categories and subcategories. Approaching a document such as the ISF SGP or the ISO 27002 can be intimidating and even overwhelming because of the large body of knowledge they contain. The Cybersecurity Framework is an excellent resource to help an organization more effectively use these more detailed documents.

NIST Security Documents

NIST has produced a large number of FIPS publications and SPs that are enormously useful to security managers, designers, and implementers. Some of these documents are prescriptive standards, but many of them are tutorials or surveys and provide a continually updated source of educational material on a broad range of security topics. This section mentions some of the most important ones.

By far the most significant of these documents is SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. This document lists management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Although intended for U.S. government systems, it is of equal applicability to IT systems in any organization. State-of-the-practice security controls and control enhancements have been integrated into the latest revision (2013) to address the evolving technology and threat space. Examples include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threats; and trustworthiness, assurance, and resilience of information systems. The revision also features eight new families of privacy controls that are based on the internationally accepted fair information practice principles.

Countermeasure

An action, a device, a procedure, or a technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Other documents of special interest include:

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006): Specifies minimum security requirements in 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

SP 800-100, Information Security Handbook: A Guide for Managers (2006): Provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Its topical coverage overlaps considerably with ISO 27002.

SP 800-55, Performance Measurement Guide for Information Security (2008): Provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.

SP 800-27, Engineering Principles for Information Technology Security: A Baseline for Achieving Security (2004): Presents a list of system-level security principles to be considered in the design, development, and operation of an information system.

SP 800-12, Introduction to Information Security, (2017): Provides an outstanding introduction to the topic of information security.

SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing: Addresses the important security/privacy issues involved in moving data and applications to the cloud.

Recently, NIST introduced a new series of publications designated SP 1800. This new series, created to complement the SP 800 series, targets specific cybersecurity challenges in the public and private sectors and provides practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity.

1.7 The CIS Critical Security Controls for Effective Cyber Defence

The Center for Internet Security (CIS) is a nonprofit community of organizations and individuals seeking actionable security resources. The CIS identifies specific security techniques and practices that the CIS group of experts agree are important.

Center for Internet Security https://www.cisecurity.org

A major contribution of CIS is The CIS Critical Security Controls for Effective Cyber Defense (CSC) [CIS18]. CSC focuses on the most fundamental and valuable actions that every enterprise should take. Value here is determined by knowledge and data—the ability to prevent, alert, and respond to the attacks plaguing enterprises today. CSC is significant for the real-world, practical nature of its information. It is not simply a list of controls that might be useful but a source that can be used to guide implementation of policy. The introduction to the CSC indicates that the controls have been matured by an international community of individuals and institutions that:

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action.
- Document stories of adoption and share tools to solve problems.
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions/
- Map the CIS controls to regulatory and compliance frameworks and bring collective priority and focus to them.
- Share tools, working aids, and translations.
- Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

The controls were developed as a result of members' experience with actual attacks and defenses that proved effective. The controls listed in the CSC are designed to be the most effective and specific technical measures available to detect, prevent, respond to, and mitigate damage from the most common to the most advanced attacks.

The bulk of the document is the presentation of 20 controls that encompass the broad range of known threats and the state of the art in countering those threats (see Table 1.10).

TABLE 1.10 The CIS CSC List of Controls

Basic CIS Controls	Foundational CIS Controls	Organizational CIS Controls
CSC 1: Inventory and Control of Hardware Assets	CSC 7: Email and Web Browser Protections	CSC 17: Implement a Security Awareness and Training Program
CSC 2: Inventory and Control of Software Assets	CSC 8: Malware Defenses	CSC 18: Application Software Security
CSC 3: Continuous Vulnerability Management	CSC 9: Limitation and Control of Network Ports, Protocols, and Services	CSC 19: Incident Response and Management
CSC 4: Controlled Use of Administrative Privileges	CSC 10: Data Recovery Capability	CSC 20: Penetration Tests and Red Team Exercises
CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	CSC 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs	CSC 12: Boundary Defense	
	CSC 13: Data Protection	
	CSC 14: Controlled Access Based on the Need to Know	
	CSC 15: Wireless Access Control	
	CSC 16: Account Monitoring and Control	

Each control section includes the following:

- A description of the importance of the control in blocking or identifying the presence of attacks and an explanation of how attackers actively exploit the absence of this control
- A chart of the specific actions, called sub-controls, that organizations are taking to implement, automate, and measure the effectiveness of this control
- Procedures and tools that enable implementation and automation
- Sample entity relationship diagrams that show components of implementation

In addition, a companion document, A Measurement Companion to the CIS Critical Security Controls, describes techniques for measuring the performance of a given sub-control, plus a set of three risk threshold values (lower, moderate, and higher). The risk threshold values reflect the consensus of experienced practitioners.

1.8 COBIT 5 for Information Security

Control Objectives for Business and Related Technology (COBIT) is a set of documents published by ISACA, which is an independent, nonprofit, global association engaged in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. COBIT 5, the fifth version of the set of documents to be released, is intended to be a comprehensive framework for the governance and management of enterprise IT. Of particular concern for this book is the section of COBIT 5 that deals with information security.

COBIT 5 http://www.isaca.org/cobit/pages/default.aspx

COBIT 5 for information security defines a number of policies that are used to develop a management and governance strategy. Table 1.11 lists the key functions associated with each policy.

TABLE 1.11 COBIT 5 for Information Security: Main Policies and Functions

Policy	Key Functions
Business continuity and disaster recovery	▪ Business impact analysis (BIA) ▪ Business contingency plans with trusted recovery ▪ Recovery requirements for critical systems ▪ Defined thresholds and triggers for contingencies, escalation of incidents ▪ Disaster recovery plan (DRP) ▪ Training and testing
Asset management	▪ Data classification ▪ Data ownership ▪ System classification and ownership ▪ Resource utilization and prioritization ▪ Asset life cycle management ▪ Asset protection measures
Rules of behavior (acceptable use)	▪ At-work acceptable use and behavior ▪ Off-site acceptable use and behavior
Information systems acquisition, software development, and maintenance	▪ Information security in the life cycle process ▪ Information security requirements definition process ▪ Information security within the procurement/acquisition process ▪ Secure coding practices ▪ Integration of information security with change management and configuration management
Vendor management	▪ Contract management ▪ Information security terms and conditions ▪ Information security evaluation ▪ Monitoring of contracts for information security compliance
Communication and operation management	▪ IT information security architecture and application design ▪ SLA ▪ IT information security operational procedures
Compliance	▪ IT information security compliance assessment process: ▪ Development of metrics ▪ Assessment repositories
Risk management	▪ Organizational risk management plan ▪ Information risk profile

COBIT 5 also provides a useful organization of the techniques used to achieve effective security into 5 domains and 37 processes, under two general categories, as follows:

- Governance of Enterprise IT
- Evaluate, Direct and Monitor (EDM): 5 processes
- Management of Enterprise IT
- Align, Plan and Organize (APO): 13 processes
- Build, Acquire and Implement (BAI): 10 processes
- Deliver, Service and Support (DSS): 6 processes
- Monitor, Evaluate and Assess (MEA): 3 processes

Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options; setting direction through prioritization and decision making; and monitoring performance, compliance, and progress against agreed-on direction and objectives. Management plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

1.9 Payment Card Industry Data Security Standard (PCI DSS)

The PCI-DSS, a standard of the PCI Security Standards Council, provides guidance for maintaining payment security. The standard sets the technical and operational requirements for organizations accepting or processing payment transactions and for software developers and manufacturers of applications and devices used in those transactions. In essence, PCI DSS compliance governs the way payment card data is processed, handled, and stored. It is required for merchants and all businesses that touch payment data in any way—and that's a lot of businesses.

The PCI defines the scope of the PCI DSS as follows:

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

PCI Security Standards Council https://www.pcisecuritystandards.org/pci_security/

The PCI DSS is structured around 6 goals and 12 requirements, as shown in Table 1.12. Each requirement is further broken up into one or two levels of sub requirements, for which testing procedures and guidance are provided.

TABLE 1.12 PCI DSS Goals and Requirements

Goal	Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The following is an example of a PCI sub requirement:

- **Sub requirement 8.1.2:** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- **Testing procedures:** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.
- **Guidance:** To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.

As you can see, the specification is clear and straightforward. Taken together, the many sub requirements with their testing procedures and guidance provide a powerful tool for managing a cybersecurity capability in the context of the use of payment cards.

1.10 ITU-T Security Documents

The International Telecommunication Union (ITU) is a United Nations specialized agency—hence the members of ITU-T are governments. The U.S. representation is housed in the Department of State. The ITU's charter states that it is "responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis." Its primary objective is to standardize, to the extent necessary, techniques and operations in telecommunications to achieve end-to-end compatibility of international telecommunication connections, regardless of the countries of origin and destination. The ITU Telecommunication Standardization Sector (ITU-T) fulfills the purposes of the ITU relating to telecommunications standardization by studying technical, operating, and tariff questions and adopting recommendations on them with a view to standardizing telecommunications on a worldwide basis.

ITU-T https://www.itu.int/en/Pages/default.aspx

ITU-T has developed thousands of recommendations organized into 23 series. Security-related recommendations are scattered throughout a number of these series, making it difficult to gain a unified view of what the ITU-T has to offer in the way of guidance and explanation related to cybersecurity. Table 1.13 summarizes the key topics on cybersecurity, information security, and network security covered in numerous recommendations. Although the ITU-T focus has traditionally been telecommunications and Internet service providers (ISPs), many of the security documents have broader applicability.

TABLE 1.13 Key Topics Covered by ITU-T Security Recommendations

Topic	Subtopics
Security requirements	Threats, risks, and vulnerabilities Personnel and physical security requirements Next-generation networks Security requirements for IPCablecom IPTV
Security architectures	Open systems security architecture Security services Security architecture for end-to-end communications Availability of the network and its components Application-specific architectures Peer-to-peer security architectures Message security Network management architecture IPCablecom architecture IPTV

Security management	Information security management
	Risk management
	Incident handling
	Asset management
	Governance of information security
	Telecommunications management
Role of the directory	Directory concepts
	Public-key security mechanisms
	Privilege management infrastructure
	Protection of Directory information
	Privacy protection
Identity management and telebiometrics	Identity management
	Overview of identity management
	Key ITU-T identity management standards
	Telebiometrics
	Telebiometric authentication
	Security and safety aspects of telebiometrics
	Telebiometrics related to human physiology
	Telebiometrics in e-health and telemedicine
Examples of approaches to authentication and non-repudiation	Secure password-based authentication protocol with key exchange
	One-time password authentication
	Non-repudiation framework based on one-time password
	Delegated non-repudiation
Securing the network infrastructure	The telecommunications management network
	Securing monitoring and control activities
	Securing network operation activities and management applications
	Protection against electromagnetic threats
	Common security management services
	CORBA (Common Object Request Broker Architecture)-based security services
Some specific approaches to network security	Next-generation network security
	Mobile communications security
	Security for home networks
	IPCablecom
	Ubiquitous sensor networks
Cybersecurity and incident response	Cybersecurity information exchange
	Exchange of vulnerability information
	Discovery of cybersecurity information
	Incident handling
Application security	Voice over IP (VoIP) and multimedia
	IPTV
	DRM for cable television multiscreen
	Secure fax
	Web services
	Tag-based services
Countering common network threats	Spam
	Malicious code, spyware, and deceptive software
	Notification and dissemination of software updates
Security aspects of cloud computing	Key characteristics of cloud computing
	Generic cloud computing capabilities and services
	Emerging cloud services
	Security threats and security challenges to cloud computing

ITU-T Recommendations https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

As a guide to understanding and using these recommendations, ITU-T maintains a security manual, Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of existing ITU-T Recommendations for Secure Telecommunications, most recently updated in 2015 [ITUT15].

1.11 Effective Cybersecurity

This section introduces a useful way of view the cybersecurity management process and discusses the role of the best practices and standards documents discussed throughout this chapter.

The Cybersecurity Management Process

An essential characteristic of cybersecurity provision is that it is not a single end that is attained but an ongoing process. The goal of effective cybersecurity is constantly receding as management strives to keep up with changes in the cyberspace ecosystem, which comprises technology, threat capability, applications, IT resources, and personnel. Figure 1.6, which is similar in nature to figures found in SP 800-53, ISF SGP, and X.1055 (Risk Management and Risk Profile Guidelines for Telecommunication Organizations), suggests the nature of the cybersecurity management process.

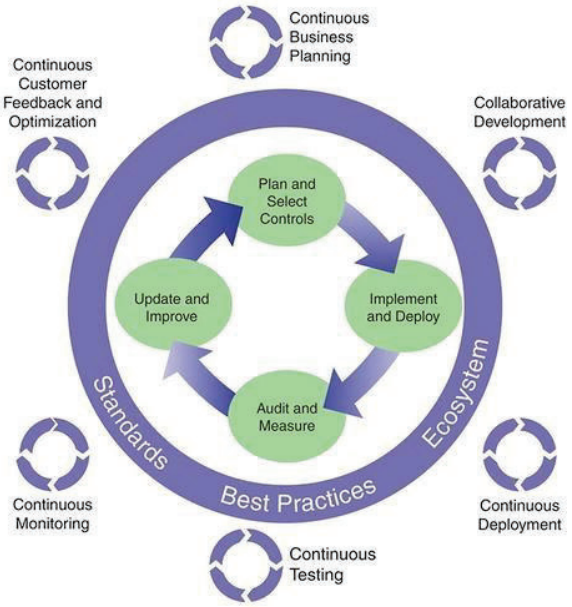


FIGURE 1.6 Cybersecurity Management Process

The process is a reiterative cycle with four major activities:

1. Assess the risk, considering the following:
   a) Assets and their value or utility
   b) Threats and vulnerabilities associated with these assets
   c) Risk of exposure of these assets to the threats and vulnerabilities
   d) Risk and impacts resulting from this risk of exposure
2. 1b. Address the risk(s), considering the following:
   a) Identification of available risk management options
   b) Selection of preferred risk management option
   c) Final risk management decision
3. Implement the risk management decision, considering the following:
   a) Selection of controls
   b) Allocation of resources, roles, and responsibilities
   c) Implementation of controls
4. Monitor, review, and communicate the risks, considering the following:
   a) Monitoring of the risk situation
   b) Risk-related measurements
   c) Review and re-assessment of the risks
   d) Communication of the risks
5. Update and improve the controls:
   a) Updating controls
   b) Improving controls

This repeating cycle is governed not only by the evolving ecosystem of cyberspace but also by evolving standards and best practices.

FIGURE 1.7 Cybersecurity Information and Decision Flows Within an Organization

At a broader perspective, there are in fact two cyclic processes at work: one at the executive level, which focuses on

organizational risk, and one at the business level, which focuses on critical infrastructure risk management. Figure 1.7, similar to one in the NIST Cybersecurity Framework, illustrates this relationship. At the executive level, upper management defines mission priorities, establishes acceptable risk tolerance, and determines available resources. At the business level, IT management translates these guidelines into controls for risk management.

Using Best Practices and Standards Documents

This chapter reviews a broad range of documents available to cybersecurity planners and implementers. Although there is considerable overlap in these documents, recognizing the differences can make the use of these documents more effective. In terms of overall planning, perhaps the key resource is the NIST Cybersecurity Framework. It provides management with a clear methodology for developing a framework profile. This profile can then be used as a guide in assembling a suite of controls for risk management.

For purposes of putting together a set of cybersecurity controls, ISF SGP and ISO 27002 provide the most thorough guidance. In particular, the ISF SGP is a comprehensive survey of what is available to cybersecurity managers, implementers, and evaluators, taken to a thorough level of detail.

For choosing specific controls, the CIS Critical Security Controls document is invaluable as its details are based on broad real-world experience.

In addition, other documents, especially from NIST and ITU-T, provide broad coverage of cybersecurity topics, including tutorial-style presentations, recommendations in specific areas, and supporting material.

1.12 Review Questions / Case Studies / Projects

1. Explain briefly each of the following terms from the perspective of cybersecurity: availability, integrity, authenticity, non-repudiation, confidentiality.
2. Enumerate three key challenges in developing an effective cybersecurity system and provide examples of each one.
3. Name a few technologies commonly implemented for cybersecurity in large organizations.
4. What is the most significant activity of the Information Security Forum (ISF)?
5. What are the three key activities for information security as per the Standard of Good Practice for Information Security?
6. Explain what the term ISMS stands for and what it means.
7. Explain briefly the five core functions in the NIST Cybersecurity Framework.
8. Which is the weakest area of information security in any organization?

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Creating a new app project**
- **Exploring the components of an Android app**
- **Setting up the emulator to run and test apps, and building a variation of the Basic App**

2.1 Introduction

provides an overview of approaches for managing and controlling the cybersecurity function; defining the requirements specific to a given IT environment; and developing policies and procedures for managing the security function. introduces the concept of information security governance. The chapter discusses how security governance enables the direction and oversight of information security-related activities across an enterprise, as an integrated part of corporate governance. Discusses the range of issues dealing with defining security requirements for an organization and developing procedures to ensure compliance. Focuses on security issues that are primarily related to the internal policies and operation of an organization. This includes:

(a) security policy and organization: issues related to defining a comprehensive security policy, keeping it up to date, and effectively communicating it; and

(b) information security management: issues relating to the management of the information security function, to ensure good practice in information security is applied effectively and consistently throughout the organization.

Starting a New App

Android Studio is an integrated development environment (IDE) provided by Google as their official tool for developing Android phone and tablet applications. This tool is continually being refined and has become quite powerful and reliable with recent versions. Especially useful is the enhanced ability to identify deprecated code, inefficient code, and code that doesn't conform to Android design guidelines.

Android is a mobile operating system designed for smartphones and tablets. The operating system is very powerful, enabling access to a diverse set of hardware resources on a smartphone or tablet. Android is provided by Google and is continually updated, improved, and extended. This makes the development of apps for Android smartphones and tablets both exciting and challenging. The many features of the Android environment are best explained through the act of developing an app.

Starting a New Project

Android Studio organizes apps into projects that are stored in a folder designated by the developer. The folder contains the application's code and resources, code libraries used by the application (or references to them), and metadata that is used to keep track of environment information for the workspace.

To begin, run Android Studio. Android Studio will open the project you were working on when you last closed the IDE. If no project was open, the IDE displays the Welcome window, which lists a number of quick-start options, including starting a new project, opening an existing project, importing a project from another IDE (e.g., Eclipse), and other update and configuration options. Most IDEs are designed with the idea that developers are going to be working on the same machine each time they work on a project. This can cause problems in the education environment, where students do not have the ability to work on the same machine and/or store their work on the machine they are currently working on. However, moving projects in Android Studio is really just a matter of moving the project folder and opening it on the new machine.

Creating the Project

The traditional beginning tutorial for many different languages and development platforms is Hello World. Your first Android app will be a slightly modified Hello World app. In Android Studio, all Android apps are created within a project. To create your first app, you will have to create your first project. Creating a new project requires stepping through a series of windows and making choices to configure your app. To get started, from Android Studio's Welcome window **choose Start a new Android Studio project**. The Choose your project window will open. In this window you choose the type of activity you'd like to start with in the app. An Activity is a core component of any Android application. Activities are typically associated with a visible screen. Most of the core functionality of an app is provided by an activity and its associated screen (called a layout). The choices of activity are limited by your choice

2.2 Security Governance

- Explain the concept of security governance and how it differs from security management.
- Provide an overview of the key components of security governance.
- Discuss the topics that should be covered in a strategic security plan.
- Discuss the topics that should be covered in an information security report.
- Explain the roles and responsibilities that are part of security governance.
- Present an overview of the concepts of information security architecture.
- Present an overview of security governance best practices

Information security governance

The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

ITU-T X.1054, Governance of Information Security, defines information security governance as "the system by which an organization's information security-related activities are directed and controlled."

More generally, the term security governance encompasses governance concerns for cybersecurity, information security, and network security.

Governance

Establishment of policies and continuous monitoring of their proper implementation by the members of the governing body of an organization. Governance includes the mechanisms required to balance the powers of the members (with the associated accountability) and their primary duty of enhancing the prosperity and viability of the organization.

Security Governance and Security Management

To better understand the role of security governance, it is useful to distinguish between information security governance (previously defined), information security management, and information security implementation/operations. ISO 27000 defines information security management as follows:

The supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

And information security implementation/operations can be defined in this fashion:

The implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework.

Figure 2.1 suggests the hierarchical relationship between these three concepts. The security governance level communicates the mission priorities, available resources, and overall risk tolerance to the security management level. In essence, security governance is the process of developing a security program that adequately meets the strategic needs of the business. The security management level uses the information as inputs into the risk management process that realizes the security program. It then collaborates with the implementation/operations level to communicate security requirements and create a cybersecurity profile. The implementation/operations level integrates this profile into the system development life cycle and continuously monitors security performance. It executes or manages security-related processes related to current infrastructure on a day-to-day basis. The security management level uses monitoring information to assess the current profile and reports the outcomes of that assessment to the governance level to inform the organization's overall risk management process.

security program

The management, operational, and technical aspects of protecting information and information systems. A security program encompasses policies, procedures, and management structure and mechanism for coordinating security activity.

Figure 2.1 illustrates the key responsibilities at each level. As indicated, there is interaction among the three layers in the ongoing evolution of the information security management system (ISMS). In addition, three supplemental factors play roles. Internal security incident reports and global vulnerability reports from various sources help define the threat and level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback comes from both internal users and external users who have access to the organization's information assets. This feedback helps improve the effectiveness of policies, procedures, and technical mechanisms. Depending on the organization and its cybersecurity approach, each of the three factors plays a role to a greater or lesser extent at each level.

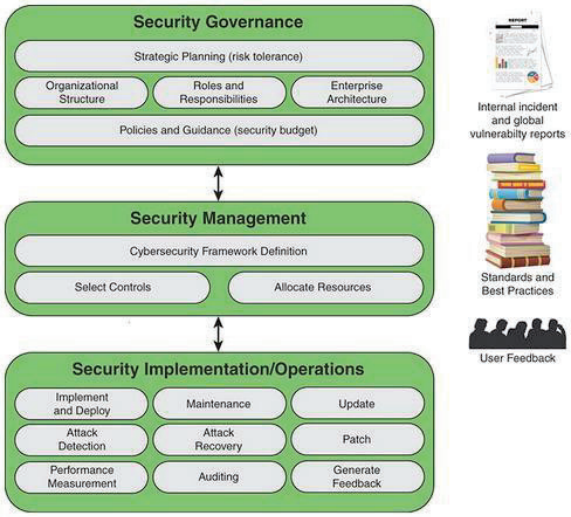


FIGURE 2.1 Information Security Management System Element

Security Governance Principles and Desired Outcomes

Before getting into the details of security governance, an overview of principles and desired outcomes provides useful context.

Principles

X.1054 provides concepts and guidance on principles and processes for information security governance, by which organizations evaluate, direct, and monitor the management of information security. X.1054 lays out as a key objective of information security governance the alignment of information security objectives and strategy with overall business objectives and strategy. X.1054 lists six principles for achieving this objective:

- **Establish organizationwide information security.** Information security, or cybersecurity, concerns should permeate the organization's structure and functions. Management at all levels should ensure that information security is integrated with information technology (IT) and other activities. Top-level management should ensure that information security serves overall business objectives and should establish responsibility and accountability throughout the organization.

  information technology (IT): Applied computer systems, both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. IT is often the name of the part of an enterprise that deals with all things electronic.
- **Adopt a risk-based approach. Security governance,** including allocation of resources and budgets, should be based on the risk appetite of an organization, considering loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.
- **Set the direction of investment decisions.** Information security investments are intended to support organizational objectives. Security governance entails ensuring that information

security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.

- **Ensure conformance with internal and external requirements**. External requirements include mandatory legislation and regulations, standards leading to certification, and contractual requirements. Internal requirements comprise broader organizational goals and objectives. Independent security audits are the accepted means of determining and monitoring conformance.
- **Foster a security-positive environment for all stakeholders**. Security governance should be responsive to stakeholder expectations, keeping in mind that various stakeholders can have different values and needs. The governing body should take the lead in promoting a positive information security culture, which includes requiring and supporting security education, training, and awareness programs.

stakeholder

A person, a group, or an organization that has interest or concern in an organization. Stakeholders can affect or can be affected by the organization's actions, objectives, and policies. Some examples of stakeholders are creditors, directors, employees, government (and its agencies), owners (shareholders), suppliers, unions, and the community from which the business draws its resources.

Review performance in relation to business outcomes. From a governance perspective, security performance encompasses not just effectiveness and efficiency but also impact on overall business goals and objectives. Governance executives should mandate reviews of a performance measurement program for monitoring, audit, and improvement that links information security performance to business performance.

Adherence to these principles is essential to the success of information security in the long term. How these principles are to be satisfied and who is responsible and accountable depend on the nature of the organization.

Desired Outcomes

The IT Governance Institute defines five basic outcomes of information security governance that lead to successful integration of information security with the organization's mission [ITGI06]:

- Strategic alignment: The support of strategic organizational objectives requires that information security strategy and policy be aligned with business strategy.
- Risk management: The principal driving force for information security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.
- Resource management: The resources expended on information security (e.g., personnel time and money) are somewhat open ended and a key goal of information security governance is to align information security budgets with overall enterprise requirements.
- Value delivery: Not only should resources expended on information security be constrained within overall enterprise resource objectives, but also information security investments need to be managed to achieve optimum value.
- Performance measurement: The enterprise needs metric against which to judge information security policy to ensure that organizational objectives are achieved.

It is worthwhile to keep these outcomes in mind throughout the discussion in the remainder of the chapter.

Security Governance Components

SP 800-100 lists the following key activities, or components that constitute effective security governances (refer to Figure 2.1):

- Strategic planning
- Organizational structure
- Establishment of roles and responsibilities
- Integration with the enterprise architecture
- Documentation of security objectives in policies and guidance

The following sections examine each of these components in turn.

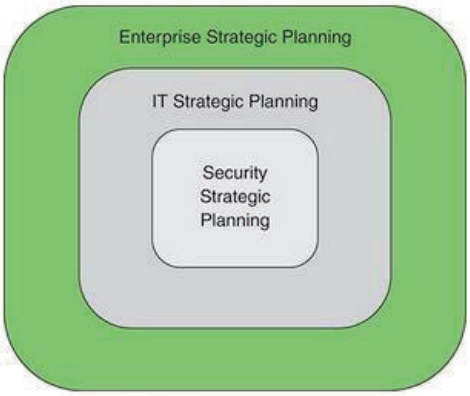


FIGURE 2.2 Strategic Planning

Strategic Planning

It is useful for this discussion to define three hierarchically related aspects of strategic planning (see Figure 2.2):

- Enterprise strategic planning
- Information technology (IT) strategic planning
- Cybersecurity or information security strategic planning

Enterprise strategic planning involves defining long-term goals and objectives for an organization (for example, business enterprise, government agency, or nonprofit organization) and the development of plans to achieve these goals and objectives. The management activity involved in enterprise strategic planning is described in the Strategic Management Group's Strategic Planning Basics [SMG17] as an activity used to set priorities, focus energy and resources, strengthen operations, ensure that employees and other stakeholders are working toward common goals, establish agreement around intended outcomes/results, and assess and adjust the organization's direction in response to a changing environment. It involves the development of a strategic plan and the ongoing oversight of the implementation of that plan.

strategic plan

A document used to communicate, within the organization, the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during planning exercises.

IT strategic planning is the alignment of IT management and operation with enterprise strategic planning. The need to move beyond IT management and to ensure that the IT planning process is integrated with enterprise strategic planning follows from two strategic factors: mission necessity and enterprise maturity [JUIZ15]. With many actors exploiting IT to maximize effectiveness, an organization must engage in strategic planning to ensure that investments in IT produce business value and that the assessment of risks is aligned with enterprise goals and objectives. This is a necessity to support the overall enterprise mission. Further, as the IT infrastructure develops and matures, meeting enterprise strategic goals is likely to involve new arrangements with outside providers, such as cloud service providers, more use of mobile devices by employees and outside actors, and perhaps

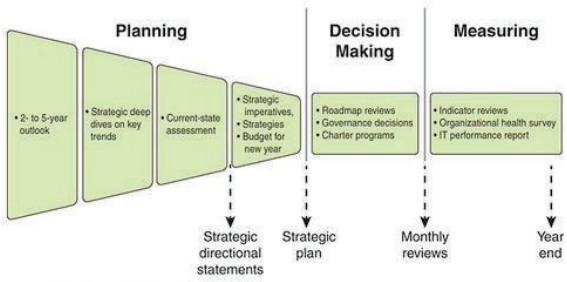


FIGURE 2.3 Intel's IT Strategic Planning Process

reliance on a variety of new hardware and software to develop Internet of Things (IoT) capability. These activities may create unintended barriers to flexibility and introduce new areas of risk. IT management must be guided by strategic planning to meet these challenges.

One of the best-documented examples of IT strategic planning is the process used at Intel [HAYD08a, HAYD08b, PETE12]. It is worth examining this model because it also serves as a model for security strategic planning. Intel's IT strategic planning process comprises six phases, as shown in Figure 2.3.

The six phases are as follows:

1. Two- to five-year business and technology outlook: At the beginning of the year, the planning team takes as input an overall vision and mission statement developed at the enterprise level. During this phase, the team reviews the enterprise strategies, technology trends, employee trends, and so on to better understand the future environment that will shape the IT organization and its deliverables. IT subject matter experts from throughout the organization are recruited to help define the major trends that may be critical in shaping the organization and its decision making in the next few years.
2. Strategic deep dive: The team identifies a small number of high-impact areas that require more in-depth analysis to inform the overall strategic planning process. Depending on circumstances at a given point in time, these may include IoT, social media trends, and changing regulatory compliance rules.
3. Current-state assessment: The planning team analyzes the current state of all the IT-related systems and policies and compares these with the long-range outlook, paying special attention to the key drivers developed in the preceding phase. The result is a set of recommendations for adjustments to IT's focus areas and spending plans.
4. Imperatives, roadmaps, and finances: The next phase is the development of a strategic plan for IT. The plan includes a discussion of strategic objectives and a budget and investment plan. The plan reflects IT's highest-priority items and provides an outcome framework for defining success. Each item includes a roadmap that can influence budget and organization decisions in the upcoming year.
5. Governance process and decision making: Once the annual budget is approved, the information from the preceding phases is used to guide the governance process and the many decisions made across the organization to implement the strategic plan and one-year strategic objectives. These decisions include project chartering, supplier selection, sourcing, investment trade-off decisions, and so on.
6. Regular reviews: Monthly reviews based on a wide variety of input help ensure that the strategic plan and governance decisions are followed. This culminates in a year-end assessment. Reviews continue into the following year until a new strategic plan and new governance decisions provide input for modifying the review process.

This process can include a security strategic planning component, or planning can occur in a coordinated and parallel fashion in another team.

Information security strategic planning is alignment of information security management and operation with enterprise and IT strategic planning. The pervasive use and value of IT within organizations has resulted in an expanded notion of IT's delivery of value to the organization to include mitigation of the organization's risk [ZIA15]. Accordingly, IT security is a concern at all levels of an organization's governance and decision-making processes, and information security strategic planning is an essential component of strategic planning.

An information security strategic plan should be embodied in a document that is approved by the appropriate executives and committees and is regularly reviewed. Table 2.1 suggests an outline for such a document.

TABLE 2.1 Elements of a Strategic Plan Document

Section	Description
Definition	
Mission, vision, and objectives	Defines the strategy for aligning the information security program with organizational goals and objectives, including the role of individual security projects in enabling specific strategic initiatives.
Priorities	Describes factors that determine strategy and the priorities of objectives.
Success criteria	Defines success criteria for the information security program. Includes risk management, resilience, and protection against adverse business impacts.
Integration	Strategy for integrating the security program with the organization's business and IT strategy.
Threat defense	Describes how the security program will help the organization defend against security threats.
Execution	
Operations plan	An annual plan to achieve agreed objectives that involves agreeing on budgets, resources, tools, policies, and initiatives. This plan (a) can be used for monitoring progress and communicating with stakeholders and (b) ensures that information security is included from the outset in each relevant project.
Monitoring plan	This plan involves planning and maintaining a stakeholder feedback loop, measuring progress against objectives, and ensuring that strategic objectives remain valid and in line with business needs.
Adjustment plan	This plan involves ensuring that strategic objectives remain valid and in line with business needs as well as procedures to communicate the value.
Review	
Review plan	This plan describes procedures and individuals/committees involved in regular review of the information security strategy.

Organizational Structure

The organizational structure to deal with cybersecurity depends, in large part, on the size of the organization, its type (for example, government agency, business, nonprofit), and the organization's degree of dependence on IT. But the essential security governance functions to be performed are in essence the same across organizations. Figure 2.4, which is based on a figure in X.1054, illustrates these basic functions within a broader context.

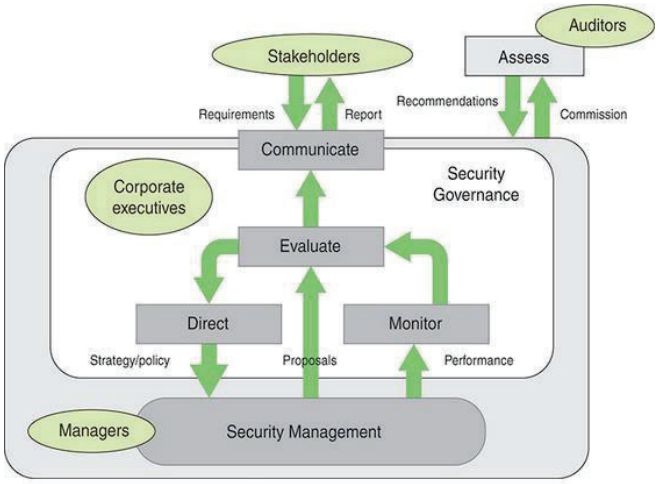


FIGURE 2.4 Framework for Security Governance

The basic security governance functions are as follows:

- **Direct:** Guiding security management from the point of view of enterprise strategies and risk management. This function involves developing an information security policy.
- **Monitor:** Monitoring the performance of security management with measurable indicators.

- **Evaluate:** Assessing and verifying the results of security performance monitoring in order to ensure that objectives are met and to determine future changes to the ISMS and its management.
- **Communicate:** Reporting enterprise security status to stakeholders and evaluating stakeholder requirements.

This framework includes the governing cycle to direct, monitor, and evaluate the ISMS. The evaluation incorporates both the results of the monitoring and proposals from security management to dictate changes and improvements. This cycle is in accordance with Requirement 4.4 in ISO 27001 that the organization shall establish, implement, maintain, and continually improve an ISMS.

The evaluate function triggers communication with stakeholders in the form of a report, which can be issued annually, more frequently, or based on a security incident. As indicated in the Information Security Governance Framework [OHKI09], reporting to stakeholders serves two purposes:

Accountability: Reporting enables stakeholders to ensure that information security is being managed effectively, and it should include the following:

- Information security policy
- Risk evaluation
- Risk measures and response
- Management systems

Effect on corporate value: Reporting should disclose the following:

- Estimates of the costs and benefits of making an inventory of information assets. The information security risk assessment process includes making a complete inventory of information assets. This inventory may support improved strategic management of the information assets, apart from security concerns, which may enhance corporate value.
- Estimates of the value of an inventory of information assets that is developed as a result of information security activities.
- The extent to which information security activities increase the brand value as well as the trust of the customers and partners.
- The economic value of protected information assets.
- The amount by which the security implementation reduces the risk of damaging the information assets.

The following sidebar provides an example of an information security report outline, from the Information Security Governance Framework [OHKI09]. This report structure is based on a study of private companies by the Japanese Ministry of Economics, Trade and Industry. It gives an overall picture of the enterprise's information security governance. Section 5, in particular, involves providing a status update, which should be in sufficient detail for stakeholders to determine whether information security activities are being carried out as planned.

Information Security Report

1. **Basic Information**
   Includes the purpose of issue of the report, cautions relating to usage, target periods and responsible departments.
2. **Concept of Management Regarding Information Security**
   Includes policy regarding information-security undertakings, target scope, ranking of stakeholders in the report and messages to stakeholders.
3. **Information Security Governance**
   Information security management system (e.g., placement of responsibility, organizational structure and compliance), risks relating to information security and information security strategy.
4. **Information Security Measures Planning and Goals**
   Includes action plan and target values.
5. **Results and Evaluation of Information Security Measures**
   Includes results, evaluation, information security quality improvement activities, management of overseas bases, outsourcing, social contribution activities relating to information security and accident reports.
6. **Principle Focal Themes Relating to Information Security**
   Includes internal controls and protection of personal information, undertakings to be particularly emphasized such as Business Continuity Plans, introduction to themes and newly devised points.
7. **Third-Party Approval, Accreditation, etc. (if Required)**

Includes ISMS compliance evaluation system, information security audits, privacy mark systems, number of persons with information security qualifications, classification, and ranking.

X.1054 provides an example of information security status report structure that includes the following detailed contents:

Introduction

- Scope (strategy, policies, standards), perimeter (geographic/organizational units), period covered (month/quarter/six months/year)

Overall status

- Satisfactory/not yet satisfactory/unsatisfactory

Updates (as appropriate and relevant)

- Progress toward achieving the information security strategy
- Elements completed/in-hand/planned
- Changes in information security management system
- ISMS policy revision, organizational structure to implement ISMS (including assignment of responsibilities)
- Progress toward certification
- ISMS (re)certification, certified information security audits
- Budgeting/staffing/training
- Financial situation, headcount adequacy, information security qualifications
- Other information security activities

- Business continuity management involvement, awareness campaigns, internal/external audit assistance

Significant issues (if any)

- Results of information security reviews
- Recommendations, management responses, action plans, target dates
- Progress in respect of major internal/external audit reports
- Recommendations, management responses, action plans, target dates
- Information security incidents
- Estimated impact, action plans, target dates
- Compliance (or noncompliance) with related legislation and regulations
- Estimated impact, action plans, target dates

Decision(s) required (if any)

- Additional resources
- To enable information security to support business initiative(s)

Such an outline is particularly useful for organizations that expect to enhance their reputation by emphasizing their security (for example, information and communications technology businesses). Transparency of the organization's approach to its security risk and appropriate disclosure is also effective at increasing trust. Common awareness can be shared among stakeholders through such activities. For example, public cloud service providers share considerable detail about the information security program and even go the extent of allowing customers to conduct audits and vulnerability testing with prior arrangement. Other service providers and organizations with business customers traditionally did not provided this level of transparency.

Finally, the assess function depicted in Figure 2.4 is performed by independent third-party auditors, commissioned by enterprise top management.

Roles and Responsibilities

A key aspect of security governance is defining the roles and responsibilities of executives related to information security. Typically, these are C-level executives. Executive positions that play a role in security governance include the following:

C-level

Chief level. Refers to high-ranking executives in an organization. Officers who hold C-level positions set the company's strategy, make high-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals.

- **Chief executive officer (CEO):** Responsible for the success or failure of the organization, overseeing the entire operation at a high level.
- **Chief operating officer (COO):** Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.
- **Chief information officer (CIO):** In charge of IT strategy and the computer, network, and third-party (for example, cloud) systems required to support the enterprise's objectives and goals.

- **Chief security officer (CSO) or chief information security officer (CISO):** Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security.
- **Chief risk officer (CRO):** Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings. This role does not exist in most enterprises. It is most often found in financial service organizations. In enterprises in which a CRO is not present, organizational risk decisions may be the responsibility of the CEO or board of directors.
- **Chief privacy officer (CPO):** Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.

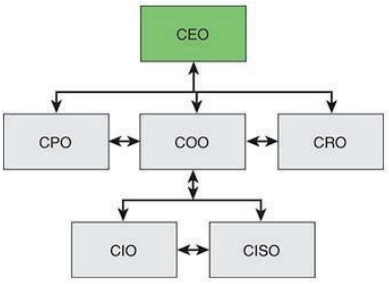


FIGURE 2.5 Possible Reporting Relationships for Security Governance

Figure 2.5 shows an example of reporting relationships among these roles for a large enterprise. In smaller organizations, a number of these roles may be assumed by a single individual.

Two breakdowns of responsibility are useful in showing how to structure security-related roles in an organization. Figure 2.6, based on one in the Corporate Governance Task Force's Information Security Governance: A Call to Action [CGTF04], shows a recommended assignment of roles and responsibilities. This useful report also provides a more detailed discussion of these roles as well as a list of recommendations for implementing effective security governance.

FIGURE 2.6 Security Governance Roles and Responsibilities Example

TABLE 2.2 Information Security Governance Responsibilities

Governance/Business Drivers	Roles and Responsibilities	Metrics/Audit
Corporate Executive		
Legislation, ROI	▪ Provide oversight and coordination of policies ▪ Provide oversight of business unit compliance ▪ Ensure compliance reporting ▪ Monitor actions to enforce accountability	Financial reporting, monetizing losses, conforming to policies
Business Unit Head		
Standards, policies, budgets	▪ Provide information security protection commensurate with the risk and business impact ▪ Provide security training ▪ Develop the controls environment and activities ▪ Report on effectiveness of policies, procedures, and practices	Policy violations, misuse of assets, internal control violations
Senior Manager		
Standards, audit results	▪ Provide security for information and systems ▪ Periodic assessments of assets and their associated risks ▪ Determine level of security appropriate ▪ Implement policies and procedures to cost-effectively reduce risk to acceptable levels ▪ Perform periodic testing of security and controls	Risk assessment and impact analysis, control environmer activities, remedial actions, policy and procedure compliance, security and control test results
CIO/CISO		
Security policies, security operations, and resources	▪ Develop, maintain, and ensure compliance with the program ▪ Designate a security officer with primary duties and training ▪ Develop required policies to support the security program and business-unit-specific needs ▪ Assist senior managers with their security responsibilities ▪ Conduct security awareness training	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

The Business Software Alliance's Information Security Governance: Toward a Framework for Action [BSA03] proposes a governance framework based on three categories (see Table 2.2):

- Governance/business drivers: What am I required to do? What should I do?
- Roles and responsibilities: How do I accomplish my objectives?
- Metrics/audit: How effectively do I achieve my objectives? What adjustments do I need to make?

Integration with Enterprise Architecture

A key element of security governance is the development of an information security architecture. This architecture provides information on how security capabilities (for example, identity and access management) are placed and used in the enterprise architecture. It allocates security requirements and controls to common services or infrastructures. It also provides a foundation for achieving risk-appropriate information system security, determining what circumstances and which security controls apply to information systems.

information security architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Architecture: The way in which the component parts of an entity are arranged, organized, and managed.

enterprise architecture: The systems, infrastructure, operations, and management of all information technology throughout an enterprise. The architecture is typically organized as high-level internally compatible representations of organizational business models, data, applications, and information technology infrastructure.

Over the past 20 years, a number of enterprise architecture models have been developed and adopted by various organizations. Two widely used governance resources for developing an information security architecture as part of an enterprise architecture are The Open Group Architecture Framework (TOGAF) [TOG11] and the Federal Enterprise Architecture Framework (FEAF) [OMB13]. The FEAF is the most comprehensive of all the enterprise architectures in use [SESS07], and this section provides an overview of it. Although developed for use by U.S. federal agencies, the FEAF is used effectively as a governance tool by other government organizations, private enterprises, nonprofit groups, and other organizations.

The FEAF provides the following:

- A perspective on how enterprise architectures are viewed in terms of sub-architecture domains
- Six reference models for describing different perspectives of the enterprise architecture
- A process for creating an enterprise architecture
- A transitional process for migrating from a pre-enterprise architecture to a post-enterprise architecture paradigm
- A taxonomy for cataloging assets that fall within the purview of the enterprise architecture
- An approach to measuring the success of using the enterprise architecture to drive business value

The sub-architecture domains represent specific areas of the overall framework. The domains provided a standardized language and framework for describing and analyzing investments and operations.

Each domain is defined in terms of a set of artifacts, which are essentially items of documentation that describe part or all of an architecture. [EAPA17] describes three levels of artifacts:

High-level artifacts: These document strategic plans and objectives, typically in the form of policy statements and diagrams.

Mid-level artifacts: These document organizational procedures and operations, such as services, supply chain elements, information flows, and IT and network architecture. Typical artifacts at this level are narrative description, flowcharts, spreadsheets, and diagrams.

Low-level EA artifacts: These document the specific resources, such as applications, interfaces, data dictionaries, hardware, and security controls. Typical artifacts at this level are detailed technical specifications and diagrams.

The FEAF describes six domains:

- Strategy
- Business
- Data and information
- Enabling applications
- Host and infrastructure
- Security

TABLE 2.3 Enterprise Architecture Reference Models

Reference Model	Elements	Goals/Benefits
Performance reference model	Goals, measurement areas, measurement categories	Improved organizational performance and governance, cost benefits
Business reference model	Mission sectors, functions, services	Organization transformation, analysis, design, and reengineering
Data reference model	Domain, subject, topic	Data quality/reuse, information sharing, Agile development
Application reference model	System, component, interface	Application portfolio management, cost benefits
Infrastructure reference model	Platform, facility, network	Asset management standardization, cost benefits
Security reference model	Purpose, risk, control	Secure business/IT environment

Corresponding to the six domains are six reference models that describe the artifacts in the corresponding domains (see Table 2.3).

The following description provides further detail of the reference models (RMs):

- **Performance reference model (PRM):** Defines standard ways of describing the value delivered by enterprise architectures, linked to the strategy domain. An example of a PRM artifact for this domain is a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis report that presents the strengths, weaknesses/limitations, opportunities, and threats involved in a project or in a business venture, including risks and impacts.
- **Business reference model (BRM):** Describes an organization through a taxonomy of common mission and support service areas. The BRM provides guidance in defining functions and services in various mission sectors of the enterprise and is linked to the business services domain. An example of a BRM artifact for this domain is a use-case narrative and diagram that describes a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal.
- **Data reference model (DRM):** Facilitates discovery of existing data holdings residing in silos and enables understanding the meaning of the data, how to access it, and how to leverage it to support performance results. The DRM is linked to the data and information domain. An example of a DRM artifact for this domain is a data dictionary, which is a centralized repository of information about data such as name, type, range of values, source, and authorization for access for each data element in the organization's files and databases.
- **Application reference model (ARM):** Categorizes the system- and application-related standards and technologies that support the delivery of service capabilities. The ARM provides guidance in developing a uniform scheme for documenting system, components, and interfaces and for managing application portfolios. It is linked to the enabling applications domain. An example of an ARM artifact for this domain is a system/application evolution diagram. This artifact documents the planned incremental steps toward migrating a suite of systems and/or applications to a more efficient suite, or toward evolving a current system or application to a future implementation.
- **Infrastructure reference model (IRM):** Categorizes the network- or cloud-related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities. The ARM provides guidance in developing a uniform scheme for

documenting platform, facility, and network elements and managing assets. It is linked to the host infrastructure domain. An example of an IRM artifact for this domain is a hosting concept of operations, which presents the high-level functional architecture, organization, roles, responsibilities, processes, metrics, and strategic plan for hosting and use of hosting services. Other artifacts provide detailed documentation of infrastructure elements.

- **Security reference model (SRM):** Provides a common language and methodology for discussing security and privacy in the context of the organization's business and performance goals. The SRM provides guidance in risk-adjusted security/privacy protection and in the design and implementation of security controls. It is linked to the security domain. An example of an SRM artifact for this domain is a continuous monitoring plan, which describes the organization's process of monitoring and analyzing the security controls and reporting on their effectiveness.

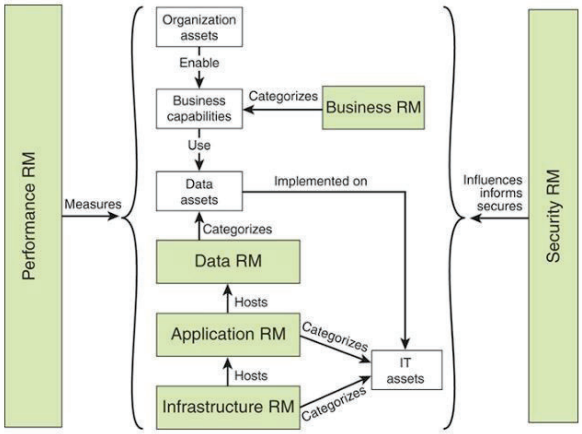


FIGURE 2.7 Relationships Between RM Components

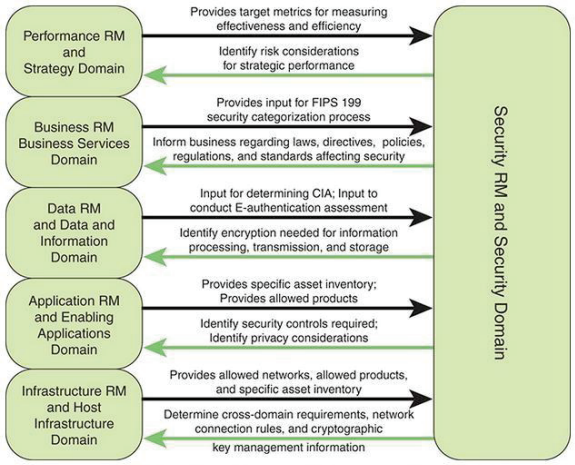


FIGURE 2.8 Interactions Between the Security Reference Model and Other Reference Models

An enterprise architecture is a powerful methodology for enabling enterprise and security governance, and it should be viewed as an essential element of governance.

Policies and Guidance

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, defines an information security policy as an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is an essential component of security governance, providing a concrete expression of the security goals and objectives of the organization. The policies, together with guidance documents on the implementation of the policies, are put into practice through the appropriate selection of controls to mitigate identified risks. The policies and guidance need to cover information security roles and responsibilities, a baseline of required security controls, and guidelines for rules of behavior for all users of data and IT assets.

Security Governance Approach

Effective security governance requires the development and clear documentation of a framework, which is a structured approach for overseeing and managing risk for an enterprise. The implementation and ongoing use of the governance framework enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.

Security Governance Framework

The definition, monitoring, and maintenance of a security governance framework entails a number of tasks:

- Appoint a single executive to be ultimately responsible for security governance, whose duties including implementing the framework and developing and monitoring an information security strategy and security assurance program. The framework needs to encompass all of the elements discussed in Section 2.3.
- Decide and communicate to top executives the objectives of the security governance framework, including ensuring alignment with overall organization policies and goals, enhancing business value, and adequately managing risk.
- Ensure integration of the security architecture with the enterprise architecture, as discussed in Section 2.3.
- Include a process that enables the governing body to evaluate the operation of the information security strategy to ensure that it aligns with business needs the organization's current risk appetite.
- Regularly review the organization's risk appetite to ensure that it is appropriate for the current environment in which the organization operates.
- Formally approve the information security strategy, policy, and architecture.

Security Direction

A governing body is responsible for ensuring that there is effective security direction. Typically, the governing body consists of those individuals ultimately responsible for what the organization does. In a publicly held company, for example, this is the board of directors, supplemented by executive managers who have operational responsibility for various business units.

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) recommends that effective security direction be provided by a combination of a single individual responsible for information security supported by a governing body. The single individual is a CISO or equivalent executive. This individual's responsibilities include implementing the organization's overall approach and ensuring that a security mind-set permeates the organization. This latter requirement entails coordination and collaboration with executives, managers, and operations personnel.

The SGP also recommends that the governing body include the CISO and have a mission to support the CISO as well as review the activities that are under the CISO's direction. Other members of the governing body could include the CIO, key department heads, and heads of business support functions such as human resources. The governing body assists in the coordination of security activities and ensuring that the CISO has the resources and authority required to effect needed changes. In addition, the governing body reports security status and plans to the stakeholders.

COBIT 5 provides a more elaborate governing body structure than the SGP suggests, and it is worthwhile for larger organizations. COBIT 5 distinguishes five distinct roles/structures:

Chief information security officer (CISO): The CISO has overall responsibility for the enterprise information security program. The CISO is the liaison between executive management and the information security program. The CISO should also work with key business stakeholders to address information protection needs. The CISO is responsible for:

i. Establishing and maintaining an ISMS
ii. Defining and managing an information security risk treatment plan
iii. Monitoring and reviewing the ISMS

- **Information security steering (ISS) committee:** This committee ensures, through monitoring and review, that good practices in information security are applied effectively and consistently throughout the enterprise. The ISS committee is responsible for enterprisewide information security decision making in support of strategic decisions made by the enterprise risk management committee.
- **Information security manager (ISM):** The ISM has overall responsibility for the management of information security efforts, including application security, infrastructure security, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.
- **Enterprise risk management (ERM) committee:** This committee is responsible for the decision making of the enterprise to assess, control, optimize, finance, and monitor risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
- **Information custodians/business owners:** These individuals serve as liaisons between the business and information security functions. They are associated with types of information, specific applications, or business units in an enterprise. They serve as trusted advisors and monitoring agents regarding information within the business.

COBIT 5 makes a distinction between the CISO and the ISM, with the CISO being a C-level position with oversight of an ISM, who has operational management responsibilities [ISAC08]. Other organizations combine the roles of CISO and ISM and may dispense with the CISO title.

Also, many organizations have a single security governing body, but COBIT 5 recommends a split into two committees for larger organizations. The ISS committee focuses on ensuring that security policies and practices are effectively implemented and monitored, and the ERM committee focuses on risk assessment. The suggested composition of the ISS committee is as follows:

- CISO: Serves as ISS committee chair and liaison to the ERM committee.
- ISM: Communicates design, implementation, and monitoring of practices.
- Information custodians/business owners: Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- IT manager: Reports on the status of IT-related information security initiatives.
- Representatives of specialist functions: May include, permanently or as needed, representatives from internal audit, human resources, and legal departments.

The suggested composition of the ERM committee is as follows:

- CISO: Provides the committee with advice on specific information risks.
- CEO, COO, CFO, etc.: One or more representatives of senior executive management.
- Information custodians/business owner: Are in charge of certain processes or business applications; responsible for communicating business initiatives that may impact information security and information security practices that may impact the user community.
- Audit/compliance representative: Advises committee on compliance risk.
- Legal representative: Provides legal input.
- CRO: Advises on risk from strategic, financial, operational, reputational, and compliance perspectives.

Responsible, Accountable, Consulted, and Informed (RACI) Charts

COBIT addresses the responsibility of all roles played by employees involved in IT governance actions. The COBIT responsibility model is formalized through a RACI chart matrix attached to all 34 COBIT processes. RACI explains what the responsibilities of all employees are regarding the key activities performance:

- Responsible: A person doing an activity and expected to deliver or submit the assigned work portion within the given deadlines. For example, in the case of software development project, developers are responsible.
- Accountable: A person with decision-making authority and who is expected to ensure the successful completion of project work. For example, a team leader or a project coordinator is accountable.
- Consulted: A stakeholder who should be included in any decision making or work activity by being consulted prior to the decision or action. This may a person whose area of responsibility would be affected by the activity, such as a business unit manager, or a person whose expertise should be consulted, such as a technical professional.
- Informed: A person who needs to know of decision making or actions after they occur. Such a person may have a direct concern in the outcome and progress of the work.

RACI charting helps avoid the following problems:

- Unclear accountability between individuals or departments
- Redundancies or work not being accomplished
- Delayed or incomplete work
- Inadequate communication and/or coordination
- Unclear approval/decision-making processes

Table 2.4 shows a portion of the RACI chart for security governance. The table indicates which entity is accountable for each activity, and which entity or entities are responsible for that activity.

TABLE 2.4 Partial COBIT 5 RACI Chart for Organizational Structures

Activity	CISO	ISS	ISM	ERM	IC/BO
Identify and communicate information security threats, desirable behaviors, and changes needed to address these points.	A		R		
Ensure that environmental and facilities management adheres to information security requirements.	A		R		
Provide ways to improve efficiency and effectiveness of the information security function (for example, through training of information security staff; documentation of processes, technology, and applications; and standardization and automation of the process).	A		R		
Define and communicate an information security strategy that is in line with the business strategy.	R	A			
Research, define, and document information security requirements.	R	A			
Validate information security requirements with stakeholders, business sponsors, and technical implementation personnel.	R	A			
Develop information security policies and procedures.	R	A			
Define and implement risk evaluation and response strategies and cooperate with the risk office to manage the information risk.	R			A	
Ensure that the potential impact of changes is assessed.	R	A			
Collect and analyze performance and compliance data related to information security and information risk management.	R		R		
Raise the profile of the information security function within the enterprise and potentially outside the enterprise.		R			R

A = accountable
R = responsible
IC/BO = Information custodians/business owners

Security Governance Evaluation

An ancient Roman saying asks "Who will guard the guards themselves?" Those who are responsible for enterprise governance and information security governance need to be open to evaluation of their efforts at governance. In a publicly held corporation, the board performs or commissions such evaluation, and in any organization, the auditing function illustrated in Figure 2.7 encompasses an assessment of the governance function.

Johnston and Hale's article "Improved Security Through Information Security Governance" reports a useful set of metrics for evaluating security governance [JOHN09] (see Table 2.5).

TABLE 2.5 Indicators of Information Security Governance Effectiveness

Indicator Category	Indicators
Executive management support	Executive management understands the relevance of information security to the organization
	Executives promote effective information security governance
	Executives actively support the information security program
	Executives comply with all aspects of the information security program
	Executive management understands their responsibility for information security
	Executives understand the liability associated with not executing information security responsibilities
Business and information security relationship	Security investments are optimized to support business objectives
	Business process owners actively support the information security program
	Business process owners view security as an enabler
	Business process owners are involved in evaluating security alternatives
	Business process owners actively support the development of a security culture
	Business process owners accept responsibility for information security
	Business process owners are accountable for information security
Information protection	All information in use within the organization is identified
	Information is classified according to criticality
	Information is classified according to sensitivity
	Information classifications are enforced
	Information classifications are applied to information received from outside entities
	Information classifications are applied to information provided to an outside entity
	Ownership responsibilities for all information are assigned
	Applications that process sensitive information are identified
	Applications that support critical business processes are identified
	Data retention standards are defined and enforced

The metrics fall into three categories:

- Executive management support: This is a critical component for cybersecurity program success. If top executives exhibit an understanding of security issues and take an active role in promoting security, this influence is felt throughout the firm. Strong executive management security awareness and support promotes a culture of secure practices.
- Business and information security relationship: An effective security governance program conveys a strong relationship between business goals and objectives and information security. When information security is incorporated into the enterprise planning process, employees

tend to feel a greater responsibility for the security of their assets and view security not as an impediment but as an enabler.

- Information protection: These indicators of security governance effectiveness deal with the pervasiveness and strength of information security mechanisms. These indicators reflect the degree of awareness of information security issues and the level of preparedness, enterprisewide, to deal with attacks.

The SGP mandates that an organization adopt a consistent and structured approach to information risk management to provide assurance that information risk is adequately addressed. A key element is that a structured technique be used at the governing body level, such as the ISF Business Impact Reference Table (BIRT), discussed in previous Chapter. The BIRT is used to document the maximum level of risk or harm that the organization is prepared to accept in any given situation and is used to inform any decisions about information risk throughout the organization.

Based on the risk appetite, the security strategy, security controls, and security assessment measures are developed.

Security Governance Best Practices

The ISF SGP breaks down the best practices in the security governance category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Security governance approach: This area provides guidance for establishing, maintaining, and monitoring an information security governance framework, which enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management.
- Security governance framework: This topic provides a checklist of actions for establishing a security governance framework and ensuring that the organization's overall approach to information security supports high standards of governance.
- Security direction: This topic outlines a recommended top-down management structure and mechanism for coordinating security activity (for example, an information security program) and supporting the information security governance approach. It includes discussion of a CISO, a working group, and the tasks of each.

Security governance components: This area provides guidance for supporting the information security governance framework by creating an information security strategy and implementing an information security assurance program that are aligned with the organization's strategic objectives.

- Information security strategy: Provides a checklist for developing an information security strategy.
- Stakeholder value delivery: Focuses on how the organization should implement processes to measure the value delivered by information security initiatives and report the results to all stakeholders.
- Information security assurance: Discusses actions to assure that information risk is being adequately addressed.

The ultimate objective of risk assessment is to enable organization executives to determine an appropriate budget for security and, within that budget, implement security controls to optimize the level of protection. This objective is met by providing an estimate of the potential cost to the organization of security breaches, coupled with an estimation of the likelihood of such breaches.

While the utility of risk assessment should be obvious, and indeed it must be considered essential, it is well at the outset to recognize its limitations, which are clearly summarized in Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions [MILL17]. If the scale of the effort is too ambitious, projects become large, complicated, and unreviewable, with a tendency to leave out things that are not easily quantified. On the other hand, if effective ways of calculating risk are not employed, managers tend to underestimate the magnitude of the risk and choose to invest in other areas that are understood better and lead to clear payoffs. Thus, responsible executives need to develop a plan for risk assessment that is balanced between too much and too little. Fortunately, relying on well-accepted best practices, such as those in the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP), makes it possible to develop a systematic approach that incorporates best practices that are reasonable for a given organization.

Risk Assessment Concepts

Risk assessment is a complex subject that is more art than science and calls for considerable management judgment. A good way to begin looking at risk assessment is to consider the terminology listed in Table 3.1, based largely on definitions in ISO 27005, Information Security Risk Management System Implementation Guidance. Nearly identical terminology is used in two other important documents: SP 800-30, Guide for Conducting Risk Assessments, and X.1055, Risk Management and Risk Profile Guidelines for Telecommunication Organizations.

TABLE 3.1 Information Security Risk Terminology

Term	ISO 27005 Definition
asset	Anything that has value to the organization and which therefore requires protection.
impact	Adverse change to the level of business objectives achieved. ISO 27005 uses the term **consequence** instead of impact. SP800-30 uses the terms **impact level** and **impact value** instead of impact.
event	Occurrence or change of a particular set of circumstances.
threat	Potential cause of an unwanted incident, which may result in harm to a system or an organization.
threat action	A realization of a threat—that is, an occurrence in which a vulnerability is exploited as a result of either an accidental event or an intentional act.
threat agent	A system entity that performs a threat action or an event that results in a threat action.
vulnerability	A weakness of an asset or a control that can be exploited by one or more threats.
security incident	An adverse event whereby some aspect of security could be threatened.
risk	A combination of the consequences of an information security event and the associated likelihood of occurrence.
likelihood	The chance of something happening, especially the likelihood of a security incident. X.1055 uses the term **risk of exposure (RoE)** instead of likelihood.
level of risk	The magnitude of a risk, expressed in terms of the combination of consequences and their likelihood.
security control	The management, operational, and technical control countermeasures prescribed to protect the confidentiality, integrity, and availability or other security property of an asset.
residual risk	Risk remaining after risk treatment.
risk identification	The process of finding, recognizing, and describing risks.
risk analysis	The process of comprehending the nature of risk and determining the level of risk.
risk criteria	Terms of reference against which the significance of a risk is evaluated.
risk evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
risk assessment	The overall process of risk identification, risk analysis, and risk evaluation.
risk treatment	The process of modifying risk. SP800-30 uses the term **risk response** instead of risk treatment.
risk management	Coordinated activities to direct and control an organization with regard to risk.

Threats and vulnerabilities need to be considered together. A threat is the potential for a threat agent to intentionally or accidentally exploit a vulnerability, which is a weakness in a system's security procedures, design, implementation, or internal controls. A threat acting on a vulnerability produces a security violation, or breach. The level of risk is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment.

Figure 3.1 illustrates in general terms a universally accepted method for determining the level of risk.

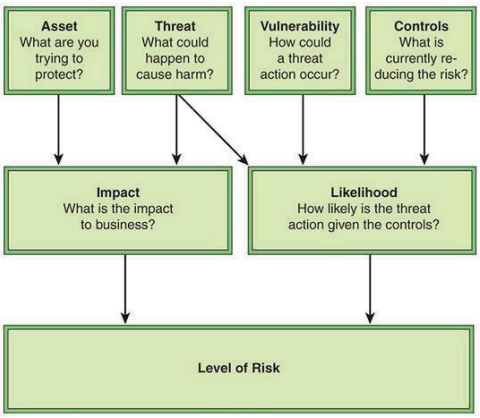


FIGURE 3.1 Determining Information Security Risk

Two main threads, impact and likelihood, should be pursued in parallel. An organization pursues the following tasks related to these threads:

Impact: Consider these two elements in determining impact:

- Assets: Develop an inventory of the organization's assets, which includes an itemization of the assets and an assigned value for each asset. These include intangible assets such as reputation and goodwill, as well as tangible assets, such as databases, equipment, business plans, and personnel.
- Threat: For each asset, determine the possible threats that could reduce the value of that asset. Then, for each asset, determine the impact to the business, in terms of cost or lost value, of a threat action occurring.

Likelihood: Consider the three elements in determining likelihood:

- Threat: For each asset, determine which threats are relevant and need to be considered.
- Vulnerability: For each threat to an asset, determine the level of vulnerability to the threat. That is, determine specifically for an asset how a threat action could be achieved.
- Controls: Determine what security controls are currently in place to reduce the risk.

Then determine how likely it is that a threat action will cause harm, based on the likelihood of a threat action and the effectiveness of the corresponding controls that are in place.

Finally, the level of risk is determined as the combination of the cost of the threat occurring combined with the likelihood of the threat occurring.

For example, a hacker (threat agent) may exploit known vulnerabilities (vulnerability) in a remote authentication protocol (vulnerability target) to disrupt (policy violated) remote authentication (asset exposed). The threat is unauthorized access. The assets are anything that can be compromised by an unauthorized access. The vulnerability expresses how a threat action could occur (for example, by access through a web interface). Existing security controls for this vulnerability reduce the likelihood of a threat action.

Note that both factors, impact and likelihood, are necessary in determining a budget allocation for security controls. If an organization focuses only on impact, the inclination will be to invest much of the security budget on high-impact threats, even if the likelihood of the impact is extremely small. Thus, threats that produce a low or moderate impact and are realized frequently may be given little attention, with the net effect of the overall loss to the business being higher than needed. Conversely, an organization errs in allocating security funds on the basis of likelihood alone. If a relatively rare security event that has very high impact costs is ignored, the organization is exposed to a very high security loss.

Risk Assessment Challenges

An organization faces enormous challenges in determining the level of risk. In general terms, these challenges fall into two categories: the difficulty of estimating and the difficulty of predicting. Consider first the problem of estimation of each of the four elements that contribute to determining risk:

- Asset: An organization needs to put a value on individual assets and how that value may be reduced by a specific threat—in other words, the impact value. A single example indicates how difficult this is. If a company maintains a database of customer credit card numbers, what is the impact of the theft of that database? There are potential legal fees and civil penalties, loss of reputation, loss of customers, and lowering of employee morale. Assessing the magnitude of these costs is a formidable undertaking.
- Threat: In determining the threats facing an organization, there is past experience to go on and, as discussed subsequently, numerous publicly available reports list current threats and their corresponding frequencies. Even so, it should be clear that it is difficult to determine the entire range of threats that are faced as well as the likelihood of any threat being realized.
- Vulnerability: An organization may face security vulnerabilities that it is not aware of. For example, software vendors have been known to delay revealing a security vulnerability until a patch is available or even delaying releasing a patch to a portion of a vulnerability until a complete patch is available (see, for example, [ASHO17], [KEIZ17]). Further, a patch may introduce new vulnerabilities. As another example, a company may have a fireproof barrier constructed around a data center enclosure. But if the contractor does not install a barrier that meets the specification, there may be no way for the company to know this.
- Controls: Controls are implemented to reduce vulnerability and therefore reduce the likelihood of particular threats being realized. However, it may be very difficult to assess the effectiveness of given controls, including software, hardware, and personnel training. For example, a particular threat action may be relatively unlikely, but controls may be introduced because of the high impact in the event that the threat action succeeds. But if the event rarely occurs, the organization has difficulty in determining whether the control has the desired effect. The threat action may be artificially generated to test the system, but this artificial action may not be realistic enough to get a true picture of how effective a control is.

Another challenge in risk assessment is the difficulty of predicting future conditions. Again, considering the four elements, the following problems emerge.

- Asset: Whether the planning period is one year, three years, or five years, changes in the value of an organization's assets complicate the effort to estimate the impact of a security threat. Company expansion, software or hardware upgrades, relocation, and a host of other factors may come into play.
- Threat: It is difficult at best to assess the current threat capability and intentions of potential adversaries. Future projections are even more subject to uncertainty. Entire new types of attack may emerge in a very short period of time. And, of course, without complete knowledge of the threat, it is impossible to provide a precise assessment of impact.
- Vulnerability: Changes within the organization or its IT assets may create unexpected vulnerabilities. For example, if an organization migrates a substantial portion of its data assets to a cloud service provider, the degree of vulnerability of that provider may not be known to the organization with a high level of confidence.
- Controls: New technologies, software techniques, or networking protocols may provide opportunities for strengthening an organization's defenses. But it is difficult to predict the

nature of these new opportunities, much less their cost, and so resource allocation over the planning period may not be optimal.

Complicating matters is the many-to-many relationship between threats, vulnerabilities, and controls. A given threat may be able to exploit multiple vulnerabilities, and a given vulnerability may be subject to attack by multiple threats. Similarly, a single control may address multiple vulnerabilities, and a single vulnerability may require the implementation of multiple controls. These facts complicate the planning of what controls to select and how much of the budget to allocate for various forms of mitigation.

With all these challenges, it is clear that today's executives are unable to follow the advice of Sun Tzu of ignoring the risk by making the position unassailable. Responsible executives can, however, follow a systematic methodology of risk assessment based on well-established best practices.

Risk Management

Risk assessment is one part of the broader security task of risk management. National Institute of Standards and Technology (NIST) Cybersecurity SP 800-37, Risk Management Framework for Information Systems and Organizations, states that risk management includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. It also includes enterprise-level activities to help better prepare organizations to execute a risk management framework at the system level.

To place risk assessment into the context of risk management, this subsection summarizes two risk management concepts defined by ITU-T and ISO.

X.1055 Risk Management Process

Risk management is an iterative process, as illustrated in Figure 3.2, based on one in X.1055.

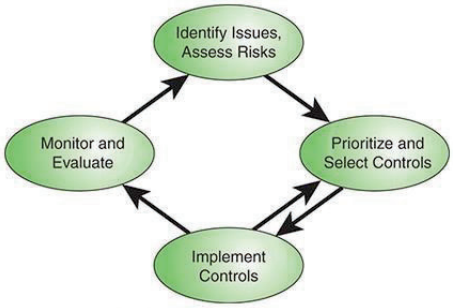


FIGURE 3.2 Risk Management Life Cycle

The steps are as follows:

1. Assess risk based on assets, threats, vulnerabilities, and existing controls. From these inputs, determine impact and likelihood and then the level of risk.
2. Identify potential security controls to reduce risk and prioritize the use of these controls.
3. Allocate resources, roles, and responsibilities and implement controls.
4. Monitor and evaluate risk treatment effectiveness.

The results of the final step are fed back into the next iteration of the risk management life cycle.

ISO 27005, Information Security Risk Management

While a simple risk analysis worksheet may be suitable for smaller organizations, for larger organizations, a broader framework to guide risk assessment is advisable. The most important such framework is ISO 27005, which describes a systematic approach to managing information security risk, particularly in the context of ISO 27001, ISMS Requirements.

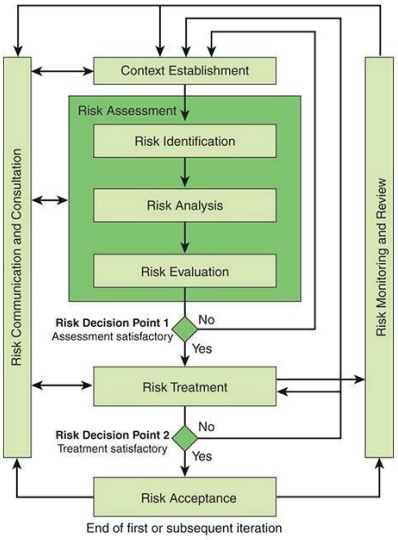


FIGURE 3.3 ISO 27005 Risk Management Process

Figure 3.3 shows the overall risk management process defined in ISO 27005.

This process consists of a number of separate activities:

Context establishment: This is a management function that involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organizational structure for information security risk management. Risk criteria are based on organizational objectives and external and internal context. They can be derived from standards, laws, policies, and other requirements. Table 3.2 lists the guidelines provided in ISO 27005 for context establishment.

Risk assessment: ISO 27001 defines risk assessment as consisting of three activities:

Risk identification: Involves the identification of risk sources, events, their causes, and their potential consequences. It involves historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

Risk analysis: Provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation.

Risk evaluation: Assists in the decision about risk treatment by comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.

Risk treatment: Involves the following:

- Avoiding the risk by deciding not to start or continue with an activity that gives rise to the risk
- Taking or increasing risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed choice

Risk acceptance: Involves ensuring that residual risks are explicitly accepted by the managers of the organization.

Risk communication and consultation: Encompasses the continual and iterative processes that an organization conducts to provide, share, or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

Risk monitoring and review: Includes ongoing monitoring and review of all risk information obtained from the risk management activities.

As shown, the risk management process is an iterative process. As mentioned earlier in this chapter, there are continual changes in business asset valuation, threat capability and frequency, vulnerability magnitude, and control technologies and techniques. In addition, implemented controls may not realize the anticipated benefits. Thus, the assessment and treatment of risk must be an ongoing activity.

Asset Identification

Risk identification is the identification of the assets, threats, existing controls, vulnerabilities, and impacts relevant to the organization and that serve as inputs to risk analysis. This section looks at asset identification.

A first step in risk assessment is to document and determine values for the organization's assets. An asset is anything of value to the business that requires protection, including hardware, software, information, and business assets. Many assets of various types can be identified, and the challenge is to develop a uniform way of documenting the assets, the security implications of each, and the costs associated with security incidents related to each. Asset valuation relates directly to business needs. Accordingly, the input for asset valuation needs to be provided by owners and custodians of assets, not by members of the risk assessment team.

Hardware Assets

Hardware assets include servers, workstations, laptops, mobile devices, removable media, networking and telecommunications equipment, and peripheral equipment. Key concerns are loss of a device, through theft or damage, and lack of availability of the device for an extended period. Another concern is device malfunction, due to deliberate malfunction or other causes. Asset valuation needs to take into account the replacement cost of the hardware, disruption losses, and recovery expenses.

Software Assets

Software assets include applications, operating systems and other system software, virtual machine and container virtualization software, software for software-defined networking (SDN) and network function virtualization (NFV), database management systems, file systems, and client and server software. Availability is a key consideration here, and asset valuation must take account of disruption losses and recovery expenses.

virtual machine

One instance of an operating system along with one or more applications running in an isolated partition within the computer. A virtual machine enables different operating systems to run in the same computer at the same time and also prevents applications from interfering with each other.

container virtualization

A technique in which the underlying operating environment of an application is virtualized. This is commonly the operating system kernel, and the result is an isolated container in which the application can run.

software-defined networking (SDN)

An approach to designing, building, and operating large-scale networks based on programming the forwarding decisions in routers and switches via software from a central server. SDN differs from traditional networking, which requires configuring each device separately and which relies on protocols that cannot be altered.

network function virtualization (NFV)

Virtualization of network functions which involves implementing these functions in software and running them on virtual machines.

Information Assets

Information assets comprise the information stored in databases and file systems, both on-premises and remotely in the cloud. As an example, ITU-T X.1055 lists the following as types of information assets in a telecommunications or network environment:

- Communication data
- Routing information
- Subscriber information
- Blacklist information
- Registered service information
- Operational information
- Trouble information
- Configuration information
- Customer information
- Billing information
- Customer calling patterns
- Customer geographic locations
- Traffic statistical information
- Contracts and agreements
- System documentation
- Research information
- User manuals
- Training materials
- Operational or support procedures
- Business continuity plans
- Emergency plan fallback arrangements
- Audit trails and archived information

Asset valuation needs to take into account the impact of threats to confidentiality, privacy, integrity, and authenticity. As an example of questions involved in information asset evaluation, NISTIR 7621, Small Business Information Security: The Fundamentals, suggests the following:

- What would happen to my business if this information were made public?

- What would happen to my business if this information were incorrect?
- What would happen to my business if my customers or I couldn't access this information?

TABLE 3.3 Identify and Prioritize Information Types

	Example: Customer Contact Information	Info Type 1	Info Type 2	...
Cost of revelation (Confidentiality)	Medium			
Cost to verify information (Integrity)	High			
Cost of lost access (Availability)	High			
Cost of lost work	High			
Fines, penalties, customer notification	Medium			
Other legal costs	Low			
Reputation/public relations costs	High			
Cost to identify and repair problem	High			
Overall Score:	High			

Table 3.3, from NISTIR 7621, is an example of a worksheet for recording this information, including a worked example.

Business Assets

The business assets category includes organization assets that don't fit into the other categories, including human resources, business processes, and physical plant. This category also includes intangible assets, such as organization control, know-how, reputation, and image of the organization.

Asset Register

In order to effectively protect assets, an organization needs to provide a systematic method of documenting assets and their security implications. This is done in an asset register that documents important security-related information for each asset. Examples of items that may be included for each asset are as follows:

- Asset name/description: This information uniquely identifies an asset.
- Asset type: This denotes the type of asset it is, such as physical/infrastructure assets, software, information, service, or human resource.
- Asset class: For purposes of risk assessment, an organization should group assets into classes so risks are measured against classes of assets rather than against individual assets. Asset class examples include desktops/workstations, servers, Payment Card Industry (PCI) devices, restricted/sensitive file shares, and restricted printers.
- Information assets: An information asset defines specifically what kind of information is processed, transmitted, or stored by the asset (for example, customer personally identifiable information [PII], PCI data). This item does not apply to all assets.
- Asset owner: An organization should define the department/company function that owns an asset and is responsible for risk associated with the asset. This is also sometimes referred to as the risk owner or business owner.
- Asset custodian: This is the individual responsible for maintaining, monitoring, and managing the asset. This is typically a network or systems administrator.
- Location: This is the physical location of the asset.
- Function/business process: This is the business process or function the asset supports (for example, information processing facility).
- Data type/classification: The company's established information classification policy should be used to classify the information transmitted, processed, or stored by the asset. This helps drive the risk assessment later.
- Asset value classification: This could be a monetary value but more typically is a ranking, such as low, medium, or high.
- Disaster recovery priority: In the event of a security breach that affects multiple assets, this is the relative priority for devoting resources to recovery. This could be a numeric scale (for example, 1 to 10) or a low/medium/high scale.

- Exposure level: This is the degree to which an asset is exposed to threats. This depends, at least, on how the asset is shared and also may depend on other factors.

Table 3.4, from the ISACA document "Security Risk Management" [RITC13], is a simplified example of the type of elements that should go into an asset register.

TABLE 3.4 Example Asset Register

Asset Name/Description	Asset Classification	Disaster Recovery Priority	Description	Exposure Level
Personnel	High	1	Employees	Medium
Client PII	High	1	Personally identifiable information	Low
Production web server	Medium	1	Company primary website (no sensitive data)	High

Threat Identification

Threat identification is the process of identifying threat sources with the potential to harm system assets. Threat sources are categorized into three areas:

Environmental: Examples include floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and power failure.

Business resources: Examples include equipment failure, supply chain disruption, and unintentional harm caused by employees.

Hostile actors: Examples include hackers, hacktivists, insider threats, criminals, and nation-state actors.

Both environmental and business resource threats must be recognized and addressed, but the bulk of the effort of threat identification—and indeed of risk assessment and risk management—involves dealing with threats from hostile actors. That is the focus of this section.

The STRIDE Threat Model

STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions [HERN06]. It involves the following categories:

- Spoofing identity: An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password. Security controls to counter such threats are in the area of authentication.
- Tampering with data: Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and alteration of data as it flows between two computers over an open network, such as the Internet. Relevant security controls are in the area of integrity.
- Repudiation: Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise (for example, a user performing an illegal operation in a system that lacks the ability to trace the prohibited operations). Relevant security controls are in the area of non-repudiation, which refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user received the package.
- Information disclosure: Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it (for example, the ability of users to read a file that they were not granted access to or the ability of an intruder to read data in transit between two computers). Relevant security controls are in the area of confidentiality.

- Denial of service: Denial-of-service (DoS) attacks deny service to valid users—for example, by making a web server temporarily unavailable or unusable. Relevant security controls are in the area of availability.
- Elevation of privilege: In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself—a dangerous situation indeed. Relevant security controls are in the area of authorization.

Threat Types

Many efforts have been made to categorize types of threats, and there is considerable overlap in the definition of some common terms. A large category of threat is malicious software, or malware, which is a general term encompassing many types of software threats, including the following:

- Malware: Malicious software. This is a general term encompassing many types of threats, including the ones listed here.
- Virus: Malware that, when executed, tries to replicate itself into other executable code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
- Worm: A computer program that runs independently and propagates a complete working version of itself onto other hosts on a network.
- Ransomware: A type of malware that tries to extract a ransom payment in exchange for unblocking access to an asset that belongs to the victim or in exchange for a promise not to release the data captured by the ransomware.
- Spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- Logic bomb: A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
- Trojan horse: A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
- Backdoor (trapdoor): Any mechanisms that bypass a normal security check; it may allow unauthorized access to functionality.
- Mobile code: Software (for example, scripts, macros, or other portable instructions) that are shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
- Exploit: Code specific to a single vulnerability or set of vulnerabilities.
- Exploit kit: Prepackaged software made available for use by others that uses an arsenal of exploits to infect a computer. Then it typically installs malware.
- Downloader: A program that installs other items on a machine that is under attack. Usually, a downloader is sent in an email.
- Dropper: An installer that surreptitiously carries malware to be executed on the compromised machine. Droppers are often disguised and hidden in a computer's directories, so that although they are visible, they look like valid programs or file types.
- Auto-rooter: A malicious hacker tool used to break into new machines remotely.
- Kit (virus generator): A set of tools for generating new viruses automatically.

- Spammer program: A program that is used to send large volumes of unwanted email.
- Flooder: A program that is used to attack networked computer systems with a large volume of traffic to carry out a DoS attack.
- Keyloggers: Software that captures keystrokes on a compromised system.
- Rootkit: A set of hacker tools used after an attacker has broken into a computer system and gained root-level access.
- Zombie or bot: A program activated on an infected machine that launches attacks on other machines.
- Spyware: Software that collects information from a computer and transmits it to another system.
- Adware: Advertising that is integrated into software. It results in pop-up ads or redirection of a browser to a commercial site.

Other cybersecurity threat terms frequently encountered include the following:

- Remote access attacks: Attacks made across the Internet or a corporate network.
- Denial-of-service (DoS) attack: An attack that prevents authorized access to resources or the delaying of time-critical operations.
- Distributed denial-of-service (DDoS) attack: A DoS technique that uses numerous hosts to perform the attack.
- DNS attacks: Attacks that encompass a variety of exploits that subvert the functioning of the Domain Name System (DNS), which provides a mapping between hostnames and IP addresses.
- Hacker or cracker: An unauthorized user who attempts to or gains access to an information system. Sometimes a distinction is made between individuals who are essentially harmless and just curious (hacker) and individuals who break security on a system for malign purposes (cracker); in other case these two terms are considered equivalent.
- Injection flaw: A vulnerability that is created from insecure coding techniques and results in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system.
- Code injection: Insertion of malicious code by exploiting an injection flaw.
- Social engineering: A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.
- Phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake website that requests information.
- Password attack: A method of accessing an obstructed device, using one of various methods, by capturing the user ID/password of a validated user.
- Website exploit: An attack that inserts malicious code on a web server, either to attack the server itself or as a means of attacking source systems of users who access the website.

These lists are not exhaustive but give you an idea of the scale of the challenge organizations face.

Sources of Information

Information on environmental threats is typically available from a variety of government and trade groups. Threats related to business resources are less easily documented but still generally can be predicted with reasonable accuracy. It is difficult to get reliable information on past events and to assess future trends for a variety of reasons, including the following:

- Organizations are often reluctant to report security events in an effort to save corporate image, avoid liability costs, and, in the case of responsible management and security personnel, avoid career damage.
- Some attacks may be carried out or at least attempted without being detected by the victim until much later, if ever.
- Threats continue to evolve as adversaries adapt to new security controls and discover new techniques.

Thus, keeping informed on threats is an ongoing and never-ending battle. The following discussion examines three important categories of threat information sources: in-house experience, security alert services, and global threat surveys.

An important source of information on threats is the experience an organization has already had in identifying attempted and successful attacks on its assets. An organization can obtain this information through an effective security monitoring and improvement function, as discussed in Chapter, “Security Monitoring and Improvement.” However, this information is of more value for threat and incident management, described in Chapter, “Threat and Incident Management,” “than for risk assessment. That is, detected attacks should prompt immediate remedial action rather than be folded into long-range actions.

Security alert services are concerned with detecting threats as they develop to enable organizations to patch code, change practices, or otherwise react to prevent a threat from being realized. Again, this category of information is of more value for threat and incident management, and these sources are addressed in Chapter.

Of great value for threat identification is the various global threat surveys that are readily available. The most important global threat survey are examined in this section.

Verizon Data Breach Investigations Report

Perhaps the most important source of information that an organization can consult is the annual Verizon Data Breach Investigations Report (DBIR). This authoritative and highly respected report is based on data on security incidents systematically collected from a wide variety of organizations. The results in the 2018 report are based on data from more than 53,000 security incidents and over 2,200 data compromises from 65 countries and 67 organizations. The results are broken down by 20 industry sectors, such as accommodation, entertainment, finance, healthcare, manufacturing, public, and utilities. Further, threats are broken down along three dimensions:

- Pattern: This includes DoS, privilege misuse, lost and stolen assets, point of sale, miscellaneous errors, web app attacks, crimeware, payment care skimmers, and cyber-espionage.
- Action: This includes hacking, malware, social breach, error, misuse, physical breach, and environmental-based damage.
- Asset: This includes servers, media, user devices, persons, networks, kiosks/terminals, and embedded devices (for example, Internet of Things [IoT] devices).

Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Along each dimension, the number of security incidents and breaches are reported for each industry sector. The DBIR defines a security incident as a security event that compromises the integrity, confidentiality, or availability of an information asset. It defines a breach as an incident that results in

the confirmed disclosure—not just potential exposure—of data to an unauthorized party. The report also summarizes, with data, key aspects of the attack, including the following:

- Actors: Broken down into the categories outsiders, internal actors, state-affiliated actors, multiple parties, partners, and organized criminal groups.
- Tactics: Includes hacking, malware, leveraging stolen and/or weak passwords, social attacks, errors, privilege misuse, and physical actions.
- Other common factors: Includes malware installed via malicious email attachments, financially motivated breaches, related to espionage, and discovered by third parties.

Other more detailed breakdowns of types of attacks are included in DBIR. With this wealth of high-quality data, the DBIR is an essential tool in the threat identification process.

Threat Horizon Report

A useful complement to the DBIR is the annual Threat Horizon Report from the ISF. It differs from the DBIR in two ways. First, it is a more broad-brush treatment, identifying key threat trends rather than detailed threats and detailed target profiles. Second, the Threat Horizon Report attempts to project the likely major threats over the next two years.

ISF Threat Horizon Report https://www.securityforum.org/research/threat-horizon-2on-deterioration/

The latest report, Threat Horizon 2019, highlights nine major threats, broken down into three challenging themes, that organizations can expect to face over the next two years as a result of increasing developments in technology. These are the key themes and challenges in the latest report are:

Disruption: Disruption is likely due to an over-reliance on fragile connectivity requiring a seismic shift in the way business continuity is planned, practiced, and implemented. The major threats are:

- Premeditated Internet outages bringing trade to its knees
- Ransomware hijacks on the IoT
- Privileged insiders being coerced into giving up the crown jewels

Distortion: As trust in the integrity of information is lost, the monitoring of access and changes to sensitive information become critical, as does the development of complex incident management procedures. The major threats are:

- Automated misinformation gaining instant credibility
- Falsified information compromising performance
- Subverted blockchains shattering trust

Blockchain

A data structure that makes it possible to create a digital ledger of transactions and share it among a distributed network of computers. Blockchain technology includes protocols and formats that provide for the secure update of and access to the ledger.

Deterioration: Controls may be eroded by regulations and technology bringing a heightened focus on risk assessment and management in light of regulatory changes and the increased prevalence of artificial intelligence in everyday technology. The major threats are:

- Surveillance laws exposing corporate secrets
- Privacy regulations impeding the monitoring of insider threats
- A headlong rush to deploy artificial intelligence (AI) leading to unexpected outcomes

The Threat Horizon Report includes detailed recommendations for countering each threat. The report states that many of the recommendations can be quickly and easily implemented over the next two years.

ENISA Threat Landscape Report

Another very useful source of information is several threat documents from European Union Agency for Network and Information Security (ENISA). One of these is the ENISA Threat Taxonomy (2016), which provides a very detailed breakdown of potential cybersecurity threats. It is organized into a three-level hierarchy of high-level threats, threats, and threat details, and defines dozens of individual threat categories. It provides is a useful checklist for ensuring that an organization considers the full range of threats.

A useful source of information on current threats is the ENISA Threat Landscape Report, most recently published in January 2018 [ENIS18]. Table 3.5 summarizes the results of the report. The 15 threats are ranked according to the volume of security incidents surveyed, and the Trend column refers to the relative change in the severity of consequences from each threat. For each threat, the report provides a kill chain for each specific threat, which defines the phases of a cyber attack.

TABLE 3.5 Top Cybersecurity Threats Reported by ENISA

Threat	Trend
1. Malware	Stable
2. Web-based attacks	Increasing
3. Web application attacks	Increasing
4. Phishing	Increasing
5. Spam	Increasing
6. DoS attacks	Increasing
7. Ransomware	Increasing
8. Botnets	Increasing
9. Insider threats (malicious, accidental)	Stable
10. Physical manipulation/damage/theft/loss	Stable
11. Data breaches	Increasing
12. Identity theft	Increasing
13. Information leakage	Increasing
14. Exploit kits	Declining
15. Cyber espionage	Increasing

kill chain

A systematic process used to target and engage an adversary to create desired effects. In the context of cybersecurity, it consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action.

The phases of the kill chain are as follows [MYER13, ENGE14]:

- Reconnaissance: The adversary determines likely targets for attack. This includes determining what information is available for targeting as well as what means are promising for targeting. For example, if names and contact details of employees are online, these could be used for social engineering purposes (for example, getting people to divulge usernames or passwords).

- Weaponization: The adversary couples an exploit with a means of gaining access to the specific system to be attacked. The result is a malicious payload, which is constructed on the attacker side, without access to the victim's system.
- Delivery: Weaponized payload is delivered to the victim via email, web access, USB, or other means.
- Exploit: The delivered bundle exploits a vulnerability to enable installation. This is relevant only when the attacker uses an exploit.
- Installation: The malware package is installed on the asset. This step is relevant only if malware is part of the threat.
- Command and control: Once a threat is in an organization's system, the attacker creates a command and control channel to be able to operate the malware remotely.
- Actions: With command and control in place, the threat can be activated to achieve the goals of the attack, which could be to obtain data, do damage, or make a ransom demand.

European Union Agency for Network and Information Security **https://www.enisa.europa.eu**

The kill chain is useful for selecting security controls to counter a particular threat. However, as [ENGE14] points out, the kill chain focuses mostly on intrusion prevention, and only the last step is relevant to intrusion detection and recovery. Thus kill chain analysis needs to be balanced with other threat intelligence.

Trustwave Global Security Report

https://www.trustwave.com/Resources/Global-Security-Report-Archive/Trustwave Global Security Report

The Trustwave Global Security Report is a well-regarded annual survey of the cyberthreat landscape. The report is based on findings from extensive data sources, including breach investigations, global threat intelligence, product telemetry, and a number of research sources. Trustwave operates a number of security operations centers (SOCs) as a managed security service and from them has logged billions of security and compliance events each day, examined data from tens of millions of network vulnerability scans, and conducted thousands of penetration tests. Its infographic style makes the Trustwave Global Security Report easy to follow, yet it contains an extraordinary amount of detailed information that can assist in threat assessment and risk treatment [RUBE14]. The key features include the following:

- Breakdown by type of data or other asset targeted, such as credit card data
- Median time between intrusion and detection
- Breakdown by vulnerability and exploitation, such as zero-day attacks on Adobe Flash Player, RIG exploit kit originating from malicious advertisements, and web attacks targeting WordPress
- Breakdown by method of intrusion, including remote access, SQL injection, misconfiguration, file upload, phishing/social engineering, malicious insider, code injection, and weak passwords

security operations center (SOC)

A facility that tracks and integrates multiple security inputs, ascertains risk, determines the targets of an attack, contains the impact of an attack, and recommends and/or executes responses appropriate to any given attack. In some cases, an organization establishes a SOC for itself. In other cases, SOC services are outsourced to a private company that specializes in providing such services.

The report also provides a detailed breakdown of how various attacks are carried out and provides examples of existing malware currently operating. It also looks at the specific state of security in the areas of network, database, and application security. The report is detailed enough to provide specific guidance to security planners and managers.

Cisco Annual Cybersecurity Report

The Cisco Annual Cybersecurity Report is yet another excellent source of threat information. The report is approximately organized along the lines of kill chain concepts. The report provides a detailed description of current attacker behavior patterns and also highlights coming vulnerabilities.

Cisco Annual Cybersecurity Report

http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

Fortinet Threat Landscape Report

The findings in the Fortinet Threat Landscape Report represent the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of network devices/sensors within production environments. This comprises billions of threat events and incidents observed in live production environments around the world, reported quarterly. Three measures are reported:

- Volume: Measure of overall frequency or proportion; the total number or percentage of observations of a threat event.
- Prevalence: Measure of spread or pervasiveness across groups; the percentage of reporting organizations that observed the threat event at least once.
- Intensity: Measure of daily volume or frequency; the average number of observations of a threat event per organization per day.

Fortinet Threat Landscape Report

https://fortinet.com/fortiguard/threat-intelligence/threat-landscape.html

The detailed results are reported in aggregate and also broken down by region and by industry.

Control Identification

Controls for cybersecurity include any process, policy, procedure, guideline, practice, or organizational structure that modifies information security risk. Controls are administrative, technical, management, or legal in nature. Control identification is defined in ISO 27005 as the process of identifying existing and planned security controls, and suggests the following steps:

Review documents containing information about the controls (for example, risk treatment implementation plans). If the processes of information security management are well documented, all existing or planned controls and the status of their implementation should be available.

Check with the people with responsibility related to information security (e.g., security manager, building manager, and operations manager) and the users about which controls are really implemented for the information process or information system under consideration.

Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented to determine whether they are working correctly and effectively.

Review results of audits.

This section provides a brief overview of the types of controls that may be contemplated. Details of these and other controls are provided in the appropriate chapters of this book. There are several particularly useful sources of information on security controls: SP 800-53, Center for Internet Security (CIS), ISO 27002, FAIR, and NISTIR 7621, introduced in the following paragraphs.

Online Catalog of Security Controls https://nvd.nist.gov/800-53/

SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, provides an invaluable and extraordinarily detailed discussion of controls and should be consulted in the development of any risk treatment plan. This 450-page document provides plenty of guidance on the overall development of a treatment plan and includes a 233-page catalog of security controls (also available online) and a 55-page catalog of privacy controls. The security control catalog is organized according to the degree of impact each control addresses and includes 115 low-impact controls, 159 moderate-impact controls, and 170 high-impact controls. The controls are organized into the following families:

- AC: Access Control
- AU: Audit and Accountability
- AT: Awareness and Training
- CM: Configuration Management
- CP: Contingency Planning
- IA: Identification and Authentication
- IR: Incident Response
- MA: Maintenance
- MP: Media Protection
- PS: Personnel Security
- PE: Physical and Environmental Protection
- PL: Planning
- PM: Program Management
- RA: Risk Assessment
- CA: Security Assessment and Authorization
- SC: System and Communications Protection
- SI: System and Information Integrity
- SA: System and Services Acquisition

For each control, the catalog provides a description of the control, supplemental guidance on implementation, a description of control enhancements, and references to other documents.

Also worthwhile is the CIS Critical Security Controls for Effective Cyber Defense, described in Section 1.7. Table 1.10 in Chapter 1 provides the current list that CIS considers most important: 20 controls that encompass the broad range of known threats and the state of the art in countering those threats. There is also a companion document, A Measurement Companion to the CIS Critical Security Controls, that describes in detail techniques for measuring the performance of a given sub-control, plus a set of three risk threshold values (lower, moderate, and higher).

ISO 27002, Code of Practice for Information Security Controls, is a document with a well-organized list of controls (refer to Table 1.4 in Chapter 1), together with guidance on the implementation of each control.

For purposes of risk assessment, it is useful to group security controls in a manner that reflects the risk assessment process. The FAIR (Factor Analysis of Information Risk) risk analysis document, which is described in Section 3.6, groups controls into four categories.

Avoidance controls: These controls, which include the following, affect the frequency and/or likelihood of encountering threats:

- Firewall filters
- Physical barriers
- The relocation of assets

The reduction of threat populations (for example, reducing the number of personnel who are given legitimate access to assets)

Deterrent controls: These controls, which include the following, affect the likelihood of a threat acting in a manner that results in harm (probability of action):

- Policies
- Logging and monitoring
- Enforcement practices

Asset hardening (for example, many threat actors are opportunistic in nature and gravitate toward easier targets, rather than targets that are perceived to be difficult)

- Physical obstacles (for example, external lights on building, barbed-wire fencing)

Vulnerability controls: These controls, which include the following, affect the probability that a threat's action will result in loss (vulnerability):

- Authentication
- Access privileges
- Patching
- Configuration settings

Responsive controls: These controls, which include the following, affect the amount of loss that result from a threat's action (loss magnitude):

- Backup and restore media and processes
- Forensics capabilities
- Incident response processes
- Credit monitoring for persons whose private information has been compromised

The following useful checklist of controls is also provided in NISTIR 7621:

Identity

- Identify and control who has access to your business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for information security

Protect

- Limit employee access to data and information
- Install surge protectors and uninterruptible power supplies (UPSs)
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

Detect

- Install and update antivirus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs

Respond

- Develop a plan for disasters and information security incidents (for example, incident response plan)

Recover

- Make full backups of important business data/information
- Make incremental backups of important business data/information
- Consider cyber insurance
- Make improvements to processes/procedure/technologies

The FAIR and NISTIR 7621 lists of controls provided here give you with some idea of the scale of the work involved in implementing an effective suite of security controls. Parts II, “Managing the Cybersecurity Function,” and III, “Security Assessment,” of this book discuss security controls in detail.

Vulnerability Identification

Vulnerability identification is the process of identifying vulnerabilities that can be exploited by threats to cause harm to assets. A vulnerability is a weakness or a flaw in a system’s security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited when a threat is manifested.

The following sections develop categories of vulnerabilities, discuss approaches to identifying and documenting vulnerabilities, and discuss the use of the National Vulnerability Database.

Vulnerability Categories

Vulnerabilities occur in the following areas:

- Technical vulnerabilities: Flaws in the design, implementation, and/or configuration of software and/or hardware components, including application software, system software, communications software, computing equipment, communications equipment, and embedded devices.
- Human-caused vulnerabilities: Key person dependencies, gaps in awareness and training, gaps in discipline, and improper termination of access.
- Physical and environmental vulnerabilities: Insufficient physical access controls, poor siting of equipment, inadequate temperature/humidity controls, and inadequately conditioned electrical power.
- Operational vulnerabilities: Lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents, and inadequate monitoring and evaluation of the effectiveness of security controls.
- Business continuity and compliance vulnerabilities: Misplaced, missing, or inadequate processes for appropriate management of business risks; inadequate business continuity/contingency planning; and inadequate monitoring and evaluation for compliance with governing policies and regulations.

In many of the areas listed here, vulnerability identification depends critically on management initiative and follow-through. Techniques such as interviews, questionnaires, review of previous risk assessments and audit reports, and checklists all contribute to developing a good picture of the vulnerability landscape.

National Vulnerability Database and Common Vulnerability Scoring System

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive. An outstanding resource is the NIST National Vulnerability Database (NVD) and the related Common Vulnerability Scoring System (CVSS) [FIRS15], described in NISTIR 7946, CVSS Implementation Guidance. The NVD is a comprehensive list of known technical vulnerabilities in systems, hardware, and software. The CVSS provides an open framework for communicating the characteristics of vulnerabilities. The CVSS defines a vulnerability as a bug, a flaw, a weakness, or an exposure of an application, a system device, or a service that could lead to a failure of confidentiality, integrity, or availability. The CVSS model attempts to ensure repeatable and accurate measurement while enabling users to view the underlying vulnerability characteristics used to generate numeric scores. The CVSS provides a common measurement system for industries, organizations, and governments requiring accurate and consistent vulnerability exploit and impact scores.

It is worthwhile to gain an understanding of the CVSS in order to understand the wide range of vulnerabilities that affect systems. In addition, the systematic scheme for evaluating vulnerabilities in

the CVSS is useful in guiding the development of a similar systematic approach to other vulnerabilities such as those related to organizational issues, policies and procedures, and physical infrastructure. CVSS is widely accepted and used. For example, the Payment Card Industry Data Security Standard (PCI DSS) standard recommends use of CVSS.

NIST National Vulnerability Database **https://nvd.nist.gov**

Figure 3.4 provides an example of one of the vulnerability entries in the NVD.

Current Description
An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.
Source: MITRE **Last Modified:** 02/01/2017 View Analysis Description

CVSS Severity (version 3.0):
CVSS v3 Base Score: 8.8 High
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 2.8

Quick Info
CVE Dictionary Entry: CVE-2017-3823
Original release date: 02/01/2017
Last revised: 04/04/2017
Source: US-CERT/NIST

CVSS Version 3 Metrics:
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

FIGURE 3.4 NVD Scoring Example

Each NVD entry includes the following:

- The unique Common Vulnerabilities and Exposure (CVE) dictionary identifier
- A description of the vulnerability
- Links to websites and other references with information related to the vulnerability
- CVSS metrics

There are 14 CVSS metrics in three groups. Table 3.6 lists the individual metrics and shows the levels defined for each one. In each case, the levels are listed from highest to lowest security concern. In

essence, the scoring is done as follows: For each identified vulnerability, the NVD provides a level for each metric in the base group, based on the characteristics of the vulnerability. For example, the attack vector metric indicates whether the attack can be launched remotely over a network or over the Internet, is launched only across the immediate network to which both the attack source and the target system are attached, must be done by a local login, or requires physical access to the machine. The more remote the attack, the more attack sources are possible, and therefore the more serious the vulnerability. This information is invaluable in enabling users to understand the characteristics of a vulnerability.

TABLE 3.6 CVSS Metrics

Base Metric Group		Temporal Metric Group	Environmental Metric Group
Exploitability	Impact		
Attack Vector ▪ Network ▪ Adjacent ▪ Local ▪ Physical **Attack Complexity** ▪ Low ▪ High **Privileges Required** ▪ None ▪ Low ▪ High **User Interaction** ▪ None ▪ Required	**Confidentiality Impact** ▪ High ▪ Low ▪ None **Integrity Impact** ▪ High ▪ Low ▪ None **Availability Impact** ▪ High ▪ Low ▪ None	**Exploit Code Maturity** ▪ Not defined ▪ High ▪ Functional ▪ Proof-of-concept ▪ Unproven **Remediation Level** ▪ Not defined ▪ Workaround ▪ Temporary fix ▪ Official fix **Report Confidence** ▪ Not defined ▪ Confirmed ▪ Reasonable ▪ Unknown	**Confidentiality Requirement** ▪ Not defined ▪ High ▪ Medium ▪ Low **Integrity Requirement** ▪ Not defined ▪ High ▪ Medium ▪ Low **Availability Requirement** ▪ Not defined ▪ High ▪ Medium ▪ Low
Scope ▪ Unchanged ▪ Changed			

As Table 3.6 shows, each level of a metric has a descriptive name. In addition, the CVSS assigns a numeric value on a scale of 0.0 to 10.0, with 10.0 being the most severe security issue. The numeric scores for the metrics in the base metric group are put into an equation defined in the CVSS that produces an aggregate base security score ranging from 0.0 to 10.0 (see Figure 3.4).

The base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It consists of three sets of metrics:

- Exploitability: These metrics reflect the ease and technical means by which the vulnerability is exploited. The metrics are:
- Attack vector: As mentioned, this metric is a measure of how remote an attacker can be from the vulnerable component.

- Attack complexity: Conveys the level of difficulty required for an attacker to exploit a vulnerability once the target component is identified. The complexity is rated high if the attacker cannot accomplish the attack at will but must invest some measurable amount of effort in preparation or execution.
- Privileges required: Measures the access an attacker requires to exploit a vulnerability. The values are none (no privileged access required), low (basic user privileges), and high (administrative-level privileges).
- User interaction: Indicates whether a user other than the attacker must participate for a successful attack.
- Impact: These metrics indicate the degree of impact on the primary security objectives confidentiality, integrity, and availability. In each of these cases, the score reflects the worst outcome if more than one component is affected (scope = changed). For each of the three objectives, the values are high (total loss of confidentiality, integrity, or availability), low (some loss), and none.
- Scope: This metric is grouped within the base metric group although it is somewhat independent of the remainder of the group. It refers to the ability for a vulnerability in one software component to impact resources beyond its means, or privileges. An example is a vulnerability in a virtual machine that enables an attacker to delete files on the host operating system. An unchanged value of this metric means that the vulnerability can only affect resources managed by the same authority.

Generally, the base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically have better information about the characteristics of a vulnerability than do users. The environmental metrics, however, are specified by users because they are best able to assess the potential impact of a vulnerability within their own environments.

The temporal metric group represents the characteristics of a vulnerability that change over time but not among user environments. It consists of three metrics. In each case, the value “not defined” indicates that this metric should be skipped in the scoring equation.

- Exploit code maturity: This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability. The levels reflect the degree to which the exploit is available and usable for exploiting the vulnerability.
- Remediation level: Measures the degree to which remediation is available.
- Report confidence: Measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.

The environmental metric group captures the characteristics of a vulnerability that are associated with a user’s IT environment. It enables the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user’s organization, measured in terms of confidentiality, integrity, and availability.

Risk Assessment Approaches

This section begins with a discussion of the distinction between quantitative and qualitative risk assessment. This is followed by discussion of a simple approach to risk assessment. Finally, this section provides an overview of FAIR, which is referenced several times elsewhere in this chapter.

Quantitative Versus Qualitative Risk Assessment

Two factors of risk assessment can be treated either quantitatively or qualitatively: impact and likelihood. For impact, if it seems feasible to assign a specific monetary cost to each of the impact areas, then the overall impact can be expressed as a monetary cost. Otherwise, qualitative terms, such as low, moderate, and high, are used. Similarly, the likelihood of a security incident may be determined quantitatively or qualitatively. The quantitative version of likelihood is simply a probability value, and again the qualitative likelihood can be expressed in such categories as low, medium, and high.

Quantitative Risk Assessment

If all factors are expressed quantitatively, then it is possible to develop a formula such as the following:

Level of risk = (Probability of adverse event) × (Impact value)

This is a measure of the cost of security breaches, expressed numerically. It can also be expressed as a residual risk level as follows:

$$\text{Residual risk level} = \frac{(\text{Probability of adverse event})}{(\text{Mitigation factor})} \times (\text{Impact value})$$

An equation reads, Residual risk level equals ((Probability of adverse event) over (Mitigation factor)) times (Impact value).

In this equation, the mitigation factor reflects the reduction in the probability of an adverse event due to the implementation of security controls. Thus, the residual risk level is equivalent to the expected cost of security breaches with the implementation of controls.

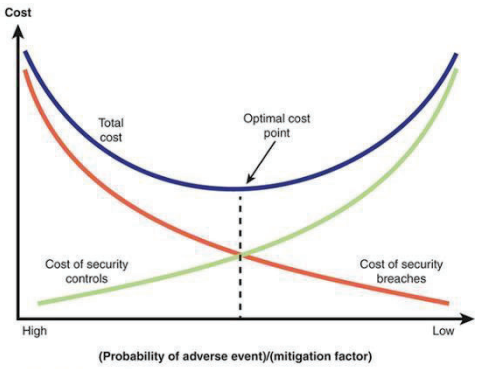


FIGURE 3.5 Cost Analysis for Risk Assessment

If the various factors can be quantified with a reasonable degree of confidence, then these equations should be used to guide decisions concerning how much to invest in security controls. Figure 3.5 illustrates this point: As new security controls are implemented, the residual probability of an adverse event declines and, correspondingly, the cost of security breaches declines. However, at the same time, the total cost of security controls increases as new controls are added. The upper curve represents the total security cost, consisting of the cost of security breaches plus the cost of security controls. The optimal cost point occurs at the lowest point of the total cost curve. This represents a level of risk that is tolerable and cannot be reduced further without the expenditure of costs that are disproportionate to the benefit gained.

Qualitative Risk Assessment

It is not reasonable to suppose that all impact costs and likelihoods can with confidence be expressed quantitatively. Security breaches are rare, and organizations are reluctant to reveal them. Consequently, security incidence information is typically anecdotal or based on surveys and cannot be used to develop reliable or accurate probability or frequency values. At the same time, the total cost or potential loss due to a security breach is hard to quantify. The cost may depend on a variety of factors, such as length of downtime, amount and effect of adverse publicity, cost to recover, and other factors that are difficult to estimate.

However, it is possible, using reasonable judgment, to use qualitative risk assessment effectively. Qualitative assessment determines a relative risk rather than an absolute risk. This considerably simplifies the analysis, producing rough estimates of risk levels. Qualitative risk assessment is usually sufficient for identifying the most significant risks and allowing management to set priorities for security expenditures with a reasonable degree of confidence that all the significant risks have been mitigated. Table 3.7 compares quantitative and qualitative risk assessment.

TABLE 3.7 Comparison of Quantitative and Qualitative Risk Assessment

	Quantitative	Qualitative
Benefits	▪ Risks are prioritized by financial impact; assets are prioritized by financial values. ▪ Results facilitate management of risk by return on security investment. ▪ Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage). ▪ Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	▪ It enables visibility and understanding of risk ranking. ▪ It is easier to reach consensus. ▪ It is not necessary to quantify threat frequency. ▪ It is not necessary to determine financial values of assets. ▪ It is easier to involve people who are not experts on security or computers.
Drawbacks	▪ Impact values assigned to risks are based on subjective opinions of participants. ▪ The process to reach credible results and consensus is very time-consuming. ▪ Calculations can be complex and time-consuming. ▪ Results are presented in monetary terms only, and they may be difficult for nontechnical people to interpret. ▪ The process requires expertise, so participants cannot be easily coached through it.	▪ There is insufficient differentiation between important risks. ▪ It is difficult to justify investing in control implementation because there is no basis for a cost/benefit analysis. ▪ Results are dependent upon the quality of the risk management team that is created.

Note in Table 3.7 that "impact values assigned to risks are based on subjective opinions of participants" is listed as a drawback of quantitative risk assessment. This is because it is not feasible to predict the cost of an impact within tight quantitative values. The official or group involved must make a subjective assessment of what the quantitative value will be for some future event. Disregarding this limitation may lead to a false impression of the accuracy of quantitative risk assessment. It is also true that subjective opinions are used to make a qualitative estimate of impact, but in this latter case, it is clear that subjective estimates are inherent in the process.

An organization needs some clearly defined categories of impact, threat, and vulnerability. For impact, FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, defines three security categories based on the potential impact on an organization should certain events occur that jeopardize the IT assets needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The categories are as follows:

Low: Expected to have a limited adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
- Result in minor damage to organizational assets
- Result in minor financial loss
- Result in minor harm to individuals

Moderate or medium: Expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
- Result in significant damage to organizational assets
- Result in significant financial loss
- Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries

High: Expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, including the following:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
- Result in major damage to organizational assets
- Result in major financial loss
- Result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, provides a number of examples of qualitative impact assessment. For example, say that a law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(confidentiality, HIGH), (integrity, MODERATE), (availability, MODERATE)}.

Similarly, ranges of probability are assigned to qualitative likelihood categories. SP 800-100, Information Security Handbook: A Guide for Managers, suggests the following categories:

Low: ≤0.1
Medium: 0.1 to 0.5
High: 0.5 to 1.0

Another possible categorization is based on an estimate of the number of times per year an event occurs:

Low: <1 time per year
Medium: 1 to 11 times per year
High: >12 times per year

With these categories in mind, Figure 3.6 illustrates the use of matrices to determine risk. The vulnerability to a particular threat is a function of the capability, or strength, of the threat and the resistance strength of a system or an asset to that particular threat. Then, the likelihood of an adverse security event causing a particular threat is a function of the frequency, or likelihood, of the threat occurring and the vulnerability to that threat. Impact is determined as a function of asset class and the exposure to loss that a particular threat could cause. For example, assets can be classified in terms of the business impact of a loss.

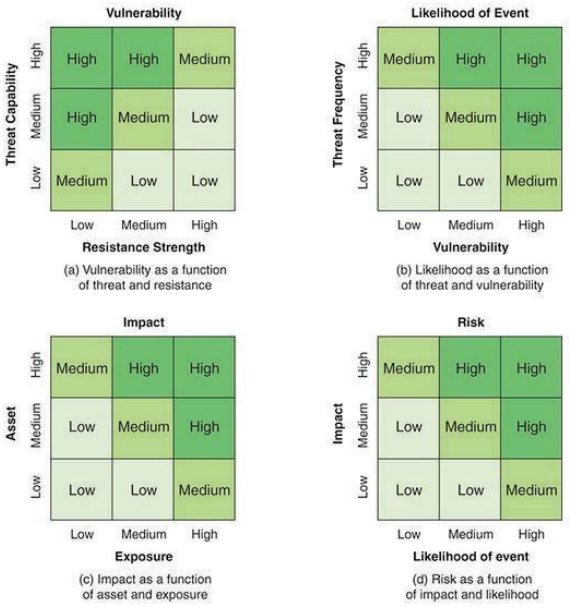


FIGURE 3.6 Qualitative Risk Determination

Review of Enterprise Security Risk Management [HIRT15] suggests the following classification examples:

- Low business impact: Public information, high-level information
- Medium business impact: Network designs, employee lists, purchase order information
- High business impact: Financial data, personally identifiable information (PII), Social Security numbers, medical record information

personally identifiable information (PII)

Information used to distinguish or trace an individual's identity, such as name, Social Security number, or biometric records, either alone or when combined with other information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so on.

Review of Enterprise Security Risk Management [HIRT15] also suggests the following exposure examples:

- Low asset exposure: Minor or no loss
- Medium asset exposure: Limited or moderate loss
- High asset exposure: Severe or complete loss

Finally, risk is determined as a function of impact and the likelihood of an adverse event that causes the impact. Thus, these matrices, coupled with an informed estimate of low, medium, and high for the various factors, provide a reasonable means of assessing risk.

It should be kept in mind, however, that results of such a coarse-grained analysis must be subject to judgment. For example, in Figure 3.6d, a low-likelihood, high-impact breach and a high-likelihood, low-impact breach are both rated as medium risk. Which should be given priority for scarce security resources? On average, each type of breach may be expected to yield the same amount of annual loss. Is it more important to deal with the former breach—because although rare, if it does occur, it could

be catastrophic for the organization—or deal with the latter type—which could produce a steady stream of losses. That is for management to decide.

Simple Risk Analysis Worksheet

A simple approach to risk assessment is to use a risk analysis worksheet, which is a table with one row for each potential threat/vulnerability pair [GADS06]. This worksheet, prepared by the risk assessment team, contains the following columns:

- Security issue: A brief statement of each security issue or area of concern. There should be one row for each threat/vulnerability pair (as well as compliance issues, described subsequently).
- Likelihood: Estimated likelihood for an occurrence of this threat/vulnerability pair. The estimate should be based on the team's judgment of the value of the affected assets and the magnitude of the exposure, using the matrices in Figures 3.6a and 3.6b.
- Impact: Estimated impact for this threat/vulnerability pair. The estimate should be based on the team's judgment of the affected assets value of the magnitude of the exposure, using the matrix in Figure 3.6c.
- Risk level: Risk level, based on the matrix in Figure 3.6d.
- Recommended security controls: Specific security control(s) that the team is recommending to address this particular issue.
- Control priorities: Relative priority of each recommended control.
- Comments: Any other information that is considered relevant to the security risk management decision-making process for this particular security issue.

Compliance issues can be documented on the same worksheet. Compliance requirements include those imposed by the organization's security policy, government regulations, and applicable accreditation standards. Compliance should be rated as follows:

0 = not implemented
1 = partially implemented
2 = implemented but not yet documented
3 = implemented and documented

For compliance issues, the Likelihood and Impact fields are irrelevant. An issue with a compliance score of less than 3 should be included in the worksheet with a risk level of high.

MUSC Information Security Guidelines: Risk Management [GADS06] includes a number of examples of threat/vulnerability pairs, including the following:

- Security issue: An authorized employee uses the system in an unauthorized manner. Threat: Deliberate misuse of the system by an insider. Vulnerability: Inadequate training (the employee doesn't know better), or inadequate audit controls (the employee believes his misuse won't be detected), or lack of effective disciplinary process (employee believes there won't be any sanctions, even if his misuse is detected).
- Security issue: A serious, ongoing system compromise is not discovered until too late because nobody was checking up on the person who was assigned to review the system activity records that would have revealed the compromise. Threat: Deliberate unauthorized access. Vulnerability: Whatever vulnerability or vulnerabilities contributed to the original intrusion,

compounded by inadequate monitoring and evaluation of the effectiveness of the system's audit controls.

The document resource site for this book provides three examples of simple risk analyses.

Cybersecurity Book Resource Site https://app.box.com/v/ws-cybersecurity

Factor Analysis of Information Risk

An important contribution to risk assessment is Factor Analysis of Information Risk (FAIR), first introduced in 2005. FAIR, which has been standardized by The Open Group, has received wide acceptance. Its relationship to International Organization for Standardization (ISO) risk standards are summarized as follows:

- ISO 27001 describes a general process for creating an information security management system (ISMS).
- In that context, ISO 27005 defines the approach to managing risk.
- FAIR provides a methodology for analyzing risk.

The Open Group

A global consortium with more than 500 member organizations that enables the achievement of business objectives through IT standards.

Thus, FAIR provides more specific guidance that can be used within the framework defined by ISO 27005.

The Open Group has published four risk-related standards documents:

Risk Taxonomy: This standard provides a rigorous set of definitions and taxonomy for information security risk as well as information regarding how to use the taxonomy.

- Requirements for Risk Assessment Methodologies: This technical guide identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements.
- FAIR—ISO/IEC 27005 Cookbook: This technical guide describes in detail how to apply the FAIR methodology to the ISO 27005 framework.
- The Open Group Risk Analysis (O-RA) Technical Standard: This document provides a set of standards for various aspects of information security risk analysis.

Open Group Security Standards http://www.opengroup.org/standards/security

Figure 3.7 illustrates the relationships between the three risk assessment tasks in ISO 27005 and the detailed definitions of those tasks in FAIR. FAIR provides a more detailed set of guidelines for all aspects of risk assessment. For example, FAIR provides definitions of the key terms that are less vague and more specifically tied to the risk analysis process than does ISO 27005.

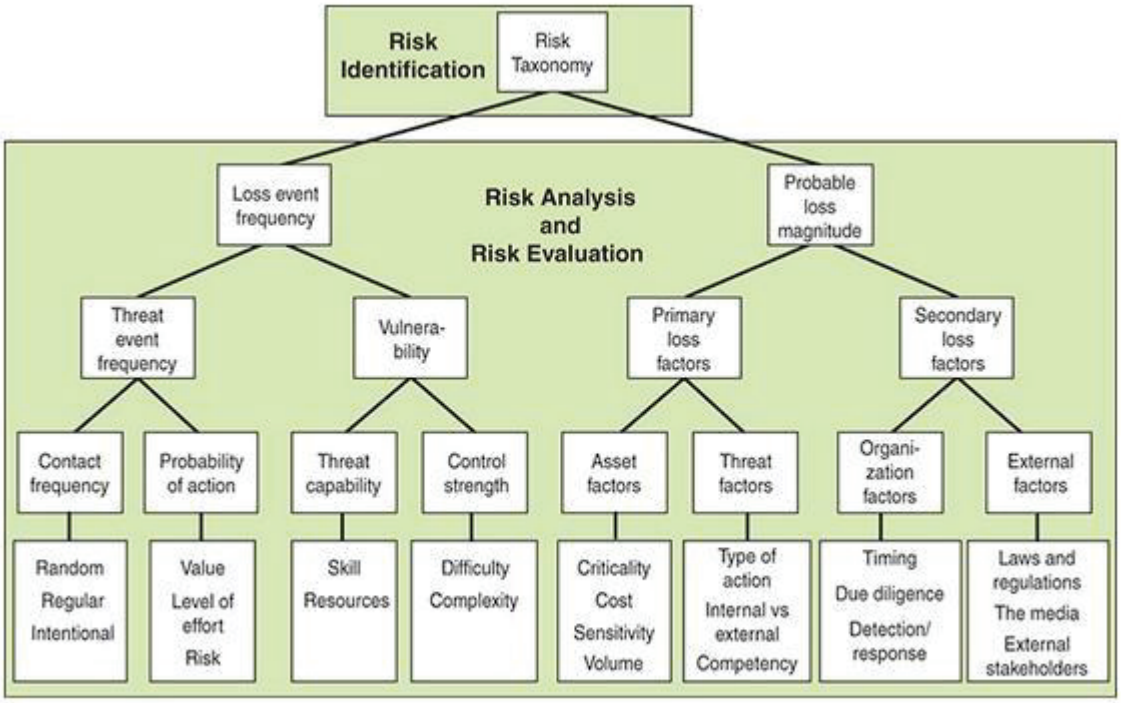


FIGURE 3.7 Risk Assessment Using FAIR

The key FAIR definitions are as follows:

- Asset: Any data, device, or other component of the environment that supports information-related activities that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.
- Risk: The probable frequency and probable magnitude of future loss.
- Threat: Anything that is capable of acting in a manner resulting in harm to an asset and/or organization—for example, acts of God (weather, geologic events, and so on), malicious actors, errors, and failures.
- Vulnerability: The probability that an asset will be unable to resist actions of a threat agent.

The FAIR methodology is based on a belief that subjective qualitative analysis is inadequate in most situations and that all risk, tangible and intangible, is measurable and quantifiable. The actual quantitative analysis results are delivered using calibrated, probabilistic estimates based on ranges of probabilities, accurate comparisons, and PERT calculations run through Monte Carlo simulations.

Both ISO 27005 and FAIR are referenced throughout this chapter.

Likelihood Assessment

In Figure 3.1, earlier in this chapter, the upper row of boxes relates to risk identification, which has been discussed in the preceding sections. The remainder of the figure relates to risk analysis, which consists of three tasks:

- Likelihood assessment
- Impact assessment
- Risk determination

This section examines likelihood assessment. Sections 3.8 and 3.9 discuss impact assessment and risk determination, respectively.

Likelihood assessment does not yield a numerical value subject to calculation using probability theory. Rather, it is the process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place. This assessment is applied to each identified potential threat action.

The essence of likelihood assessment for a given threat to a given asset is shown in the following steps:

Step 1. Determine the likelihood that a threat event will occur. That is, determine the likelihood that this threat will develop into an attack on the given asset.
Step 2. Determine the degree of vulnerability of the asset to the threat.
Step 3. Based on Step 1 and Step 2, determine the likelihood that a security incident will occur.

This analysis needs to be repeated for every threat to every asset.

ISO 27005 and other ISO documents provide limited guidance on how to perform this function. FAIR provides detailed guidance on how to systematically characterize event likelihood, referred to in the FAIR documents as loss event frequency. This guidance, although clear, is rather complex; this chapter provides an overview. As indicated in the left-hand portion of Figure 3.7, FAIR adopts a top-down approach to determining loss event frequency. At the top level, it may be possible, based on historical data, to develop an estimate of loss event frequency, simply on the basis of how frequently a loss event has occurred in the past. It is not necessary, and indeed not possible, to derive an exact frequency or probability. For one thing, a security event in the past may remain undetected at the time of the risk assessment. In addition, the past cannot be considered an exact predictor of the future. The examples in the FAIR documents use five levels (very low, low, moderate, high, very high) with an order of magnitude change between levels, as shown in Table 3.8.

TABLE 3.8 FAIR Risk Assessment Levels

Level	Loss Magnitude	Event Frequency	Threat Capability	Resistance Strength	Secondary Loss Probability
Very high (VH)	>1,000X	>100 times per year	Top 2% when compared against the overall threat population	Protects against all but the top 2% of an average threat population	90% to 100%
High (H)	100X to 1,000X	Between 10 and 100 times per year	Top 16% when compared against the overall threat population	Protects against all but the top 16% of an average threat population	70% to 90%
Moderate (M)	10X to 100X	Between 1 and 10 times per year	Average skill and resources (between bottom 16% and top 16%)	Protects against the average threat agent	30% to 70%
Low (L)	X to 10X	Between 0.1 and 1 times per year	Bottom 16% when compared against the overall threat population	Only protects against bottom 16% of an average threat population	10% to 30%
Very low (VL))	<X	<0.1 times per year (less than once every 10 years)	Bottom 2% when compared against the overall threat population	Only protects against bottom 2% of an average threat population	0% to 10%

X = monetary value assigned by organization

If the organization's management or security analysts do not have confidence that a good loss event frequency can be directly estimated, then the process is broken down into two tasks: estimating threat event frequency and estimating vulnerability.

Estimating Threat Event Frequency

The assessment of threat event frequency involves two aspects: determining the frequency with which a threat agent will come in contact with an asset and the probability that, once in contact, the threat agent will act against the asset.

Contact can be physical or logical. Physical access, for example, is possible for employees, contract workers such as cleaning and maintenance crews, and outside actors, such as clients, customers, salespeople, and inspectors. Logical access is via a network. Contact can be unplanned, or random, or it can be regular, such as with a cleaning crew, or it can be intentional, as when a hacker tries to gain logical access. The task for a security analyst is to come up with a reasonable estimate, such as using five levels (refer to Table 3.8) of frequency.

The next task is to determine the probability or likelihood that the threat agent will take action, given that contact has been made. This, of course, depends on the nature of the threat and the type of action available to the threat agent. But in general, the factors that an analyst needs to consider are the perceived value to the threat agent in performing the action, the level of effort required to perform the act, and the risk of discovery and/or punishment if the action is detected.

Based on estimates of contact frequency and probability of action, the analyst should be able to make a reasonable estimate of the threat event frequency.

Estimating Vulnerability

As with the estimation of threat event frequency, the estimation of vulnerability involves assigning relative values to two dimensions. In the case of vulnerability, the two dimensions are the threat capability and the control strength. FAIR defines threat capability as the capability of the threat community to act against an asset using a specific threat. This needs to be expressed relative to some baseline, and the technique used in FAIR is to define five levels of threat capability that describe the strength of a specific threat relative to the overall threat population (refer to Table 3.8).

Estimating vulnerability involves looking at two factors:

- Skill: The knowledge and experience of the threat agent are critical factors in the severity of the threat action. Skill is reflected in the manner in which a threat agent is able to act, such as performing social engineering or bypassing logon or other access barriers. In the case of malware, the skill applied to constructing and propagating the malware determine the severity of the threat.
- Resources: The other important factor is the resources, such as the time, financial resources, and materials that a threat agent can bring to bear.

Thus, for a given threat to a given asset, the task of an analyst is to generate a reasonable estimate using the five threat capability levels shown in Table 3.8. For software-based threats, the CVSS discussed in Section 3.5 is a useful resource.

The other dimension of vulnerability is control strength, also referred to in the FAIR documents as resistance strength; it is also called difficulty by FAIR practitioners. This dimension relates to the asset's ability to resist compromise. The FAIR approach is to define five levels of resistance strength, based on the percentage of a threat population that an asset can successfully thwart, as shown in Table 3.8. The purpose of the controls is to increase the difficulty and complexity of causing a successful threat event. The more difficult that task is, the greater the capability the threat agent must have to overcome the controls currently in place.

For a given threat to a given asset, once an analyst has developed estimates of threat capability and resistance strength, these two dimensions can be combined to produce a measure of vulnerability. This is done using the matrix shown in Figure 3.8a. (Compare this figure to Figure 3.6a.) As shown, the higher the resistance strength, the lower the vulnerability, and the higher the threat capability, the higher the vulnerability. The vulnerability values shown in the matrix are based on the experience of those involved in developing the FAIR model. For example, a high-threat capability applied to an asset with a low-resistance strength for that threat is rated as a very high vulnerability.

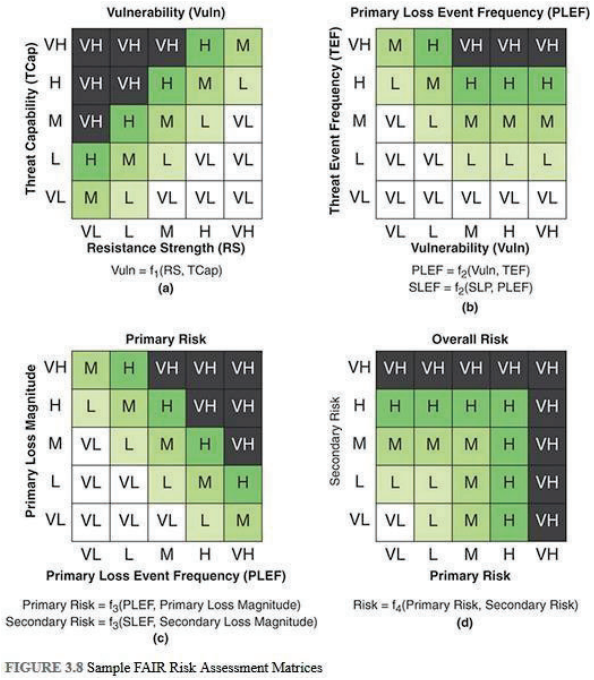


FIGURE 3.8 Sample FAIR Risk Assessment Matrices

It is worth making a distinction here between an estimated parameter and a derived parameter. Threat capability and resistance strength are parameters whose values are estimated by an analyst, which involves analytic effort. Once these two parameters are estimated, the analyst simply plugs them into the matrix to derive the desired vulnerability rating. The matrix defines a qualitative function, f1, that is expressed as:

Vulnerability = f1 (Resistance strength, Threat capability)

Loss Event Frequency

The likelihood of a loss, referred to as loss event frequency in the FAIR documents, is derived from the threat event frequency and vulnerability by using the matrix shown in Figure 3.8b. Again, the loss event frequency entries in the 5 × 5 matrix are based on judgments made by the FAIR designers. For example, if the threat event frequency is very high and the vulnerability is in the range of medium to very high, then the likelihood of a loss event is rated as very high. Note that the loss event frequency is limited by the threat event frequency; that is, the loss event frequency is never higher than the threat event frequency, no matter what the degree of vulnerability.

This matrix defines a function f2:

Primary loss event frequency = f2 (Vulnerability, Threat event frequency)

This derived quantity is also referred to as the primary loss event frequency, to contrast it with the secondary loss event frequency discussed subsequently.

SP 800-30 defines an approach to determining loss event frequency that is less complex than the FAIR approach. Table 3.9, adapted from SP 800-30, summarizes this approach. The table allows the use of either qualitative values or what the standard refers to as semi-quantitative values. This table is used both for adversarial and non-adversarial threats. The likelihood of a threat event combined with the likelihood that the threat event results in adverse impact are used as inputs to the matrix in Figure 3.8b to determine the likelihood of an adverse impact.

TABLE 3.9 Likelihood Assessment Scales

Qualitative Value	Semi-Quantitative Values	Likelihood of Threat Event Initiation (Adversarial)	Likelihood of Threat Event Occurrence (non-adversarial)	Likelihood of Threat Event Resulting in Adverse Impact
Very high	96–100	Adversary is almost certain to initiate the threat event.	Error, accident, or act of nature is almost certain to occur or occurs more than 100 times a year.	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80–95	Adversary is highly likely to initiate the threat event.	Error, accident, or act of nature is highly likely to occur or occurs between 10 and100 times a year.	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21–79	Adversary is somewhat likely to initiate the threat event.	Error, accident, or act of nature is somewhat likely to occur or occurs between 1 and10 times a year.	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5–20	Adversary is unlikely to initiate the threat event.	Error, accident, or act of nature is unlikely to occur or occurs less than once a year but more than once every 10 years.	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very low	0–4	Adversary is highly unlikely to initiate the threat event.	Error, accident, or act of nature is highly unlikely to occur or occurs less than once every 10 years.	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

Impact Assessment

Impact assessment is the process of developing some sort of agreed-upon impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action.

The essence of impact assessment is that, for a given threat to a given asset, you determine the impact (cost or relative magnitude of impact) on the asset if the threat were to become an actual security incident. This analysis needs to be repeated for every threat to every asset.

ISO 27005 and other ISO documents provide limited guidance on how to perform this function. The FAIR documents note that this is one of the most difficult aspects of risk assessment. FAIR provides detailed guidance on how to systematically characterize impact. This guidance, although clear, is rather complex, so this section provides an overview.

FAIR impact analysis depends on two categories of loss, as shown Figure 3.7 and Table 3.10.

TABLE 3.10 FAIR Loss Categories

Loss Category	Loss Factors	Forms of Loss
Primary loss	▪ **Asset:** Includes the value/liability characteristics of an asset and the volume of assets at risk ▪ **Threat:** Includes type of action, whether internal or external, and threat competence.	▪ **Productivity:** The reduction in an organization's ability to generate its primary **value proposition** (for example, income, goods, services). ▪ **Response:** Associated with managing a loss event (for example, internal or external person-hours, logistical expenses). ▪ **Replacement:** The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (for example, rebuilding a facility, purchasing a replacement laptop).
Secondary loss ▪ Secondary loss event frequency ▪ Secondary loss magnitude	▪ **Organization:** Includes timing, due diligence, type of response, and detection capability. ▪ **External:** Entities that can inflict a secondary form of harm upon the organization as a result of an event.	▪ **Competitive advantage:** Losses associated with diminished competitive advantage; associated with assets that provide competitive differentiation between the organization and its competition. Examples include trade secrets and merger and acquisition plans. ▪ **Fines/judgments:** Legal or regulatory actions levied against an organization. ▪ **Reputation:** Associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.

value proposition
A statement that identifies clear, measurable, and demonstrable benefits to consumers when they buy a particular product or service. The value proposition should convince consumers that this product or service is better than others on the market.

The two loss categories are:

- **Primary loss:** Occurs directly as a result of the threat agent's action upon the asset. The owner of the affected assets is considered the primary stakeholder in an analysis. This event affects the primary stakeholder in terms of productivity loss, response costs, and so on.
- **Secondary loss factors:** Occurs as a result of secondary stakeholders (for example, customers, stockholders, regulators) reacting negatively to the primary event. The reactions of the secondary stakeholders may, in turn, act as new threat agents against the organization's assets (such as reputation, legal fees, and so on), which, of course, affects the primary stakeholder.

Estimating the Primary Loss

For a given threat acting on a given asset, the FAIR impact (referred to as loss in the FAIR documents) assessment begins with determining the primary loss suffered as the result of the event. There are two aspects to this assessment:

- Asset factors: The value of the asset under threat.
- Threat factors: Threat factors that contribute to the loss.

The magnitude of the loss depends on a number of factors, such as how critical the asset is to the organization, the cost of replacement and/or recovery, and the sensitivity of information that might be disclosed or modified. The process of asset identification, discussed in Section 3.2, feeds into this evaluation.

The next step, for this asset and this threat, is to determine what threat action might apply to this asset. Possible actions include:

- Access: Simple unauthorized access
- Misuse: Unauthorized use of assets (for example, identity theft, setting up a pornographic distribution service on a compromised server)
- Disclosure: The threat agent illicitly disclosing sensitive information
- Modification: Unauthorized changes to an asset
- Deny access: Destruction or theft of a non-data asset

Other considerations are whether the threat agent is internal or external, which helps to indicate the motivation and intent of any threat event, and the ability of the threat agent to cause damage.

Once the asset and threat factors are understood, the analyst needs to determine the form of the loss, which includes productivity, response, and replacement (refer to Table 3.10). For each potential threat action, the analyst should estimate the probable loss magnitude for each form of loss. It is unrealistic to assign an exact monetary value to each loss. Rather, a hierarchy of levels can be used, with a monetary range for each level. The examples in the FAIR documents use five levels (very low, low, moderate, high, very high) with an order of magnitude change between levels (refer to Table 3.7). Once a loss magnitude is estimated for each form of loss, the maximum loss magnitude across all forms of loss is assigned as the primary loss magnitude for this asset and this threat.

Estimating the Secondary Loss

The estimation of secondary loss is more complex than the estimation of the primary loss. There are two components to this portion of the analysis:

- Secondary loss magnitude: Losses that are expected to materialize from dealing with secondary stakeholder reactions (for example, fines and judgments, loss of market share)
- Secondary loss event frequency: The percentage of time that a primary loss event is expected to result in a secondary loss as well

Estimating Secondary Loss Magnitude

The analysis of secondary loss magnitude proceeds in a manner similar to that for the primary loss. The analyst first determines the nature of the threat that applies in a given context and then determines the forms of loss and which form yields the greatest potential loss in this case.

Two sets of factors need to be considered in determining the nature of the threat:

- Organizational factors: Characteristics of the organization that determine the magnitude of the loss
- External factors: Entities that inflict a secondary form of harm upon the organization as a result of an event

A number of organizational factors need to be considered. For example, the timing of a security event in relationship to the organization's activities may determine how much loss is incurred. If a security event occurs just prior to a shareholders' meeting, the organization may not have time to react and resolve the problem before being held accountable by shareholders. The degree to which the organization has exercised due diligence, such as implementing a program in compliance with ISO 27001 and ISO 27002, can influence its degree of liability. The organization's ability to detect and rapidly respond contribute to its ability to contain secondary damage.

There are also external factors to consider. Laws and regulations can trigger penalties or sanctions for a security event. Public exposure of security failure can damage the organization's reputation. Customers or partners may be deterred from future business with the organization.

Once the analyst has a grasp on the secondary loss possibilities, the next step is to determine the form of the loss, which includes competitive advantage, fines/judgments, and reputation (refer to Table 3.8). For each potential threat consequence, the analyst must estimate the probable loss magnitude for each form of loss, as is done for primary losses. Once a loss magnitude is estimated for each form of loss, the maximum loss magnitude across all forms of loss is assigned as the secondary loss magnitude for this asset and this threat.

Estimating Secondary Loss Event Frequency

To derive the secondary loss frequency, the analyst first needs to estimate the probability that a secondary stakeholder would be engaged, generating some form of secondary loss. The scale shown in the last column of Table 3.7 is used. This estimate is based on analyst judgment. To carry forward the analysis, it is necessary to convert this into a secondary loss frequency, using the matrix in Figure 3.7b. In functional form:

Secondary loss event frequency = f2 (Secondary loss probability, Primary loss event frequency)

Note that this is the same matrix pattern used to evaluate the primary loss event frequency. Because a secondary loss is defined as one that may occur as a result of a primary loss, the secondary loss frequency must be less than or equal to the primary loss frequency, and this is reflected in the f2 matrix.

Business Impact Reference Table

A useful tool for performing impact assessment is the Business Impact Reference Table (BIRT). The BIRT was developed by the ISF to enable all involved in the risk assessment process to have a common view of the risk elements. The BIRT provides consistent definitions to different types of impacts and severity levels. Typically, impact types include financial loss, reputation and image damage, stakeholder impact, and regulatory/statutory violations. Severity levels range from 1 (insignificant

impact) through to 5 (catastrophic impact). The terminology in Table 3.7 indicates the type of common understanding of levels that is required.

Table 3.11 (A and B) is an example that shows part of the BIRT for a refining and marketing company specializing in premium-quality, lower-emission traffic fuels. The company has operations in 14 countries worldwide and employs some 5,000 people.

TABLE 3.11A Example Business Impact Reference Table (part 1 of 2)

Impact Type	Unforeseen Impacts of Changes in Operations or Systems	Delayed Delivery to Customers or Clients	Loss of Customers or Clients	Loss of Confidence by Key Institutions and Partners	Damage to Corporate Image and Reputation
Measure	Extent of delay or halt in operations	Extent of delay	Percentage of customers lost	Extent of loss of confidence	Extent of negative publicity
Very high	Service delayed for 24 hours	Delivery delayed by 24 hours	>25%	Complete loss of confidence	Worldwide negative publicity
High	Service delayed for 12 hours	Delivery delayed by 12 hours	11% to 25%	Serious loss of confidence	Continentwide negative publicity
Moderate	Service delayed for 4 hours	Delivery delayed by 4 hours	6% to 10%	Significant loss of confidence	Nation-wide negative publicity
Low	Service delayed for 1 hours	Delivery delayed by 1 hours	1% to 5%	Moderate loss of confidence	Local negative publicity
Very low	Service delayed for 0.5 hours	Delivery delayed by 0.5 hours	<1%	Minor loss of confidence	Minor negative publicity

TABLE 3.11B Example Business Impact Reference Table (part 2 of 2)

Impact Type	Loss of Retail Customers	Loss of b-to-b Customers	Reduction in Staff Morale/Productivity	Injury or Death
Measure	Loss of Customers	Loss of Customers	Extent of Loss of Morale/Productivity	Number of Incidents
Very HIGH	>20%	>20%	Complete loss	Multiple loss of life
High	11% to 20%	11% to 20%	Serious loss	Loss of life
Moderate	6% to 10%	6% to 10%	Significant loss	Serious harm
Low	1% to 5%	1% to 5%	Moderate loss	Moderate harm
Very low	<1%	<1%	Minor loss	Minor harm

Risk Determination

Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk. This is done separately for primary and secondary losses, and then the two are combined.

The primary risk determination is illustrated in Figure 3.8c and is expressed as:

Primary risk = f3 (Primary loss event frequency, Primary loss magnitude)

The individual matrix values are a matter of judgment, which may differ from one organization to another. The matrix f3 takes a relatively conservative view. Thus, if the loss magnitude is rated as very high, then the risk is assigned a value of very high even if the loss event frequency is only moderate. Similarly, even if the loss magnitude is rated as moderate, if the loss event frequency is rated as very high, the risk is assigned a value of very high.

The same f3 calculation is applied to secondary loss to determine the secondary risk. The two risks are then combined to determine an overall risk using the matrix in Figure 3.8d, which is expressed as:

Overall risk = f4 (Primary risk, Secondary risk)

Again, the individual matrix values are a matter of judgment. For example, a conservative view might be that if both primary and secondary risk are at the same level, the overall risk should be raised to the next level. In that case, if both risks are rated high, the overall risk is rated very high. A less conservative strategy is indicated in function f4.

Risk Evaluation

Once a risk analysis is done, senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk. This process, known as risk evaluation, involves comparing the results of risk analysis with risk evaluation criteria.

The advice provided for risk evaluation, both by ISO 27005 and the FAIR documents, is general as the criteria developed vary significantly from one organization to another. ISO does make a distinction between risk evaluation criteria and risk acceptance criteria. Evaluation criteria focus on the importance of various business assets and the impact that can be caused to the organization by various security events. The goal is to be able to specify priorities for risk treatment. Risk acceptance criteria relate to how much risk the organization can tolerate and provide guidance on how much budget can be allocated for risk treatment.

SP 800-100 provides some general guidance for evaluating risk and prioritizing action based on a three-level model:

- High: If an observation or a finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- Moderate: If an observation is rated as moderate risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
- Low: If an observation is described as low risk, the system's authorizing official must either determine whether corrective actions are still required or decide to accept the risk.

Risk Treatment

Once the risk assessment process is complete, management should have a list of all the threats posed to all assets, with an estimate of the magnitude of each risk. In addition, a risk evaluation provides input in terms of the priority and urgency with which each threat should be addressed. The response to the set of identified risks is referred to as risk treatment (or risk response), as shown in Figure 3.9.

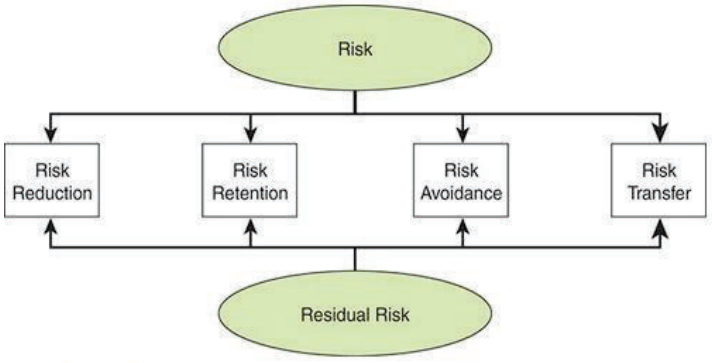


FIGURE 3.9 Risk Treatment

ISO 27005 lists these options for treating risk:

Risk reduction or mitigation: Actions taken to lessen the probability and/or negative consequences associated with a risk

- Risk retention: Acceptance of the cost from a risk

- Risk avoidance: Decision not to become involved in, or action to withdraw from, a risk situation
- Risk transfer or sharing: Sharing with another party the burden of loss from a risk

There is a many-to-many relationship between risks and treatments. A single treatment may affect multiple risks, and multiple treatments may be applied to a single risk. Further, the four options are not mutually exclusive. Multiple strategies may be adopted as part of a risk treatment plan.

Any risk treatment plan can reduce but not eliminate risk. What remains is referred to as residual risk. On the basis of the plan, the organization should update the risk assessment and determine whether the residual risk is acceptable or whether the plan needs to be updated.

Risk Reduction

Risk reduction is achieved by implementing security controls. Security controls can result in the following:

- Removing the threat source
- Changing the likelihood that the threat can exploit a vulnerability
- Changing the consequences of a security event

Part II of this book is devoted to risk reduction techniques.

Risk Retention

Risk retention, also called risk acceptance, is a conscious management decision to pursue an activity despite the risk presented or to refrain from adding to the existing controls, if any, in place to protect an asset from a given threat. This form of treatment, which is in fact non-treatment, is acceptable if the defined risk magnitude is within the risk tolerance level of the organization. In particular cases, the organization may accept risk that is greater than usually acceptable if a compelling business interest presents itself. In any case, the risk needs to be monitored and response plans that are acceptable to the stakeholders must be in place.

Risk Avoidance

If the risk in a certain situation is considered too high and the costs of mitigating the risk down to an acceptable level exceed the benefits, the organization may choose to avoid the circumstance leading to the risk exposure. This could mean, for example, forgoing a business opportunity, relocating to avoid an environmental threat or legal liability, or banning the use of certain hardware or software.

Risk Transfer

Sharing or transferring risk is accomplished by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization. This can take the form of obtaining insurance or subcontracting or partnering with another entity.

The SGP breaks down the best practices in the information risk assessment category into 2 areas and 12 topics and provides detailed checklists for each topic. The areas and topics are as follows:

Information risk assessment framework: The objective of this area is to conduct regular information risk assessments for target environments (for example, critical business environments, processes, and applications, including supporting systems/networks) in a rigorous, consistent manner, using a systematic, structured methodology.

Information risk assessment—management approach: Summarizes tasks to enable individuals who are responsible for target environments to identify key information risks, evaluate them, and determine the treatment required to keep those risks within acceptable limits.

Information risk assessment—methodology: Summarizes a systematic and structured methodology to make information risk assessments effective, easy to conduct, and consistent throughout the organization and to produce a clear picture of key information risks. The document recommends the use of ISO 27005 and NIST SP 800-30 for detailed guidance.

Information risk assessment—supporting material: Describes supporting material needed to ensure that each phase of a risk assessment is performed correctly, assessments provide practical results, and effective decisions about risk can be made. The document recommends using BIRT and developing a set of security controls based on ISO 27002 and the NIST Cybersecurity Framework.

Information risk assessment process: The objective of this area is to adopt an information risk assessment methodology that includes important activities covering scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation, and risk treatment.

2.4 Review Questions / Case Studies / Projects

1. Briefly differentiate between information security governance and information security management.
2. Explain how the three supplemental factors in Figure 2.1—internal incident and global vulnerability reports, standards and best practices, and user feedback—play interconnected roles in designing a security program.
3. Differentiate between internal and external stakeholders from an information security point of view.
4. What are the two key pillars on which IT strategy planning should ideally be based?
5. What are the three categories of metrics for evaluating an organization's security governance?
6. What are the five roles within a security governing body structure defined in COBIT 5?
7. Explain the acronym RACI from context of information security policy.
8. Why is risk assessment needed in an organization?
9. Explain the term residual risk and provide an example.
10. Differentiate between a threat and a vulnerability.
11. What are the four factors that determine risk, and how are they related to each other?
12. Differentiate between qualitative and quantitative risk assessment.
13. Explain key ingredients of a risk analysis worksheet.
14. Explain the six stages of the information security risk management process.
15. Name the four risk-related standard documents that are published by The Open Group.

Chapter 3: Security Management

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Demonstrate key security program areas that must be overseen by the security management function**
- **Illustrate the purpose and general content of a security plan**
- **Presentation on the topic of security-related capital planning**
- **Discuss the role and typical content of a security & an acceptable use policy**
- **Present an overview of security management best practices**

3.1 Introduction

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) describes security management as encompassing several key elements. An organization should provide a sufficiently senior manager, such as a chief information security officer (CISO), with the authority and adequate resources for organizationwide information security. The CISO, or a similar individual, is responsible for supervising security-related projects, promoting information security throughout the organization, managing risk, and developing a comprehensive, approved information security policy.

This chapter looks at various aspects of security management.

3.2 The Security Management Function

Broadly speaking, the security management function entails establishing, implementing, and monitoring an information security program, under the direction of a senior responsible person.

Security management involves multiple levels of management. The different levels of management contribute to the overall security program with various types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) best understand the organization as a whole and have more authority. On the other hand, frontline managers (at the IT facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary so that each can help the others be more effective.

Recall that Chapter , “Security Governance,” defines two individual roles:

Chief information security officer (CISO): The CISO has overall responsibility for the enterprise information security program. The CISO is the liaison between executive management and the information security program. The CISO should also communicate and coordinate closely with key business stakeholders to address information protection needs. The CISO is responsible for:

- Establishing and maintaining an ISMS
- Defining and managing an information security risk treatment plan
- Monitoring and reviewing the ISMS

Information security manager (ISM): The ISM has responsibility for the management of information security efforts. COBIT 5 lists the following as areas of responsibility:

- Application information security
- Infrastructure information security
- Access management
- Threat and incident management
- Risk management
- Awareness program
- Metrics

Vendor assessments

COBIT 5 makes a distinction between the CISO and the ISM, with the CISO being a C-level position with oversight of an ISM, who has operational management responsibilities. Some organizations combine the roles of CISO and ISM. For purposes of this chapter, we simply refer to this role as CISO.

NISTIR 7359, Information Security Guide for Government Executives, provides a useful summary of the tasks that comprise information security management Although addressed to government executives, NISTIR 7359 discusses the general functional areas of an information security or cybersecurity program that should be the responsibility of the CISO in any organization. The key security program areas include the following:

Security planning: Security planning includes strategic security planning, which is defined in Chapter 2 as the alignment of information security management and operation with enterprise and IT strategic planning. But it also includes more detailed planning for the organization, coordination, and implementation of security. Key actors within the organization, such as department heads and project managers, need to be consulted and brought into the ongoing process of planning. Security planning is discussed in more detail in the following section.

Capital planning: Capital planning is designed to facilitate and control the expenditure of the organization’s funds. Part of the planning process, and part of the CISO’s responsibility, is to prioritize potential IT security investments for allocating available funding. Capital planning overlaps with security planning and is discussed subsequently in this section.

capital planning

A decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of an organization’s missions and business needs.

- Awareness and training: Awareness and training programs ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and

protect the information resources entrusted to them. Chapter, “People Management,” covers this topic.

- Information security governance: The CISO should advise C-level executives and the board concerning the development of effective security governance, which is covered in Chapter 2.
- System development life cycle: This is the overall process of developing, implementing, and retiring information systems. Chapter, “System Development,” is devoted to this topic.
- Security products and services acquisition: Management supervision of the acquisition of security-related products and services includes considering the costs involved, the underlying security requirements, and the impact on the organizational mission, operations, strategic functions, personnel, and service-provider arrangements. Acquisition is discussed subsequently in this section.
- Risk management: This topic is discussed in previous Chapters.

Configuration management: The CISO should employ configuration management to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

Configuration Management

- The process of controlling modifications to a system’s hardware, software, and documentation, which provides sufficient assurance that the system is protected against the introduction of improper modification before, during, and after system implementation.
- Incident response: Incident response, which occurs after the detection of a security event, seeks to minimize the damage of the event and facilitate rapid recovery. The CISO should ensure that an adequate incident response system is in place and operating properly. Chapter , “Threat and Incident Management,” covers this topic.
- Performance measures: The CISO should ensure that an organizationwide performance measures are defined and used. Performance measures are a key feedback mechanism for an effective information security program. Chapter, “Security Monitoring and Improvement,” covers this topic.

Another useful source of guidance on the information management security function is the ISF SGP, which recommends that this function encompass the following:

- Consistent organizationwide use of security: The CISO (or equivalent) is responsible for developing, maintaining, and regularly reviewing an overall security strategy for the organization and the accompanying policy document.
- Support function: The CISO should:
  Act as a clearinghouse for security advice, making experts available to business unit managers and project managers, as needed
  Promote security awareness throughout the organization

  Develop standard terms and agreements in contracts to ensure that suppliers and other external relationships meet the security standards of the organization
  Evaluate the security implications of new business initiatives
  Oversee the risk assessment process
  Set standards for use of cryptographic algorithms and security protocols

- Monitor function: The CISO should monitor trends and developments to be aware of how they may affect the organization's security strategy and implementation, including in the area of business trends, new technical developments, security solutions, standards, legislation, and regulation.
- Projects function: The CISO should be responsible for overseeing security-related projects.
- External requirements function: The CISO should manage the implications of laws, regulations, and contracts.

Security Planning

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, indicates that the purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan is basically documentation of the structured process of planning adequate, cost-effective security protection for a system.

security plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

SP 800-18 recommends that each information system in an organization have a separate plan document with the following elements:

- Information system name/identifier: A name or identifier uniquely assigned to each system. Assignment of a unique identifier supports the organization's ability to easily collect information and security metrics specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance. The identifier should remain the same throughout the life of the system and retained in audit logs related to system use.
- Information system owner: The person responsible for managing this asset.
- Authorizing individual: The senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.
- Assignment of security responsibility: The individual responsible for the security of the information system.
- Security categorization: Using the FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, categories, the acceptable level of risk (low, moderate, or high) for confidentiality, integrity, and availability (for each distinct element of the system, if necessary).
- Information system operational status: Status, such as operational, under development, or undergoing major modification.
- Information system type: Type, such as major application or support system.
- Description/purpose: A brief description (one to three paragraphs) of the function and purpose of the system.
- System environment: A general description of the technical system, including the primary hardware, software, and communications equipment.

- System interconnections/information sharing: Other systems/information assets that interact with this information system.
- Related laws/regulations/policies: Any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system.
- Existing security controls: Description of each control.
- Planned security controls: Description of each control plus implementation plan.
- Information system security plan completion date: The target date.
- Information system security plan approval date: The data plan approved date.

This sort of documentation enables the CISO to oversee all security projects throughout the organization. The CISO should also coordinate a process for developing and approving these plans. One good description of such a process is provided in Federal Enterprise Architecture Security and Privacy Profile [OMB10] and illustrated in Figure 4.1.

This process involves three steps, each of which has goals, objectives, implementing activities, and output products for formal inclusion in agency enterprise architecture and capital planning processes:

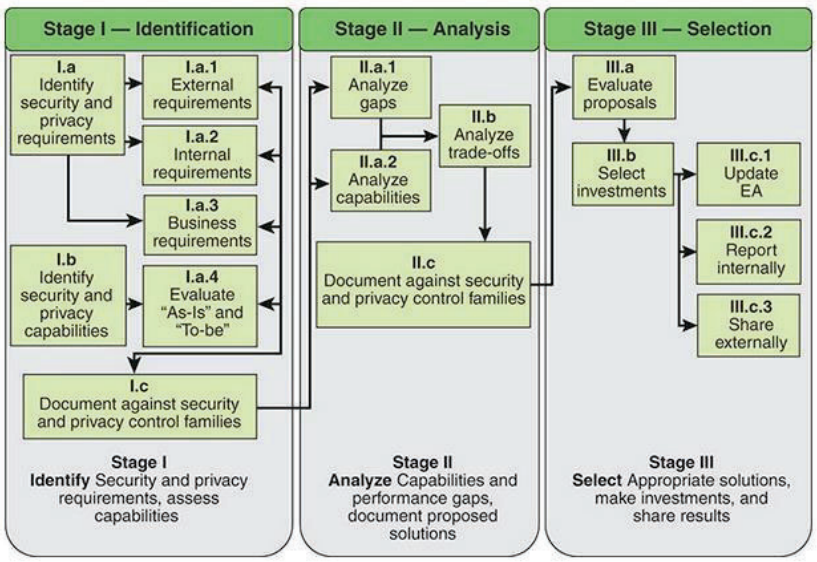


FIGURE 4.1 Example of a Security Planning Process

1. Identify: Encompasses the research and documentation activities necessary to identify security and privacy requirements in support of the mission objectives so that they can be incorporated into the enterprise architecture.
2. Analyze: Involves an analysis of organization security and privacy requirements and the existing or planned capabilities that support security and privacy.
3. Select: Involves an enterprise evaluation of the solutions proposed in the preceding phase and the selection of major investments.

Step 1 refers to three types of requirements, defined as follows:

- External requirements: These are security requirements imposed from outside the organization, such as laws, regulations, and contractual commitments.
- Internal requirements: These are security requirements developed as part of the security policy, such as the acceptable degree of risk and confidentiality, integrity, availability, and privacy guidelines.
- Business requirements: This refers to requirements other than security requirements that are related to the overall business mission. Examples include finance, accounting, and audit requirements. In general, these requirements refer to the organization's need to discharge business responsibilities.

Capital Planning

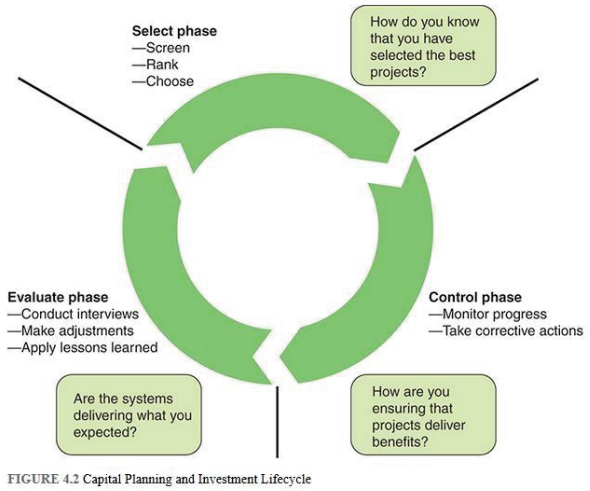


FIGURE 4.2 Capital Planning and Investment Lifecycle

Determining the benefit to an organization from IT security investments is a key element of IT security planning. Traditionally, capital planning has been applied to IT procurement overall and has been a separate function from security planning. As pointed out in NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, it is important to integrate capital planning methodology into the security planning process. An effective way of doing this—and one recommended by SP 800-65 is the Select/Control/Evaluate framework defined in the U.S. Government Accountability Office (GAO) publication Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity [GAO04], as shown in Figure 4.2.

The Select/Control/Evaluate framework defines a cyclical process consisting of three steps for deciding which projects to pursue or which investments to make:

1. Select: Identify and analyze each project's risks and returns before committing significant funds to any project. The organization then selects the IT projects that best support its mission needs. The organization repeats this process each time funds are allocated to projects.
2. Control: Ensure that as projects develops and investment expenditures continue, the project continues to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps must be quickly taken to address the deficiencies. If mission needs have changed, the organization needs to adjust its objectives for the project and appropriately modify expected project outcomes.
3. Evaluate: Compare actual results and expected results after a project was fully implemented. This is done for the following reasons:
   - To assess the project's impact on mission performance
   - To identify any necessary changes or modifications to the project
   - To revise the investment management process based on lessons learned

Apply this process to every security-related investment in the organization. The costs typically incurred or contemplated are usually in three categories:

- Direct costs of providing IT security for the specific IT investment
- Costs for products, procedures, and personnel that have an incidental or integral component and/or a quantifiable benefit for the specific IT investment
- Allocated security control costs for networks that provide some or all necessary security controls for associated applications

Note that investment choices involve not only hardware and software but also procedures or processes within the organization. For example, risk assessment itself is a cost. How many employee-hours and at what levels should be devoted to this process? This includes effort to collect threat and vulnerability data from external sources, internal security incident review, and security-related reports from department heads, managers, and even individual employees. If the assessment is pursued to a great level of detail, the results may be well beyond the needs of the organization in making cost-effective decisions. Underinvestment may produce results that lack the breadth and depth necessary to reasonably protect assets. Similar considerations apply in other process-related costs, such as employee awareness efforts.

Table 4.1 describes the three categories in detail.

TABLE 4.1 Information Security Costs

Direct Costs	Products, Procedures, and Personnel	Allocated Security Control Costs
▪ Risk assessment ▪ Security planning and policy ▪ Certification and accreditation ▪ Specific security controls ▪ Authentication or cryptographic applications ▪ Education, awareness, and training ▪ System reviews/evaluations ▪ Oversight or compliance inspections ▪ Development or maintenance of security reports ▪ Contingency planning and testing ▪ Physical and environmental controls for hardware and software ▪ Auditing and monitoring ▪ Computer security investigations and forensics ▪ Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations ▪ Privacy impact assessments	▪ Configuration or change management control ▪ Personnel security ▪ Physical security ▪ Operations security ▪ Privacy training ▪ Program/system evaluations ▪ System administrator functions ▪ System upgrades with new features that obviate the need for other standalone security controls	▪ Firewalls ▪ Intrusion detection/prevention systems ▪ Forensic capabilities ▪ Authentication capabilities ▪ Additional add-on security considerations

3.3 Security Policy

Recall from Chapter 2 that an information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is helpful to distinguish four types of documents before proceeding:

- Information security strategic plan: Relates to the long-term goals for maintaining security for assets.
- Security plan: Relates to security controls in place and planned to meet strategic security objectives.
- Security policy: Relates to the rules and practices that enforce security.
- Acceptable use policy: Relates to how users are allowed to use assets.

TABLE 4.2 Security-Related Documents

Document Type	Description	Primary Audience
Information security strategic plan	A document used to communicate with the organization the organization's long-term goals with respect to information security, the actions needed to achieve those goals, and all the other critical elements developed during the planning exercise.	C-level executives
Security plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.	C-level executives, security managers, other managers
Security policy	A set of laws, rules, and practices that regulate how an organization manages and protects assets and the rules for distribution of sensitive information. It includes associated responsibilities and the information security principles to be followed by all relevant individuals.	All employees, especially those with some responsibility for an asset or assets
Acceptable use policy	A policy that defines for all parties the ranges of use that are approved for use of information, systems, and services within the organization.	All employees

Table 4.2 provides a more detailed description. All these documents should be approved by a CISO or comparable executive. The CISO may task an individual or a team with document preparation. With these distinctions in mind, this section addresses security policy.

The purpose of an information security policy is to ensure that all employees in an organization, especially those with responsibility of some sort for one or more assets, understand the security principles in use and their individual security-related responsibilities. Lack of clarity in information security policies can defeat the purpose of the security program and may result in significant losses. An information security policy is the means by which the organization provides management direction and support for information security across the organization. The security policy document defines what is expected from employees and possibly others who have roles in the organization, such as contractors, outside partners or vendors, and visitors.

Security Policy Categories

An organization may choose to use a single security policy document. For larger organizations, this may need to be a lengthy document. It is preferable to have a collection of policy documents so that employees and managers can consult only the relevant documents, as needed. Some of the security policies an organization may adopt include the following [INFO14]:

- Access control policy: How information is accessed
- Contingency planning policy: How availability of data is provided 24/7
- Data classification policy: How data are classified
- Change control policy: How changes are made to directories or the file server
- Wireless policy: How wireless infrastructure devices need to be configured
- Incident response policy: How incidents are reported and investigated

Termination of access policy: How employee access to organization assets is handled during termination

- Backup policy: How data is backed up
- Virus policy: How virus infections need to be dealt with
- Retention policy: How data can be stored
- Physical access policy: How access to the physical area is obtained
- Security awareness policy: How security awareness is carried out
- Audit trail policy: How audit trails are analyzed
- Firewall policy: How firewalls are named, configured, and so on
- Network security policy: How network systems are secured
- Encryption policy: How data are encrypted, the encryption method used, and so on

- BYOD policy: What devices an employee may use both on premises and off to access organization assets
- Cloud computing policy: Security aspects of using cloud computing resources and service

Ultimately, a CISO and a security manager are responsible for developing these policies. Typically, a security analyst or team of analysts are tasked with the actual formulation of policy documents, which are then approved by higher management.

Security Policy Document Content

Whether a single document or a set of documents, each security policy document should include the following sections:

- Overview: Background information on what issue the policy addresses
- Purpose: Why the policy was created
- Scope: What areas the policy covers
- Targeted audience: To whom the policy is applicable
- Policy: A complete but concise description of the policy
- Noncompliance: Consequences for violating the policy
- Definitions: Technical terms used in the document
- Version: Version number to keep track of the changes made to the document

A good source of guidance for developing a policy document is the set of policy document templates provided by the SANS Institute. These have been made freely available as a public service. The complete set that is available is shown in Table 4.3.

TABLE 4.3 Security Policy Templates Provided by the SANS Institute

General	Network Security	Server Security	Application Security
Acceptable Encryption	Acquisition Assessment	Database Credentials	Web Application Security
Acceptable Use	Bluetooth Baseline Requirements	Technology Equipment Disposal	
Clean Desk	Remote Access	Information Logging Standard	
Data Breach Response	Remote Access Tools	Lab Security	
Disaster Recovery Plan	Router and Switch Security	Server Security	
Digital Signature Acceptance	Wireless Communication	Software Installation	
Email	Wireless Communication Standard	Workstation Security	
Ethics			
Pandemic Response Planning			
Password Construction Guidelines			
Password Protection			
Security Response Plan			
End User Encryption Key Protection			

SANS Institute Information Security Policy Templates https://www.sans.org/securityresources/policies/

As an example, the following sidebar shows one of the SANS Institute policy templates.

SANS Institute Router and Switch Security Policy

1. PURPOSE

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <Company Name>.

2. SCOPE

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.

3. POLICY

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled: IP directed broadcasts; incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses; TCP small services; UDP small services; all source routing and switching; all web services running on router; cisco discovery protocol on Internet connected interfaces; Telnet, FTP, and HTTP services; Auto-configuration
4. The following services should be disabled unless a business justification is provided: Cisco discovery protocol and other discovery protocols; dynamic trunking; scripting environments, such as the TCL shell
5. The following services must be configured: password encryption; NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including: IP access list accounting; device logging; incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped; router console and modem access must be restricted by additional security controls

4. POLICY COMPLIANCE

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 EXCEPTIONS

Any exception to the policy must be approved by the Infosec team in advance.

5.3 NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Management Guidelines for Security Policies

The SGP provides a useful set of guidelines for the creation, content, and use of security policy documents, which can be categorized as follows:

- Responsibilities: Identify the following:
  Those responsible for ratifying policy document (for example, the board)
  Responsibilities of all relevant individuals to comply with the policy
  Individuals responsible for protecting specific assets
  That all individuals must confirm the understanding of, acceptance of, and compliance with relevant policies and understand that disciplinary action will follow policy violation
- Principles: Specify the following:
  All relevant assets to be identified and classified by value/importance

All assets protected with respect to CIA (confidentiality, integrity, and availability) and other security requirements
All laws, regulations, and standards complied with

- Actions: Specify the following:
  That all individuals are made aware of the security policy and their responsibilities
  That all assets are subject to risk assessment periodically and before a major change
  That all breaches are reported in a systematic fashion
  That auditing occurs periodically and as needed
  That policy documents are reviewed regularly and as needed
- Acceptable use: Policies that include the following:
  Documentation of what behaviors are required, acceptable, and prohibited with respect various assets
  Responsibility for establishing, approving, and monitoring acceptable use policies

Monitoring the Policy

The CISO should designate an individual or a group responsible for monitoring the implementation of the security policy. The responsible entity should periodically review policies and make any changes needed to reflect changes in the organization's environment, asset suite, or business procedures. A violation-reporting mechanism is needed to encourage employees to report.

3.4 Acceptable Use Policy

An acceptable use policy (AUP) is a type of security policy targeted at all employees who have access to one or more organization assets. It defines what behaviors are acceptable and what behaviors are not acceptable. The policy should be clear and concise, and it should be a condition of employment for each employee to sign a form indicating that he or she has read and understood the policy and agrees to abide by its conditions.

The MessageLabs white paper Acceptable Use Policies—Why, What, and How [NAYL09] suggests the following process for developing an AUP:

1. Conduct a risk assessment to identify areas of concern. As part of the risk assessment process, identify the elements that need to go into an AUP.
2. Create the policy. The policy should be tailored to the specific risks identified, including liability costs. For example, the organization is exposed to liability if customer data is exposed. If the failure to protect the data is due to an employee's action or inaction, and if this behavior violates the AUP, and if this policy is clear and enforced, then this may mitigate the liability of the organization.
3. Distribute the AUP. This includes educating employees on why an AUP is necessary.
4. Monitor compliance. A procedure is needed to monitor and report on AUP compliance.

Enforce the policy. The AUP must be enforced consistently and fairly when it is breached.

An example of a template for an AUP is provided by the SANS Institute. It has a similar structure to the security policy template shown in Section 4.1. The heart of the document is the policy section, which covers the following areas:

SANS Institute AUP Template https://www.sans.org/security-resources/policies/general#acceptable-use-policy

- General use and ownership: Key points in this section include:
  Employees must ensure that proprietary information is protected.
  Access to sensitive information is allowed only to the extent authorized and necessary to fulfill duties.
  Employees must exercise good judgment regarding the reasonableness of personal use.
- Security and proprietary information: Key points in this section include:
  Mobile devices must comply with the company's BYOD policies.
  System- and user-level passwords must comply with the company's password policy.
  Employees must use extreme caution when opening email attachments.
- Unacceptable use—system and network activities: Key points in this section include:
  Unauthorized copying of copyrighted material
- The prohibition against accessing data, a server, or an account for any purpose other than conducting company business, even with authorized access
  Revealing your account password to others or allowing use of your account by others
  Making statements about warranty unless it is a part of normal job duties
  Circumventing user authentication or security of any host, network, or account
  Providing information about, or lists of, company employees to outside parties
- Unacceptable use—email and communication activities: Key points in this section include:
  Any form of harassment
  Any form of spamming
  Unauthorized use, or forging, of email header information
- Unacceptable use—blogging and social media: Key points in this section include:
  Blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate company policy, is not detrimental to company's best interests, and does not interfere with an employee's regular work duties.
  Any blogging that may harm or tarnish the image, reputation, and/or goodwill of company and/or any of its employees is prohibited.
  Employees may not attribute personal statements, opinions, or beliefs to the company.

3.5 Security Management Best Practices

The SGP breaks down the best practices in the security management category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Security policy management: Discusses a specialist information security function, led by a sufficiently senior manager (e.g., a CISO), that is assigned adequate authority and resources to run information security-related projects; promote information security throughout the organization; and manage the implications of relevant laws, regulations and contracts.
- ✓ Information security policy: Documents the governing body's direction on and commitment to information security and communicate it to all relevant individuals.
- ✓ Acceptable use policies: Lists recommended actions for establishing AUPs, which define the organization's rules on how each individual (for example, an employee, a contractor) may use information and systems, including software, computer equipment, and connectivity.

- Information security management: Provides guidance for developing a comprehensive, approved information security policy (including supporting policies, standards, and procedures) and communicating it to all individuals who have access to the organization's information and systems.

✓ Information security function: Ensures that good practice in information security is applied effectively and consistently throughout the organization.

✓ Information security projects: Lists recommended actions for ensuring that all information security projects apply common project management practices, meet security requirements, and are aligned with the organization's business objectives.

✓ Legal and regulatory compliance: Describes a process that should be established to identify and interpret the information security implications of relevant laws and regulations.

3.6 Review Questions / Case Studies / Projects

1. Define the security management function.
2. What are the two key individual roles in security management?
3. Explain key security program areas.
4. Describe the “select-control-evaluate” framework for capital planning.
5. Briefly explain the need of an effective information security policy. Also list different documents related to security.
6. Describe some common security policies of an organization.
7. What can be an effective structure of a security document?
8. What are the key aspects of security policy document?
9. What functions does information security management perform?
10. What do you understand by “acceptable use policy”?

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Describe the key security considerations in the three phases of the employment life cycle.**
- **Explain the four phases in the cybersecurity learning continuum.**
- **Explain the steps involved in information classification.**
- **Understand the requirements for information labeling.**
- **Present an overview of threats to privacy.**
- **Present an overview of people management best practices , the General Data Protection Regulation, considerations involved in protecting sensitive physical information and information management best practices.**
- **Discuss the differences between document management and records management.**

4.1 Introduction - Managing the Cybersecurity Function

The basic idea is that the several components in any complex system will perform particular sub functions that contribute to the overall function.

- ✓ **People Management**
- ✓ **Information Management**
- ✓ Physical Access Management
- ✓ System Development
- ✓ Business Application Management
- ✓ System Access
- ✓ System Management
- ✓ **Networks and Communications**
- ✓ Supply Chain Management
- ✓ Technical Security Management
- ✓ **Threat and Incident Management**
- ✓ Local Environment Management
- ✓ Business Continuity

Chapter 6, 7 & 8 will discuss about People Management, Information Management, Networks and Communications & Threat and Incident Management but you have research about all other sub function. Your assessments will have the combination all sub functions.

4.2 People Management

The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) uses the term people management to refer to all aspects of security related to the behavior of employees and others who have access to the organization's information and systems. As many security experts have pointed out, superb technical solutions for ensuring security are bound to fail if employees do not understand their security responsibilities and are trained and motivated to fulfill those responsibilities.

Broadly speaking, this topic encompasses two areas. The first has to do with what could be called the employment life cycle: the relationship of the individual to the organization prior to employment, during employment, and at and after employment termination. The SGP refers to this area as human resource security. The other area has to do with the security-related training of employees, both in terms of general security awareness, as well as in terms of the use of IT assets. The SGP refers to this area as security awareness/education. These topics are covered in the first two sections of this chapter, followed by a review of best practices.

Human Resource Security

Android Studio is an integrated development environment (IDE) provided by Google as their official tool for developing Android phone and tablet applications. This tool is continually being refined and has become quite powerful and reliable with recent versions. Especially useful is the enhanced ability to identify deprecated code, inefficient code, and code that doesn't conform to Android design guidelines.

Sound security practice dictates that information security requirements be embedded into each stage of the employment life cycle, specifying security-related actions required during the induction of each individual, the employee's ongoing management, and termination of his or her employment. Human resource security encompasses all security aspects involving employees:

- Hiring new employees
- Training employees
- Monitoring employee behavior
- Handling employee departure/termination

Especially important is the management of personnel with privileged user access to information and IT assets.

It is important for executive management—and indeed for all employees—to understand that cybersecurity is not exclusively—or even primarily—a technical challenge to be relegated to the work of IT and security professionals. As the Council on Cyber-Security points out in its Cybersecurity Workforce Handbook [COCS14], cybersecurity is similar to health and safety considerations, in which the actions of each employee affect the health and safety of everyone. In the case of cybersecurity, the actions of any one employee can compromise security for the entire organization. Technical fixes cannot remove vulnerabilities inherent in the workforce itself, including social engineering (such as

emails with malicious links), poor credential management (such as weak or unprotected passwords), and use of insecure or poorly configured devices and applications (such as connecting “dirty” thumb drives or installing applications from unverified websites).

Thus, all employees, through awareness training, should learn basic security practice. Fortunately, many of the tasks associated with this effort are not onerous. Rather, there are some basic tasks that every employee can perform to ensure good cyber hygiene.

Security problems caused by employees fall into two categories: non-malicious and malicious. Some people unwittingly aid in the commission of security incidents by failing to follow proper procedure, by forgetting security considerations, and by not understanding what they are doing. If an organization does not have effective awareness and training programs, a problem could occur because an employee was never told what constitutes proper procedure in terms of security. Such behavior does not involve a motive to cause harm. It may be either accidental, when there is no decision to act inappropriately, or it may be negligent, when there is a conscious decision to act inappropriately. As an example of the latter case, someone may take a shortcut to increase productivity or simply to avoid hassle but might feel that he or she can do so without causing a security incident.

Other people knowingly violate controls and procedures to cause or aid in security incidents. The security problems caused by such persons can exceed those caused by outsiders, as employees with privileged access are the ones who know the controls and know what information of value may be present.

Security in the Hiring Process

ISO 27002, Code of Practice for Information Security Controls, lists the following security objective of the hiring process: to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Although this section is primarily concerned with employees, the same considerations apply to contractors and third-party users.

Background Checks and Screening

From a security viewpoint, hiring presents management with significant challenges. In the Computer Security Handbook, Kabay and Robertson [KABA14] point out that growing evidence suggests that many people inflate their resumes with unfounded claims. Compounding this problem is the increasing reticence of former employers. Employers may hesitate to give poor references for incompetent, underperforming, or unethical employees for fear of a lawsuit if their comments become known and an employee fails to get a new job. On the other hand, a favorable reference for an employee who subsequently causes problems at his or her new job may invite a lawsuit from the new employer. As a consequence, a significant number of employers have a corporate policy that forbids discussing a former employee’s performance in any way, positive or negative. The employer may limit information to the dates of employment and the title of the position held.

Despite these obstacles, employers must make a significant effort to do background checks and otherwise screen applicants. Of course, such checks are done to ensure that the prospective employee is competent to perform the intended job and poses no security risk. In addition, employers need to be cognizant of the concept of “negligent hiring” that applies in some jurisdictions. In essence, an

employer may be held liable for negligent hiring if an employee causes harm to a third party (individual or company) while acting as an employee.

General guidelines for checking applicants include the following:

- Ask an applicant for as much detail as possible about employment and educational history. The more detail that is provided, the more difficult it is for the applicant to lie consistently.
- Investigate the accuracy of the applicant's details to a reasonable extent.
- Arrange for experienced staff members to interview candidates and discuss discrepancies.

For highly sensitive positions, more intensive investigation is warranted. The Information Technology Security Handbook [SADO03] gives the following examples of measures that may be warranted in some circumstances:

- Have an investigation agency do a background check.
- Get a criminal record check of the individual.
- Check the applicant's credit record for evidence of large personal debt and inability to pay it. Discuss problems, if you find them, with the applicant. People who are in debt should not be denied jobs: If they are, they will never be able to regain solvency. At the same time, employees who are under financial strain may be more likely to act improperly.
- Consider conducting a polygraph examination of the applicant (if legal). Although polygraph examinations are not always accurate, they can be helpful if you have a particularly sensitive position to fill.
- Ask the applicant to obtain bonding for his or her position.

For many employees, these steps are excessive. However, an employer should conduct extra checks of any employee who will be in a position of trust or privileged access—including maintenance and cleaning personnel.

In addition, after employment commences, managers should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.

Employment Agreements

As part of their contractual obligation, employees should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. The agreement should include a confidentiality and non-disclosure agreement that spells out specifically that the organization's information assets are confidential unless classified otherwise and that the employee must protect that confidentiality. Confidentiality agreements put all parties on notice that the organization owns its information, expects strict confidentiality, and prohibits information sharing except for that required for legitimate business needs. The agreement should also reference the organization's security policy and indicate that the employee has reviewed and agrees to abide by the policy.

Job Descriptions

The Federal Financial Institutions Examination Council [FFIE02] suggests that job descriptions be designed to increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees within their job descriptions. Management should

expect all employees, officers, and contractors to comply with security and acceptable use policies and protect the institution's assets, including information. The job descriptions for security personnel should describe the systems and processes they will protect and the control processes for which they are responsible. Management can take similar steps to ensure that contractors and consultants understand their security responsibilities as well.

A key aspect of clarifying the security responsibilities attached to a particular job description is to specify the cybersecurity tasks associated with each type of job. Figure 5.1, based on a figure in the Cybersecurity Workforce Handbook [COCS14], lists tasks that must be performed by everyone in the enterprise, with additional tasks assigned to those with increased responsibility for data and systems.

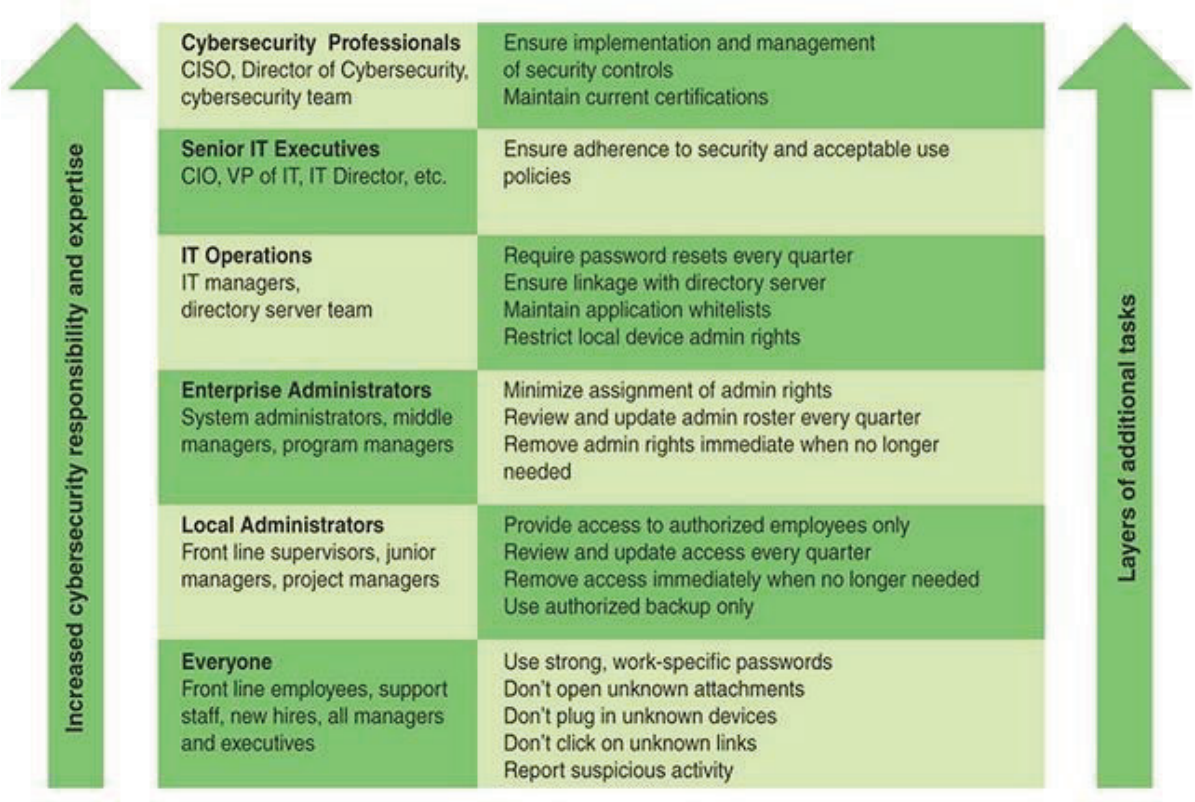


FIGURE 5.1 Security-Related Tasks by Job Description

directory server: Manages user identity and authorization data in a directory format.

Whitelist: A list of discrete entities, such as hosts or applications, that are known to be benign and are approved for use within an organization and/or information system.

application whitelisting: A process that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

During Employment

ISO 27002 lists the following security objective with respect to current employees: to ensure that employees and contractors are aware of and fulfill their information security responsibilities. Specifically, employees and contractors should:

- Be aware of information security threats and concerns
- Be aware of their responsibilities and liabilities with regard to information security
- Be equipped to support organizational security policy in the course of their normal work

Two essential elements of personnel security during employment are (1) comprehensive security policy and acceptable use documents and (2) an ongoing awareness and training program for all employees. These are covered in Chapter, "Security Management," and Section 5.2, respectively.

In addition to enforcing the security policy in a fair and consistent manner, there are certain principles that need to be followed for personnel security:

- Least privilege: Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on every system and has physical access to everything, then all users are roughly equivalent in their level of threat.
- Separation of duties: Carefully separate duties so that people involved in checking for inappropriate use are not also capable of perpetrating such inappropriate use. For example, one individual should not have overlapping security access and audit responsibilities. In that case, the individual can violate security policy and cover up any audit trail that would reveal the violation.
- Dual operator policy: In some cases, it may be possible to define specific tasks that require two people. A similar policy is two-person control, which requires that two employees approve each other's work.
- Mandatory vacations: Mandatory vacation policies help expose employees involved in malicious activity, such as fraud or embezzlement. As an example, employees in positions of fiscal trust, such as stock traders or bank employees, are often required to take an annual vacation of at least five consecutive workdays.

Termination of Employment

ISO 27002 lists the following security objective with respect to termination of employment: to protect the organization's interests as part of the process of changing or terminating employment.

The termination process is complex and depends on the nature of the organization, the status of the employee in the organization, and the reason for departure. From a security point of view, the following actions are important:

- Removing the person's name from all lists of authorized access to applications and systems
- For IT personnel, ensuring that no rogue admin accounts were created
- Explicitly informing guards that the ex-employee is not allowed into the building without special authorization by named employees
- Removing all personal access codes
- If appropriate, changing lock combinations, reprogramming access card systems, and replacing physical locks
- Recovering all assets, including employee ID, disks, documents, and equipment (assets that should have been documented when provided to the employee)
- Notifying, by memo or email, appropriate departments so that they are aware of the change in employment status

- If appropriate, escorting the ex-employee off the premises

Security Awareness and Education

A critical element of an information security program is the security awareness and training program. It is the means for disseminating security information to all employees, including IT staff, IT security staff, and management, as well as IT users and other employees. A workforce that has a high level of security awareness and appropriate security training for each individual's role is as important as, if not more important than, any other security countermeasure or control.

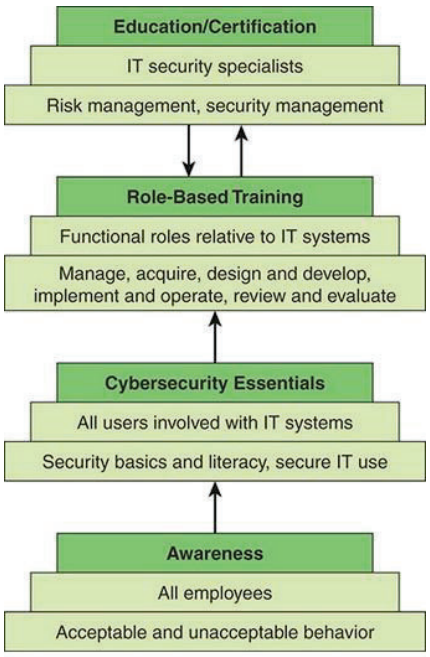


FIGURE 5.2 Cybersecurity Learning Continuum

Two key National Institute of Standards and Technology (NIST) publications, SP 800-16, A Role-Based Model for Federal Information Technology/Cybersecurity Training, and SP 800-50, Building an Information Technology Security Awareness and Training Program, are valuable resources in this area, and this section draws on both. SP 800-50 works at a higher strategic level and discusses how to build and maintain an information security awareness and training program; SP 800-16 addresses a more tactical level and discusses the awareness–training–education continuum, role-based training, and course content considerations. Both publications define and describe a cybersecurity learning continuum that depicts a progression of learning across the spectrum of roles throughout the organization, consisting of four phases (see Figure 5.2).

The four phases are as follows:

- Awareness: A set of activities that explains and promotes security, establishes accountability, and informs the workforce of security news. Participation in security awareness programs is required for all employees.
- Cybersecurity essentials: Intended to develop secure practices in the use of IT resources. This level is needed for those employees, including contractor employees, who are involved in any way with IT systems. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.
- Role-based training: Intended to provide knowledge and skills specific to an individual's roles and responsibilities relative to information systems. Training supports competency development and helps personnel understand and learn how to perform their security roles.
- Education/certification: Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social).

Security Awareness

Because all employees have security responsibilities, all employees must have suitable awareness training. Awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness is a program that continually pushes the security message to users in a variety of formats. Note that a

security awareness program must reach all employees, not just those with access to IT resources. Such topics as physical security, protocols for admitting visitors, social media rules, and social engineering threats are concerns with all employees.

The overall objective of the organization should be to develop a security awareness program that permeates to all levels of the organization and that is successful in promoting an effective security culture. To that end, the awareness program must be ongoing, focused on the behavior of various categories of people, monitored, and evaluated.

security awareness: The extent to which staff understand the importance of information security, the level of security required by the organization, and their individual security responsibilities.

security culture: The extent to which staff demonstrate expected security behavior in line with their individual security responsibilities and the level of security required by the organization.

Specific goals for a security awareness program should include:

- Providing a focal point and a driving force for a range of awareness, training, and educational activities related to information security, some of which might already be in place but perhaps need to be better coordinated and more effective
- Communicating important recommended guidelines or practices required to secure information resources
- Providing general and specific information about information security risks and controls to people who need to know
- Making individuals aware of their responsibilities in relation to information security
- Motivating individuals to adopt recommended guidelines or practices
- Being driven by risk considerations (for example, assigning risk levels to different groups of individuals, based on their job function, level of access to assets, access privileges, and so on)
- Providing employees with an understanding of the different types of inappropriate behavior—such as malicious, negligent, and accidental—and how to avoid negligent behavior or accidental behavior and recognize malicious behavior in others

negligent behavior: Behavior that does not involve a motive to cause harm but does involve a conscious decision to act inappropriately (for example, using unauthorized services or devices to save time, increase productivity, or enable remote working).

accidental behavior: Behavior that does not involve a motive to harm or a conscious decision to act inappropriately (for example, emailing sensitive information to unauthorized recipients, opening malicious email attachments, publishing personal information on publicly available servers).

malicious behavior: Behavior that involves a combination of motive to cause harm and a conscious decision to act inappropriately (for example, copying business files before taking employment with a competitor, leaking sensitive information, misusing information for personal gain).

- Creating a stronger culture of security, with a broad understanding and commitment to information security
- Helping enhance the consistency and effectiveness of existing information security controls and potentially stimulating the adoption of cost-effective controls
- Helping minimize the number and extent of information security breaches, thus reducing costs directly (for example, data damaged by viruses) and indirectly (for example, reduced need to investigate and resolve breaches)

The European Union Agency for Network and Information Security (ENISA) has identified three main processes in the development of an information security awareness program [ENIS08], as shown in Figure 5.3.

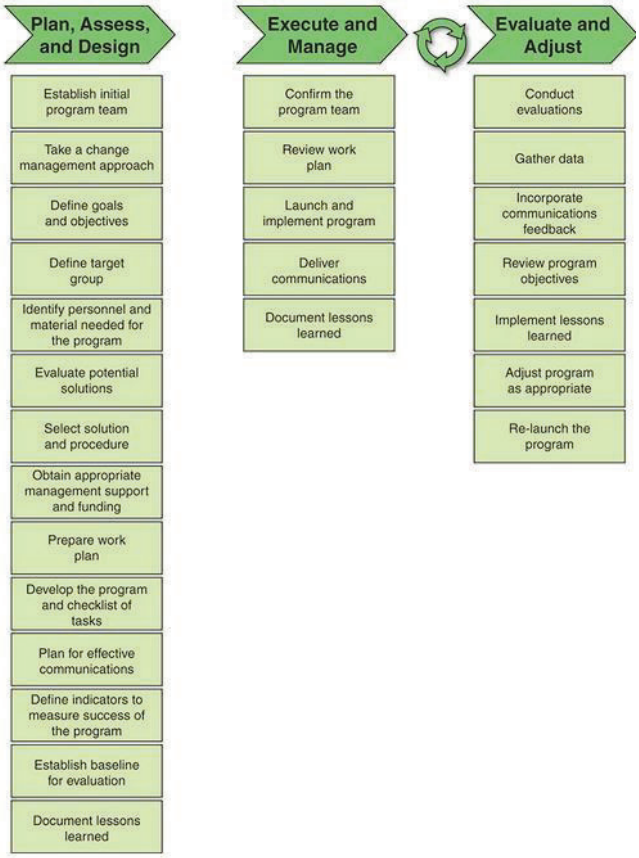


FIGURE 5.3 Security Awareness Processes

change management

Business processes that seek to ensure that only authorized modifications are made to an item, while mitigating risk and impact to the whole. Change management is designed to minimize resistance to organizational change through involvement of key players and stakeholders.

The three main processes are as follows:

- Plan, assess, and design: Awareness programs must be designed with the organization mission in mind. They should support the business needs of the organization and be relevant to the organization's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented. In the design step of the program, the awareness needs are identified, an effective awareness plan is developed, organizational buy-in is sought and secured, and priorities are established.
- Execute and manage: This process includes activities necessary to implement an information security awareness program. The initiative is executed and managed only when:
  - ✓ A needs assessment has been conducted
  - ✓ A strategy has been developed
  - ✓ An awareness program plan for implementing that strategy has been completed
  - ✓ Material has been developed
- Evaluate and adjust: Formal evaluation and feedback mechanisms are critical components of any security awareness program. The feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements are solidified, design and implement a feedback strategy.

Awareness Program Communication Materials

At the heart of an awareness training program are the communication materials and methods used to convey security awareness. There are two options for the awareness program designer:

- Use in-house materials
- Use externally obtained materials

A well-designed program should have materials from both sources.

In-house materials that are effectively used include the following:

- Brochures, leaflets, and fact sheets: These short documents are used to highlight key points such as password selection and use.
- Security handbook: The security policy document is one candidate for a handbook. However, a document specifically geared toward awareness could be produced, covering all the security topics needed for all employees.
- Regular email or newsletter: This communication channel is used to highlight changes either in organization security policy or outside threats, especially social engineering threats. In addition, this channel can be used to send reminders on specific topics.
- Distance learning: The organization can set up a set of self-paced courses that are available online.
- Workshop and training sessions: A block of time, such as an hour or an entire day, can be set aside, with mandatory attendance by certain categories of staff.
- Formal classes: Classes can be held much like workshops, but perhaps offered off-site and lasting multiple days. They could be part of a professional development program.
- Video: Available online or via disk, a video can cover one or more topics in depth and may be watched by individuals on their own time or on time allowed during work hours.
- Website: An organization security website can be established that can be updated to reflect changes, present content for multiple audiences, and link to other information.

Short communications, such as messages and emails, cover topics tailored to the role and level of access of the individual, including:

- Emphasizing the difference between critical information and sensitive information, which must be treated differently
  - ✓ **critical information:** Information that needs to be available and have integrity (for example, product prices/exchange rates, manufacturing information, medical records).
  - ✓ **sensitive information:** Information that can be disclosed only to authorized individuals (for example, product designs, merger and acquisition plans, medical records, business strategy information).
- Providing updates on details of current and anticipated threats
- Reinforcing expected security-related activity
- Reinforcing the individual's personal responsibility for security
- Restating key security policy points
- Highlighting specific concerns related to electronic communications, such as email, blogs, and texting
- Highlighting specific security concerns related to information systems

Externally obtained information and materials include the following:

- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office
- Professional organizations and vendors
- Online IT security daily news websites
- Periodicals
- Conferences, seminars, and courses

The NIST Computer Security Division website's awareness, training, education, and professional development pages contain a number of links to government, industry, and academic sites that offer or sell both awareness and training materials.

Awareness Program Evaluation

Just as in other areas of security, evaluation is needed to ensure that an awareness program is meeting objectives. ENISA has developed a set of metrics that are useful for awareness program evaluation [ENIS07], as shown in Table 5.1.

TABLE 5.1 Metrics for Measuring the Success of Awareness Programs

Metric	Considerations
Number of security incidents due to human behavior	Can quickly show trends and deviations in behavior
	Can help understand root causes and estimate costs to the business
	May not be enough incidents to draw meaningful results
	May be other factors that affect the incidents
Audit findings	Generally conducted by independent and knowledgeable people who can provide third-party assurance on behaviors
	May be significant areas of awareness not reviewed
Results of staff surveys	If used before and after specific training, can be used to gauge the effectiveness of campaigns
	If sufficiently large, can provide statistical conclusions on staff behaviors
	Need to be targeted at verifying key messages
	Have to be carefully designed because staff may respond with "expected" answers and not true behaviors
Tests of whether staff follow correct procedures	Very good way of actually measuring behaviors and highlighting changes after training
	Have to be carefully planned and carried out because there could be breaches of employment and data protection laws
	Need a big enough sample if results are to be meaningful
Number of staff completing training	Need to decide what combination of classroom and computer-based training to use
	Have to consider what training to make mandatory
	May need to be tailored for different areas or regions
	May need regular and potentially costly updates

Cybersecurity Essentials Program

A cybersecurity essentials program serves two purposes. Its principal function is to target users of IT systems and applications, including company-supplied mobile devices and bring your own device (BYOD) policies, and develop sound security practices for these employees. Secondarily, it provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.

bring your own device (BYOD)

An IT strategy in which employees, business partners, and others use their personally selected and purchased client devices to execute enterprise applications and access data and the corporate

network. Typically, a BYOD policy spans smartphones and tablets, but the strategy may also be used for laptops, and it may include a subsidy.

NIST SP 800-16 defines cybersecurity essential program as a program that refers to an individual's familiarity with, and ability to apply, a core knowledge set that is needed to protect electronic information and systems. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know these essentials and be able to apply them. The training at this level should be tailored to a specific organization's IT environment, security policies, and risks.

Key topics that should be covered include:

- Technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges
- Common information and computer system security vulnerabilities
- Common cyberattack mechanisms, their consequences, and motivations for use
- Different types of cryptographic algorithms
- Intrusion, types of intruders, techniques, and motivation
- Firewalls and other means of intrusion prevention
- Vulnerabilities unique to virtual computing environments
- Social engineering and its implications to cybersecurity
- Fundamental security design principles and their role in limiting points of vulnerability

Role-Based Training

Role-based training is targeted at individuals who have functional rather than user roles with respect to IT systems and applications. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, whereas awareness seeks to focus an individual's attention on an issue or a set of issues.

The nature of the training depends on the role of the individual in the organization. SP 800-16 develops training recommendations based on differentiation of four major roles:

- Manage: The individual's job functions encompass overseeing a program or technical aspect of a security program; overseeing the life cycle of a computer system, network, or application; or having responsibilities for the training of staff.
- Design: The individual's job functions encompass scoping a program or developing procedures, processes, and architectures; or designing a computer system, a network, or an application.
- Implement: The individual's functions encompass putting programs, processes, or policies into place; or operation/maintenance of a computer system, a network, or an application.
- Evaluate: The individual's functions encompass assessing the effectiveness of any of the above actions.

SP 800-50 gives as an example of training an IT security course for system administrators, which addresses in detail the management controls, operational controls, and technical controls that should be implemented. Management controls include policy, IT security program management, risk management, and life cycle security. Operational controls include personnel and user issues, contingency planning, incident handling, awareness and training, computer support and operations, and physical and environmental security issues. Technical controls include identification and authentication, logical access controls, audit trails, and cryptography.

Education and Certification

An education and certification program is targeted at those who have specific security responsibilities, as opposed to IT workers who have some other IT responsibility but must incorporate security concerns.

Security education is normally outside the scope of most organization awareness and training programs. It more properly fits into the category of employee career development programs. Often, this type of education is provided by outside sources, such as college or university courses or specialized training programs.

The following are examples of such programs:

- Global Information Assurance Certification (GIAC) Security Essentials (GSEC): Designed for IT pros who want to demonstrate skills in IT system hands-on roles with respect to security tasks. Ideal candidates for this certification possess an understanding of information security beyond simple terminology and concepts.
- International Information System Security Certification Consortium (ISC)2 Certified Information Systems Security Professional (CISSP): Ideal candidates for this certification are information assurance pros who know how to define the information system architecture, design, management, and controls to ensure the security of business environments.
- (ISC)2 Systems Security Certified Practitioner (SSCP): Designed for those with proven technical skills and practical security knowledge in hands-on operational IT roles. The SSCP provides confirmation of a practitioner's ability to implement, monitor, and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity, and availability.
- Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM): For candidates who have an inclination toward organizational security and want to demonstrate the ability to create a relationship between an information security program and broader business goals and objectives. This certification ensures knowledge of information security and development and management of an information security program.
- SANS computer security training and certification: The SANS Institute provides intensive immersion training designed to an organization's staff master the practical steps necessary for defending systems and networks against the most dangerous threats—the ones being actively exploited.

People Management Best Practices

The SGP breaks down the best practices in the People Management category into two areas and six topics and provides detailed checklists for each topic. The areas and topics are:

- Human resource security: The objective of this area is to embed information security into each stage of the employment life cycle, which includes assigning ownership of information (including responsibility for its protection) to capable individuals and obtaining confirmation of their understanding and acceptance.

  - ✓ Employment life cycle: Provides checklists of desired actions during the three main phases of the employment life cycle: incoming, active employee, and termination
  - ✓ Ownership and responsibilities: Outlines practices to achieve individual accountability for information and systems, provide a sound management structure for individuals running or using them, and give their owners a vested interest in their protection
  - ✓ Remote working: Elaborates on the principle that individuals working in remote environments (for example, in locations other than the organization's premises) should be subject to authorization; protect computing devices and the information they handle against loss, theft, and cyber attack; be supported by security awareness material; and employ additional controls when traveling to high-risk countries or regions
- Security awareness/education: The objective of this area is to maintain a comprehensive, ongoing security awareness program to promote and embed expected security behavior in all individuals who have access to the organization's information and systems.
  - ✓ Security awareness program: Outlines the specific activities that should be undertaken, such as a security awareness program, to promote and embed expected security behavior in all individuals who have access to the organization's information and systems
  - ✓ Security awareness messages: Discusses topics that can be addressed in messages, tailored to the role and level of access of the individual
  - ✓ Security education/training: Lists key components of an education and training program

4.3 Information Management

The area of information management, according to the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP), encompasses four topics, all of which are covered in this chapter:

- Information classification and handling: Deals with methods of classifying and protecting an organization's information assets
- Privacy: Is concerned with threat, controls, and policies related to the privacy of personally identifiable information (PII)
- Document and records management: Is concerned with the protection and handling of the documents and records maintained by an organization
- Sensitive physical information: Covers specific issues related to the security of information assets in physical form

Information Classification and Handling

A necessary preliminary step to the development of security controls and policies for protecting information is that all the information assets of the organization must be classified according to their importance and according to the impact of security breaches involving the information. In addition, an organization needs to have clear procedures for ensuring that the link between a given type of information and its classification is maintained throughout the life cycle of the information and that procedures designate how the information is handled. ISO 27001, ISMS Requirements, puts all these

requirements under the generic security control category of information classification, with the following requirements:

- Classification of information: The classification scheme should take into account legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.
- Labeling of information: The organization should develop and implement an appropriate set of procedures for information labeling in accordance with the information classification scheme.
- Handling of assets: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme.

This section examines these three activities

Information Classification

It is useful to view information classification and handling in the overall context of risk management. National Institute of Standards and Technology (NIST) SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, defines a risk management framework that views the risk management process as consisting of six steps (see Figure 6.1):

1. Categorize: An organization needs to identify the information to be transmitted, processed, or stored by the system and define applicable levels of information categorization based on an impact analysis. The handling and safeguarding of PII should be considered. The purpose of the categorization step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the compromise or loss of organizational assets—including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.
2. Select: An organization needs to select an initial set of baseline security controls for the system based on the security categorization as well as tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. Implement: An organization needs to implement security controls and document how the controls are employed within the system and its environment of operation.
4. Assess: An organization needs to assess the security controls using appropriate assessment procedures. It must also determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements for the system.
5. Authorize: Management officially authorizes a system to operate or continue to operate based on the results of the security control assessment. This decision is based on a determination of the risk to organizational operations and assets resulting from the operation of the system and the determination that this risk is acceptable.

6. Monitor: An organization needs to continuously monitor security controls to ensure that they are effective over time as changes occur in the system and the environment in which the system operates. This includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

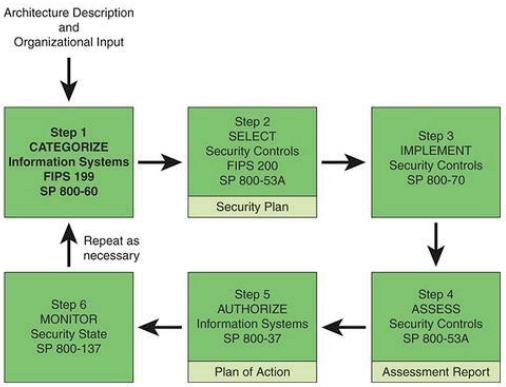


FIGURE 6.1 NIST Risk Management Framework

One of the inputs to the categorize step consists of architecture considerations. These considerations include:

- Information security architecture: Recall from Chapter 2, "Security Governance," that this is defined as a description of the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
- Mission and business processes: This refers to what the organization does, what the perceived mission or missions are, and what business processes are involved in fulfilling the mission.
- Information system boundaries: These boundaries, also referred to as authorization boundaries, establish the scope of protection for organizational information systems (that is, what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes.

The other major type of input to the categorize step consists of organizational inputs, including:

- Laws, directives, and policy guidance
- Strategic goals and objectives
- Priorities and resource availability
- Supply chain considerations

Before proceeding, let's distinguish some interrelated concepts that are essential to information classification:

- Information type: A specific category of information (for example, privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, directive, policy, or regulation.
- Security objective: The characteristic of security to be achieved, which typically consists of confidentiality, integrity, and availability.
- Impact: An adverse change to the level of business objectives achieved. Also called impact level or impact value. Typically either three (low, medium, high) or five (very low, low, medium, high, very high) levels are used.
- Security classification: The grouping of information into classes that reflect the value of the information and the level of protection required. Also called security categorization.

Classification provides people who deal with information with a concise indication of how to handle and protect that information. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. For example, an access control policy may dictate that access to a certain group of information is limited to personnel in certain defined roles. This approach reduces the need for case-by-case risk assessment and custom design of controls.

The way classification is approached varies from one standards body to another. ISO 27001 indicates that information is to be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. ISO 27002, Code of Practice for Information Security Controls, provides further guidance, stating that results of classification should indicate value of assets, depending on their sensitivity and criticality to the organization (for example, in terms of confidentiality, integrity, and availability).

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, provides a more precise definition of security categories, specifying the following generalized format for expressing a security category:

SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}

Thus, in FIPS 199, the category for an information type consists of three values. An organization may instead use a more descriptive set of terms and may make a distinction between critical and sensitive information, as discussed in Chapter, “People Management.”

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, defines the security categorization process as consisting of four steps, as shown in Figure 6.2. The following sections examine these four steps.

Identifying Information Types

The first step of the security categorization process according to SP 800-60 is to identify the information types to be classified. The result of this step should be an information taxonomy or catalog of information types. The level of detail, or granularity, must be decided by those involved in security governance. The determination may be based on factors such as the size of the organization, its range of activities, and the perceived overall level of risk.

The identification process must cover all forms of information, including:

- Electronic, consisting of data that can be stored, transmitted, and processed
- Electronic communication, such as email and text messages
- Spoken communication, such as telephone, Skype, and teleconferencing
- Multimedia information, such as video presentations and surveillance camera recordings
- Physical information, such as paper documents

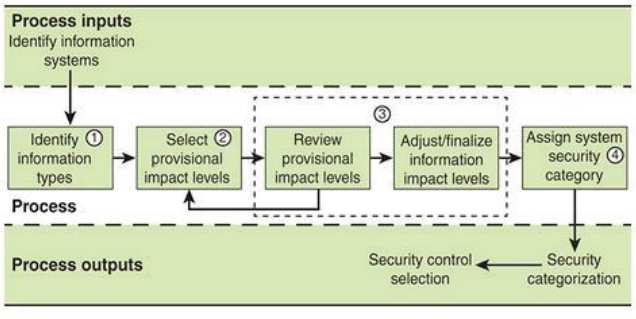


FIGURE 6.2 Security Categorization Process

SP 800-60 suggests three general organizational areas from which individual information types are defined:

- Mission-based information: This area encompasses types of information that relate specifically to the mission of the organization. For example, an organization in the healthcare field has information on what healthcare delivery services it provides, fee schedules, insurance arrangements, and policies for providing financial help to clients. A technology company has information about its research and development plans and goals, outside consulting arrangements, and long-range plans for new technology.
- Services delivery support functions: These are types of information that support the operation of the organization and relate to specific services or products offered by the organization. For example, in the area of risk management and mitigation, information types include contingency planning, continuity of operations, and service recovery.
- Back office support functions: These support activities enable the organization to operate effectively. SP 800-60 identifies five main groups of information types in this area:
    - ✓ Administrative management
    - ✓ Financial management
    - ✓ Human resource management
    - ✓ Information management
    - ✓ Technology management

As an example, in the information and technology management group, SP 800-60 lists system and network monitoring as an information type, with the following suggested classification:

{(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Whatever classification scheme an organization uses, it needs to have clear definitions of the various classification levels so that all those involved in classifying information types are working with the same understanding. A useful tool in this context is the Business Impact Reference Table (BIRT; refer to Figure 3.11 in Chapter, “Information Risk Assessment”), which provides consistent definitions to different types of impacts and severity levels.

Selecting and Reviewing Impact Levels

The second step of the security categorization process according to SP 800-60 is to assign security impact levels for the identified information types. The worksheet in Figure 3.4 and the asset register in Figure 3.5 examples of ways to document this process.

As an example, in the information and technology management group, SP 800-60 lists system and network monitoring as an information type, with the following suggested classification:

{(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

The third step of the security categorization process according to SP 800-60 is simply to review the provisional impact levels, allowing a range of managers and information owners to contribute to the process.

Assigning Security Categories

The final step of the security categorization process according to SP 800-60 is to assign a security classification for each information type. If the scheme suggested in SP 800-60 is used, the overall classification of an information type corresponds to its assessed impact, which is the highest of the confidentiality, integrity, and availability impacts. Otherwise, the impact information needs to be mapped into a classification scheme.

An important consideration is the naming of each classification level. The name should make sense in the context of the classification scheme's application. Classifying information types and properly naming them provide people who deal with information with a concise indication of how to handle and protect that information.

Information Labeling

A label needs to be associated with each instance of an information type so that its classification is clearly and unambiguously known. Methods are needed to ensure that a label is not separated from the information and that the content of the label is secure from unauthorized modification. The organization, for convenience and efficiency, may choose not to label non-confidential information.

For physical information types, some sort of physical label needs to be attached. This could be a readable label or bar code that adheres to the medium. In some cases, a radio-frequency identification (RFID) tag, which provides other security functionality, may be attached to the information medium. For information stored in electronic form, a number of techniques could be used, including using electronic watermarking, labeling headers and footers, embedding labels in metadata (such as document properties), and using filename conventions. Digital signatures can be used in electronic communications.

radio-frequency identification (RFID)

A data collection technology that uses electronic tags attached to items to allow the items to be identified and tracked with a remote system. The tag consists of an RFID chip attached to an antenna.

Information Handling

Information handling refers to processing, storing, communicating, or otherwise handling information consistent with its classification.

ISO 27002 lists the following relevant considerations:

- Access restrictions supporting the protection requirements for each level of classification
- Maintenance of a formal record of the authorized recipients of assets
- Protection of temporary or permanent copies of information to a level consistent with the protection of the original information
- Storage of IT assets in accordance with manufacturers' specifications
- Clear marking of all copies of media for the attention of the authorized recipient

Wherever possible, use automated tools to enforce the proper handling of information based on its classification level. These can be special-purpose tools for the following:

- Labeling information easily, correctly, and consistently
- Binding classification details to information (for example, using metadata, XML attributes, or similar techniques)
- Communicating their protection requirements effectively

An organization can also take advantage of broader information management tools, such as a document management system (DMS) or a records management system (RMS); these are discussed in Section 6.3.

The automated tools should facilitate integration with other security tools, such as encryption and digital signature modules and data loss prevention (DLP) packages.

data loss prevention (DLP)

A set of technologies and inspection techniques used to classify information content contained within an object—such as a file, an email, a packet, an application, or a data store—while at rest (in storage), in use (during an operation), or in transit (across a network). DLP tools also have the ability to dynamically apply a policy—such as log, report, classify, relocate, tag, and encrypt—and/or apply enterprise data rights management protections.

Privacy

ISO 7498-2, Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture, defines privacy as the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. The U.S. National Research Council's report At the Nexus of Cybersecurity and Public Policy [CLAR14] indicates that in the context of information, the term privacy usually refers to making ostensibly private information about an individual unavailable to parties who should not have that information. Privacy interests attach to the gathering, control, protection, and use of information about individuals.

In the context of cybersecurity, there is concern with the privacy of PII (as opposed, say, to video surveillance). Examples of information that might be considered PII are as follows:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number (PIN), such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, or financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of a person's face or other distinguishing characteristic), X-rays, fingerprints, or other biometric image or template data (for example, retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (for example, date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, financial information)

The two concepts of privacy and information security are closely related. On the one hand, the scale and interconnectedness of personal information collected and stored in information systems has increased dramatically, motivated by law enforcement, national security, and economic incentives. Economic incentives have perhaps been the main driving force. In a global information economy, it is likely that the most economically valuable electronic asset is aggregation of information on individuals

[JUDY14]. On the other hand, individuals have become increasingly aware of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities.

Although security and privacy are related, they are not equivalent. Cybersecurity, or information security, protects privacy. For example, an intruder seeking ostensibly private information (for example, personal emails or photographs, financial or medical records, phone calling records) may be stymied by good cybersecurity measures. In addition, security measures can protect the integrity of PII and support the availability of PII. However, At the Nexus of Cybersecurity and Public Policy [CLAR14] points out that certain measures taken to enhance cybersecurity can also violate privacy. For example, some proposals call for technical measures to block Internet traffic containing malware before it reaches its destination. But to identify malware-containing traffic, the content of all in-bound network traffic must be inspected. But inspection of traffic by any party other than its intended recipient is regarded by some as a violation of privacy because most traffic is in fact malware-free. Under many circumstances, inspection of traffic in this manner is also a violation of law.

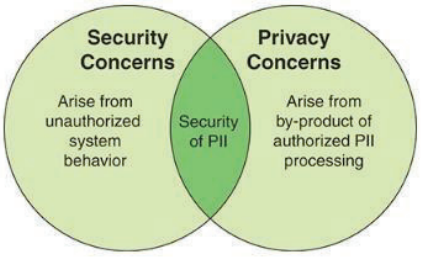


FIGURE 6.3 Relationship Between Information Security and Privacy

Figure 6.3, from NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, shows a non-proportional representation of the relationship between the privacy and security domains. While some privacy concerns arise from unauthorized activity, privacy concerns also can arise from authorized processing of information about individuals. Recognizing the boundaries and overlap between privacy and security is key to determining when existing security risk models and security-focused guidance may be applied to address privacy concerns—and where there are gaps that need to be filled in order to achieve an engineering approach to privacy. For instance, existing information security guidance does not address the consequences of a poor consent mechanism for use of PII, the purpose of transparency, what PII is being collected, or which changes in use of PII are permitted as long as authorized personnel are conducting the activity. Given these material distinctions in the disciplines, it should be clear that agencies cannot effectively manage privacy solely on the basis of managing security.

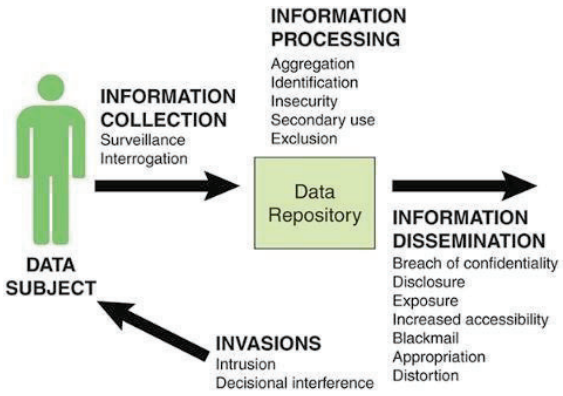


FIGURE 6.4 Potential Privacy Threats

Information collection is not necessarily harmful but can in some cases constitute a privacy threat. Two types of threat actions can occur:

- Surveillance: This is the watching, listening to, or recording of an individual's activities. It can be problematic and a violation of the right to privacy, especially if the target doesn't know about the surveillance.
- Interrogation: Interrogation is the pressuring of individuals to divulge information. For example, if certain fields in a form or in an online registration process are required in order to proceed, the individual is compelled, or at least pressured, to divulge information that he or she may prefer not to give.

Information processing refers to the use, storage, and manipulation of data that have been collected. Privacy issues relating to information processing arise from how data that have already been collected are handled and the ability to link the results back to the individuals to whom it pertains. Potential sources of privacy threats in this area include the following:

- Aggregation: Aggregation of data about an individual in various databases allows anyone with access to the aggregated data to learn more about an individual than could be learned from separate, and separately protected, data sets.
- Identification: It is possible, with sufficient data, to be able to aggregate data from various sources and use those data to identify persons who are not otherwise identified in the data sets.
- Insecurity: Insecurity refers to the improper protection and handling of PII. Identity theft is one potential consequence of insecurity. Another possible consequence is the dissemination of false information about a person, through alteration of that person's record.
- Secondary use: With secondary use, information about a person obtained for one purpose is used or made available for other purposes without consent.
- Exclusion: This is the failure to provide individuals with notice and input about their records.

Chase Bank Online Privacy Policy https://www.chase.com/digital/resources/privacy-security/privacy/onlineprivacy-policy

Google Privacy Policy https://www.google.com/intl/en_us/policies/privacy/?fg=1

The area of information dissemination encompasses the revelation of personal information or the threat of such revelation. Potential sources of privacy threat in this area include the following:

- Disclosure: Disclosure refers to the release of true information about a person. The potential harm is damage to reputation or position in some form. For example, a website may have a privacy link at the bottom of the main page that goes to a page that states the organization's privacy policy, which is focused on disclosure issues. Typical sections of a policy include what information is collected; use of information; disclosure of information; cookies, web beacons and other tracking technologies; and user choice. Links to two examples of policies are provided in the margin.
- Breach of confidentiality: Solove's A Taxonomy of Privacy [SOLO06] distinguishes between disclosure and breach of confidentiality, defining the latter as a disclosure that involves the violation of trust in a relationship. Thus, even if a disclosure itself is not harmful, the source of the disclosure is an entity that the person has a specific expectation of trust with. An example is the unauthorized release of medical information to a third party.
- Exposure: Exposure involves the exposure to others of certain physical and emotional attributes about a person, such as nude photographs or a video of a surgical procedure.
- Increased accessibility: With increased accessibility, information that is already publicly available is made easier to access. Increased accessibility does not create a new harm but does increase the likelihood and therefore the risk.
- Blackmail: Blackmail involves the threat of disclosure. Ransomware is an example of blackmail in the cybersecurity context.

- Appropriation: Appropriation involves the use of a person's identity or personality for the purpose of another. This is not identity theft, in that the offender is not claiming to be the victim. Rather, the offender makes use of the image or other identifying characteristic for some purpose, such as advertising, not authorized by the victim.
- Distortion: Distortion is the manipulation of the way a person is perceived and judged by others; it involves the victim being inaccurately exposed to the public. Distortion is achieved by modifying records associated with an individual.

The fourth area of privacy threats is referred to as invasions, and it involves impingements directly on the individual. Potential sources of privacy threat in this area include the following:

- Intrusion: In general terms, intrusion involves incursions into a person's life or personal space. In the context of cybersecurity, intrusion relates to penetrating a network or a computer system and achieving some degree of access privilege. Intrusion is a part of a variety of security threats but can also cause a privacy threat. For example, the actual intrusion, or threat of intrusion, into a personal computer can disrupt the activities or peace of mind of the personal computer user.
- Decisional interference: This is a broad legal concept. In terms of the present discussion, it involves the individual's interest in avoiding certain types of disclosure. To the extent that certain actions, such as registering for a government benefit, might generate data that could potentially be disclosed, the decision to perform those actions is deterred.

The preceding list of potential threats is comprehensive, and it is unlikely that any organization's set of privacy controls will attempt to address all of them. However, it is useful to have such a list in determining priorities for selecting privacy controls.

Privacy Principles and Policies

A number of international organizations and national governments have introduced standards, laws, and regulations intended to protect individual privacy. The following sections examine one standard and two regional examples.

ISO 29100

ISO 29100, Privacy Framework, lists the following 11 privacy principles that form the bases of this international standard:

- Consent and choice: Enables the PII principal (the person to whom the PII relates) to exercise consent to use PII and provides an opt-out/opt-in choice.
- Purpose legitimacy and specification: Defines the purposes for which PII can be used with clear specification to the PII principal.
- Collection limitation: Limits the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
- Data minimization: Minimizes the processing of PII.

- Use, retention, and disclosure limitation: Limits the use, retention, and disclosure (including transfer) of PII to that which is necessary in order to fulfill specific explicit and legitimate purposes.
- Accuracy and quality: Ensures that the PII is accurate, obtained from a reliable and verified source, and provides periodic checks of information integrity.
- Openness, transparency, and notice: Provides PII principals with clear and easily accessible information about the PII controller's policies, procedures, and practices with respect to the processing of PII.
- Individual participation and access: Gives PII principals the ability to access their PII, challenge its accuracy, and provide amendments or removals.
- Accountability: Adopts concrete and practical measures for PII protection.
- Information security: Protects PII under its authority with appropriate controls at operational, functional, and strategic levels to ensure the integrity, confidentiality, and availability of the PII and protects it against risks such as unauthorized access, destruction, use, modification, disclosure, or loss throughout the whole of its life cycle.
- Privacy compliance: Verifies and demonstrates that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors.

These principles include information security considerations but are much broader than that.

European Union's GDPR

One of the most comprehensive initiatives is European Union's (EU's) General Data Protection Regulation (GDPR), approved by the European Parliament in 2016, with an effective enforcement date of May 2108. It is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations, both public and private, across the region approach data privacy.

Table 6.1 summarizes the key principles at the heart of the GDPR.

TABLE 6.1 Key Principles of the EU's GDPR

Principle	Description
Fair, lawful, and transparent processing	The requirement to process personal data fairly and lawfully is extensive. It includes, for example, an obligation to tell data subjects what their personal data will be used for.
Purpose limitation	Personal data collected for one purpose should not be used for a new, incompatible, purpose. Further processing of personal data for archiving, scientific, historical, or statistical purposes is permitted, subject to appropriate laws and regulations.
Data minimization	Subject to limited exceptions, an organization should only process the personal data that it actually needs to process in order to achieve its processing purposes.
Accuracy	Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
Data retention periods	Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.
Data security	Technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.
Accountability	The controller is obliged to demonstrate that its processing activities are compliant with the data protection principles.

Kinast's 10 Key Facts Businesses Need to Note About the GDPR [KINA16] summarizes important aspects of the GDPR that organizations that do business in Europe need to be aware of:

- The GDPR applies to all companies worldwide that process personal data of EU citizens. Any company that works with information related to EU citizens must comply with the requirements of the GDPR, making it the first global data protection law. This aspect alone contributes significantly to all companies around the world taking data privacy more seriously.
- The GDPR widens the definition of personal data compared to prior EU regulations. As a result, parts of IT that have been unaffected by data protection laws in the past will need attention from businesses to ensure that they comply with the new regulation. The GDPR definition states that personal data means any information related to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- The GDPR tightens the rules for obtaining valid consent to use personal information. Having the ability to prove valid consent for using personal information is likely to be one of the biggest challenges presented by the GDPR. The GDPR states that the consent of the data subject means any freely given, specific, informed, and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
- The GDPR requires public authorities processing personal information to appoint a data protection officer (DPO), as well as other entities, when core activities require regular and systematic monitoring of data subjects on a large scale or consist of “processing on a large scale of special categories of data.
- The GDPR mandates data protection impact assessments. Data controllers must conduct assessments where privacy breach risks are high in order to minimize risks to data subjects. This means before an organization can implement projects involving personal information, it must conduct a privacy risk assessment and work with the DPO to ensure that it is in compliance as projects progress.
- The GDPR requires organizations to notify the local data protection authority of a data breach within 72 hours of discovering it. This means organizations need to ensure that they have technologies and processes in place that enable them to detect and respond to a data breach.
- The GDPR introduces the right to be forgotten. Also known as data erasure, the right to be forgotten entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing or a data subject withdrawing consent. This means organizations must get fresh consent before they alter the way they are using the data they have collected. It also means organizations must ensure that they have the processes and technologies in place to delete data in response to requests from data subjects.
- The GDPR requires that privacy be included in systems and processes by design. At its core, privacy by design calls for the inclusion of data protection from the outset of the designing of systems rather than as an addition.

The GDPR is an important landmark in the evolving integration of privacy in cybersecurity. Even organizations unaffected by this regulation should be aware of its provision and consider them in designing their own privacy controls.

U.S. Privacy Laws and Regulations

There is no single law or regulation covering privacy in the United States. Rather, a collection of federal privacy laws cover various aspects of privacy; many of them impose mandates on private organizations as well as government agencies and departments. These include:

- The Privacy Act of 1974: Specifies the rules that a federal agency must follow to collect, use, transfer, and disclose an individual's PII.
- The Fair and Accurate Credit Transaction Act of 2003 (FACTA): Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA): Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records.
- The Family Educational Rights and Privacy Act of 1974 (FERPA): Designed to protect students and their families by ensuring the privacy of student educational records.
- The Gramm–Leach–Bliley Act of 1999 (GLBA): Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data.
- Federal Policy for the Protection of Human Subjects: Outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects. Published in 1991 and codified in separate regulations by 15 federal departments and agencies.
- The Children's Online Privacy Protection Act (COPPA): Governs the online collection of personal information from children under age 13.
- The Electronic Communications Privacy Act: Generally prohibits unauthorized and intentional interception of wire and electronic communications during the transmission phase and unauthorized access of electronically stored wire and electronic communications.

Privacy Controls

So far, this section has looked at potential threats to privacy and a broad approach to government regulation of privacy. To counter privacy threats and comply with government laws and regulations, organizations need a set privacy controls that encompass their privacy requirements and that respond to legal requirements. A useful and comprehensive set of such controls is provided in NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations. The set is organized into 8 families and a total of 24 controls:

- Authority and purpose: This family ensures that organizations identify the legal bases that authorize a particular PII collection or activity that impacts privacy and specify in their notices the purpose(s) for which PII is collected. These controls would be embodied in a policy statement.
- Accountability, audit, and risk management: This family consists of controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk. It includes the following controls:

- ✓ Governance and privacy program: This includes designating a chief privacy officer, monitoring national privacy laws, allocating sufficient resources for an organizationwide privacy program, developing a strategic privacy plan, and developing a privacy policy.
- ✓ Privacy impact and risk assessment: This includes implementing a risk management process and conducting privacy impact assessments where appropriate.
- ✓ Privacy requirements for contractors and service providers: This involves establishing and including in contracts privacy responsibilities.
- ✓ Privacy monitoring and auditing: This involves monitoring and auditing privacy controls and the internal privacy policy to ensure effective implementation.
- ✓ Privacy awareness and training: This involves implementing awareness programs for all employees and training for those with privacy responsibilities.
- ✓ Privacy reporting: This involves developing any mandated privacy reports for regulatory bodies.
- ✓ Privacy-enhanced system design and development: This involves designing information systems to support privacy by automating privacy controls.
- ✓ Accounting of disclosures: This involves keeping an accurate accounting of disclosures and making it available to the person affected.

- Data quality and integrity: The objective of this family is to ensure that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used. This control includes procedures for confirming to the greatest extent possible the quality of the PII collected or created and documenting processes to ensure integrity.
- Data minimization and retention: This family includes the following controls:
  - ✓ Minimization of PII: This involves establishing procedures to identify the minimum relevant and necessary PII.
  - ✓ Data retention and disposal: This involves retaining PII only as long as necessary and providing secure methods of deletion and destruction.
  - ✓ Minimization of PII used in testing, training, and research: This involves developing and implementing policies and procedures to minimize use of PII in testing, training, and research.
- Individual participation and redress: This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. It includes the following:
  - ✓ Consent: This involves providing means, where feasible and appropriate, for individuals to express explicit consent to the use of their PII and to be aware of and consent to all additional uses of their PII beyond the initial consent.
  - ✓ Individual access: This involves providing individuals the ability to have access to their PII.
  - ✓ Redress: This involves providing a process by which an individual can have inaccurate PII corrected.
  - ✓ Complaint management: This involves implementing a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
- Security: This family ensures that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure. These controls are meant to supplement the organization's security controls

that may be relevant to privacy. Included are the maintenance of an inventory of PII and developing a privacy incident response plan.

- Transparency: This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities. This includes procedures for notifying individuals of the status of their PII and dissemination of privacy program information.
- Use limitation: This family ensures that the scope of PII use is limited to the intended purpose. This includes developing policies and procedures to limit internal access to PII to only those personnel who require and are authorized access, as well as similar policies and procedures for third parties outside the organization.

With respect to awareness and training, NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, suggests covering the following topics:

- Definition of PII
- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents and reporting

The scope of privacy controls that an organization needs to implement depends on the extent of the organization's involvement with PII.

Document and Records Management

A specific class of information consists of documents and records. There are no standardized, universally accepted definitions in this realm, but for this context, the following definitions are appropriate:

- Document: A set of information pertaining to a topic, structured for human comprehension, represented by a variety of symbols, and stored and handled as a unit. A document may be modified.
- Record: A subclass of documents that clearly delineates terms and conditions, statements, or claims or that provides an official record. Generally a record, once created, is not modified.

The following additional definitions are useful for this section:

- Document management: The capture and management of documents within an organization. The term originally implied only the management of documents after they were scanned into a computer. Subsequently, it became an umbrella term embracing document imaging, workflow, text retrieval, and multimedia.
- Document management system: Software that manages documents for electronic publishing. It generally supports a large variety of document formats and provides extensive access control and searching capabilities across networks. A document management system may support multiple versions of a document and may be able to combine text fragments written

by different authors. It often includes a workflow component that routes documents to the appropriate users.

- Records management: The creation, retention, and scheduled destruction of an organization's sensitive or important paper and electronic records. Computer-generated reports fall into the records management domain, but traditional data processing files do not.
- Records management system: Software that provides tools for and aids in records management.

Table 6.2, based on the CMS Wire article "6 Ways Document Management and Records Management Differ" [ROE10], summarizes some key differences between document and records management.

TABLE 6.2 Differences Between Document and Records Management

Function	Document Management	Records Management
Purpose	Makes it easier for users with a shared purpose to access and manage documents. It also allows these users to collaborate on those documents.	Is concerned with identifying, storing, maintaining, and managing data that is used to describe events in an organization's work cycle that are related to statutory, regulatory, fiscal, or operational activities within the organization.
Storage	Includes the ability to access and revise, possibly with version tracking and histories.	Intended to keep records with their original format and content.
Automated processes	May include capture and storage, control of the document's life cycle, and access control.	Manages records in a consistent manner, preserving content as well as the context and structure they came from. Supports auditing of records in their original form.
Security	Provides access control, with a means of tracking who has been using a document, when it was accessed, and any changes that were made to the document.	Provides more stringent security, including authentication and data integrity.
Disposal	The disposal of documents in a document management system occurs when the life cycle of the document has been complete and is no longer needed in the business process. Disposal can consist of simple destruction or turning the documents into records. The decision to turn a document into a record depends on the need of the company and whether there are legal requirements to hold on to the documents.	The destruction of records is generally regulated by law with strict procedures so that the information contained in them will not be disclosed.

Document Management

Document management is a key business function because of the importance of documents to the operation of an organization. Table 6.3, from the *MIS Quarterly* article "Electronic Document Management: Challenges and Opportunities for Information Systems Managers" [SPRA95], lists some of the important roles and purposes of documents within an organization.

TABLE 6.3 Roles of Documents

Role	Examples
To record or to document contracts and agreements	Employment contracts, maintenance agreements, consulting contracts, purchase agreements, leases, mortgages, loans, and so on
To record policies, standards, and procedures	Procedure manuals, standards specifications, instruction handbooks, executive memos and letters that state corporate policy, and so on
To represent a view of reality at a point in time (reports and plans)	Status reports, problem analyses, operational reports, staff recommendations, budgets, strategic plans, and so on
To create an image or impression	Annual reports, marketing brochures, TV or radio commercials, and so on
To generate revenue as a product	A book for sale by a publisher, a report by a consulting firm to be sold to its client, a news item from a wire service, a reference from a bibliographic service, and so on
To support revenue by adding value to a product	A user's manual for a car or an appliance or a software product, a warranty form, a catalog, a discount coupon for another purchase, and so on
To act as a mechanism for communication and interaction among people and groups	Memos, letters, presentations, email messages, minutes of meetings, and so on
To act as a vehicle for organizational process	Orders, invoices, approval letters, most business forms, and so on
To provide a discipline for capture and articulation of concepts and ideas	Nearly all the kinds of documents that carry concepts and ideas

Although the focus of document management and of document management systems is the ease of creation and use of documents, security must be an integral aspect. One key element is the management of the document life cycle, including creation, categorization, storage, retrieval, modification, and destruction. Security mechanisms need to be implemented to ensure that security objectives are met during each stage of the document life cycle.

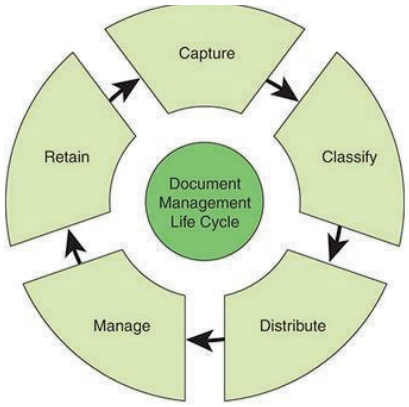


FIGURE 6.5 Document Management Life Cycle

An important security policy consideration with document management is document retention. Classify documents by type with respect to legal and regulatory requirements for retention. Define a process for third-party access to documents. And specify the retention period for each class of documents. Reclassify any documents as records that are to be retained indefinitely after they are no longer available for modification.

Figure 6.5 illustrates a typical document management life cycle.

It consists of the following phases:

- Capture: Capture documents from various sources and place them in the document management system.
- Classify: Classify a document to give it business context and to allow metadata to be assigned.
- Distribute: Allow documents to continue through the life cycle, gathering additional information to be reviewed and approved.
- Manage: Present documents to users through various interfaces and applications to make the delivery as seamless as possible.
- Retain: Keep the document for a period defined in the classification before archiving or destruction.

As in other areas, an organization should develop acceptable use policies and awareness programs with respect to documents.

Records Management

Records management is a vital business function that requires stronger security measures than those for document management. You should treat as records those documents that have significant business value or are within the scope of relevant laws or regulations. A general process for records management is shown in Figure 6.6.

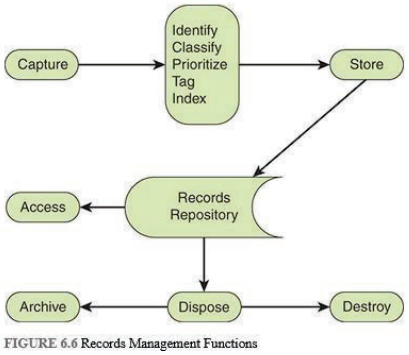


FIGURE 6.6 Records Management Functions

Important guidelines for securing records include:

- Develop clear and detailed policies that define what documents should be classified as records.
- Store only a single instance of the document, whether it is physical or electronic.
- Define access restrictions as tightly as is reasonable.
- Monitor each record to ensure compliance with the organization's records retention policy.

- Ensure secure destruction of a record or secure archival of the record when the retention period has expired.

The Information Security Guide developed by the Higher Education Information Security Council (HEISC), suggests the following considerations for developing a records management program [HEIS14]:

- Establish a strategic planning group that includes top managers/executives to support the program.
- Write and communicate a directive on the objectives of the program, which should link to organizational goals.
- Identify a records manager to oversee all aspects of the program, including ongoing management and use of internal personnel or outside consultants.
- Write a policy statement identifying purpose, responsibility, objectives, and so on.
- Determine staffing and organizational structure for overseeing the program's day-to-day operations.
- Conduct a preliminary file purge of non-records from filing systems.
- Complete a records inventory.
- Develop and implement a retention schedule.
- Protect the vital records of the organization.
- Develop a records management manual with defined policies and procedures.
- Implement filing standards throughout.
- Identify a process for managing inactive records in a low-cost space.
- Implement forms management and reports management programs.
- Automate records management where it makes sense to do so.
- Make records management a high priority.

A key aspect of records management is the retention and disposition policy. The life cycle of records is distinguished in three stages:

- Active: Currently used to support the organization's functions and reporting requirements. Generally, active records are those that are referred to often during the regular course of business.
- Semi-active: Records that are no longer needed to carry out current activities but must still be retained to meet the organization's administrative, fiscal, legal, or historical requirements. These records can be stored in less accessible storage.
- Inactive: Records that are no longer required to carry out the administrative or operational functions for which they were created and that are no longer retrieved or accessed. Such records can either be archived or destroyed.

Sensitive Physical Information

Sensitive information held in physical form (that is, sensitive physical information) needs to be protected against corruption, loss, and unauthorized disclosure. Examples of sensitive physical information are blank checks, bonds, and printouts of documents such as personal information, financial projections, business plans, and product designs.

COBIT 5 summarizes the requirement for protection of sensitive physical information as follows: Provide adequate, specific information security measures for data and information that exist in non-

digital forms, including documents, media, facilities, physical perimeter, and transit. COBIT 5 lists the following as supporting technologies:

- Closed-circuit television (CCTV)
- Locks
- Alarms
- Access control
- Vaulting
- Intelligence reports
- First responder interfaces
- Facilities management solutions
- Fire protection systems
- Time locks
- Physical access solutions

The key issues involved with securing physical information throughout its life cycle include the following:

- Identify and document: Each item of physical information needs to be identified properly and its existence documented.
- Classification: Every physical document or other type of media (for example, DVD) should be classified using the same security categories used for all other organization assets.
- Label: The appropriate security classification label must be affixed to or incorporated into the document itself.
- Storage: Secure storage is needed. This may be a safe, a secure area of the facility, or other physical means of restricting and controlling access.
- Secure transport: If sensitive information is to be sent by a third party, such as a courier or shipping service, policies and procedures must be in place to ensure that this is done securely. Employees who carry documents must be given guidance and the technical means needed to maintain security.
- Disposal: A retention and disposal policy is needed, and secure means of destroying physical information must be followed.

Information Management Best Practices

The SGP breaks down the best practices in the information management category into two areas and four topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Information classification and privacy: This area includes the following topics:
  - ✓ Information classification and handling: The objective for this topic is to develop an information classification scheme that provides consistent classification of all forms of information, including electronic, physical, and spoken. The scheme should be supported by information handling guidelines to help protect information against corruption, loss, and unauthorized disclosure.
  - ✓ Information privacy: This topic deals with the need for implementing policies and security controls for the handling of PII. The SGP recommends a separate privacy policy document and an acceptable use document. Methods are required for dealing with breaches, including detection, response, and notification.
- Information protection: This area includes the following topics:

- ✓ Document management: This topic specifies how to manage documents through the life cycle of creation, categorization, storage, retrieval, modification, and destruction. Topics covered include employee obligations, backup and archive, document retention policy, and enhanced protection for records
- ✓ Sensitive physical information: The objective is to protect sensitive physical information in accordance with information security and regulatory requirements, preserve the integrity of sensitive physical information, and protect it from unauthorized disclosure. The SGP provides checklists for identification and labeling; storage of sensitive physical information; protection against unauthorized disclosure of sensitive physical information; secure transportation of sensitive physical information; and handling and disposing of sensitive physical information.

4.4 Review Questions / Case Studies / Projects

1. What does the term employment life cycle mean?
2. How can you categorize the security problems caused by employees?
3. What should a company check, in general, before hiring a new employee?
4. How can a company ensure personnel security?
5. Suppose X has resigned from company Alpha. What actions should the security officer of Alpha take before relieving X from duty?
6. What are the four phases of the cybersecurity learning continuum?
7. What should be the goals for a security awareness program?
8. Explain the term privacy from an information point of view.
9. Does privacy have the same meaning as information security?
10. In today's information scenario, what are some possible types of threats in the information collection process?
11. How can privacy be violated at the information processing stage?
12. List some potential privacy threats that may occur as information is being disseminated.
13. What kind of privacy threats are exposed by invasions?
14. Enumerate and briefly explain key principles of the GDPR.
15. How does NIST SP 800-53 organize privacy controls?
16. Differentiate between the terms document and record.
17. What is the life cycle of a record?
18. What are some supporting technologies that can be used to protect sensitive physical information?
19. What are some key issues in securing physical information throughout its life cycle?

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **List and define the key functions that a network management system should include.**
- **Give an overview of a network management system and explain each of its key components.**
- **Explain the role of firewalls as part of a computer and network security strategy.**
- **List the key characteristics of firewalls.**
- **Understand the security considerations for various aspects of network management.**
- **Understand the security considerations for various aspects of electronic communication.**
- **Present an overview of network and communications best practices.**

5.1 Introduction

This chapter provides a survey of security and security management issues related to two broad and related topics: networks and electronic communications. The chapter begins with an overview of network management concepts. Following this are sections covering firewalls and virtual private networks. With this background, the chapter then addresses the specific security concerns involved with network management. Next, the chapter examines electronic communications in the enterprise environment, including email, instant messaging, voice over IP networks, and telephony and conferencing.

5.2 Network Management Concepts

This section provides an overview of network management. Let's begin by looking at the requirements for network management. This will provide an idea of the scope of the task to be accomplished. To manage a network, it is fundamental to know something about the current status and behavior of that network.

Effective management requires a network management system that includes a comprehensive set of data gathering and control tools and that is integrated with the network hardware and software. Let's look at the general architecture of a network management system.

Network Management Functions

Table 12.1 lists key functions of network management, as suggested by the International Organization for Standardization (ISO) in ISO 7498-4, Open Systems Interconnection—Basic Reference Model—Part 4: Management Framework. A much more detailed description of these network management functions is contained in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) M.3400, Telecommunications Management Functions. These categories provide a useful way of organizing this discussion of requirements.

TABLE 12.1 ISO Management Functional Areas

Category	Description
Fault management	The facilities that enable the detection, isolation, and correction of abnormal operation of the Open Systems Interconnection (OSI) environment
Accounting management	The facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects
Configuration management	The facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services
Performance management	The facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities
Security management	The aspects of security essential to operate OSI network management correctly and to protect managed objects

Fault Management

To maintain proper operation of a complex network, make sure that systems as a whole, as well as each essential component individually, are in proper working order. When a fault occurs, it is important to do the following as rapidly as possible:

- Determine exactly where the fault is
- Isolate the rest of the network from the failure so it continues to function without interference
- Reconfigure or modify the network in such a way as to minimize the impact of operation without the failed component or components
- Repair or replace the failed components to restore the network to its initial state

Central to the definition of fault management is the fundamental concept of a fault, as distinguished from an error. A fault is an abnormal condition that causes a device or system component to fail to perform in a required manner and that requires management attention (or action) for repair. A fault is usually indicated by failure to operate correctly or by excessive errors. For example, if a communications line is physically cut, no signals get through. Or a crimp in the cable can cause wild distortions so that there is a persistently high bit error rate. Certain errors (for example, a single bit error on a communication line) can occur occasionally and are not normally considered to be faults. It is usually possible to compensate for errors using the error control mechanisms of the various protocols.

Users expect fast and reliable problem resolution. Most end users tolerate occasional outages. When these infrequent outages do occur, however, users generally expect to receive immediate notification and expect the problem be corrected almost immediately. Providing such a level of fault resolution requires very rapid and reliable fault detection and diagnostic management functions. The impact and duration of faults are also minimized by the use of redundant components and alternate communication routes, to give the network a degree of fault tolerance. An organization should make sure the fault management capability is redundant to increase network reliability.

Users expect to be kept informed of the network status, including both scheduled and unscheduled disruptive maintenance. Users expect reassurance of correct network operation through mechanisms that use confidence tests or that analyze dumps, logs, alerts, or statistics. After correcting a fault and restoring a system to its full operational state, the fault management service must ensure that the problem is truly resolved and that no new problems are introduced. This requirement is called problem tracking and control.

To satisfy requirements, fault management generally includes functions to do the following:

- Maintain and examine error logs
- Accept and act upon error detection notifications
- Trace and identify faults
- Carry out sequences of diagnostic tests
- Correct faults

As with other areas of network management, fault management should have minimal effect on network performance.

Accounting Management

In many enterprise networks, individual divisions or cost centers, or even individual project accounts, are charged for the use of network services. These are internal accounting procedures rather than actual cash transfers, but they are important to the participating users nevertheless. Furthermore, even if no such internal charging is employed, a network manager needs to be able to track the use of network resources by user or user class for a number of reasons, including the following:

- A user or group of users may abuse their access privileges and burden the network at the expense of other users.
- Users can make inefficient use of the network, and the network manager can assist in changing procedures to improve performance.
- The network manager is in a better position to plan for network growth if user activity is known in sufficient detail.

A network manager must specify the kinds of accounting information to be recorded at various nodes, the desired interval between successive transmissions of the recorded information to higher-level management nodes, and the algorithms used in calculating the charging.

To limit access to accounting information, the accounting facility must provide the capability to verify users' authorization to access and manipulate that information.

To satisfy requirements, accounting management generally includes functions to do the following:

- Inform users of costs incurred or resources consumed

- Enable accounting limits to be set and tariff schedules to be associated with the use of resources
- Enable costs to be combined where multiple resources are invoked to achieve a given communication objective

Configuration Management

Modern data communication networks are composed of individual components and logical subsystems (for example, the device driver in an operating system) that are configured to perform many different applications. The same device, for example, can be configured to act either as a router or as an end system node or both. Once it is decided how a device is to be used, the configuration manager chooses the appropriate software and set of attributes and values (for example, a transport layer retransmission timer) for that device.

Configuration management is concerned with initializing a network and gracefully shutting down part or all of the network. It is also concerned with maintaining, adding, and updating the relationships among components and the status of components during network operation.

Startup and shutdown operations on a network are part of configuration management. It is often desirable for these operations on certain components to be performed unattended (for example, starting up or shutting down a network interface unit). A network manager needs to be able to identify initially the components that comprise the network and to define the desired connectivity of those components. Those who regularly configure a network with the same or a similar set of resource attributes need ways to define and modify default attributes and to load those predefined sets of attributes into the specified network components. A network manager needs to be able to change the connectivity of network components when users' needs change. Reconfiguration of a network is often desired in response to performance evaluation or in support of network upgrade, fault recovery, or security checks.

Users often need to, or want to, be informed of the status of network resources and components. Therefore, when changes in configuration occur, the network or system manager should notify users of these changes. The network or system manager should also generate configuration reports either on some routine periodic basis or in response to a request for such a report. Before reconfiguration, users often want to inquire about the upcoming status of resources and their attributes.

Network managers usually want only authorized users (operators) to manage and control network operation (for example, software distribution and updating).

To satisfy requirements, configuration management generally includes functions to do the following:

- Set the parameters that control the routine operation of the system
- Associate names with managed objects and sets of managed objects
- Initialize and close down managed objects
- Collect information on demand about the current condition of the system
- Obtain announcements of significant changes in the condition of the system
- Change the configuration of the system

Performance Management

Modern data communications networks are composed of many and varied components, which must intercommunicate and share data and resources. In some cases, it is critical to the effectiveness of an application that the communication over the network be within certain performance limits. Performance management of a computer network comprises two broad functional categories: monitoring and controlling. Monitoring is the function that tracks activities on the network. The controlling function enables performance management to make adjustments to improve network performance. Some of the performance issues of concern to a network manager are as follows:

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?

To deal with these concerns, a network manager must focus on some initial set of resources to be monitored to assess performance levels. This includes associating appropriate metrics and values with relevant network resources as indicators of different levels of performance. For example, what count of retransmissions on a transport connection is considered to be a performance problem requiring attention? Performance management, therefore, must monitor many resources to provide information in determining network operating level. By collecting this information, analyzing it, and then using the resultant analysis as feedback to the prescribed set of values, a network manager becomes more and more adept at recognizing situations that indicate present or impending performance degradation.

Before using a network for a particular application, a user may want to know such things as the average and worst-case response times and the reliability of network services. Thus, performance must be known in sufficient detail to respond to specific user queries. End users expect network services to be managed in such a way as to afford their applications consistently good response time.

Network managers need performance statistics to help them plan, manage, and maintain large networks. Performance statistics are used to recognize potential bottlenecks before they cause problems to end users. They also enable network managers to take appropriate corrective action. This action either takes the form of changing routing tables to balance or redistribute traffic load during times of peak use or when a bottleneck is identified by a rapidly growing load in one area. Over the long term, capacity planning based on such performance information indicates the proper decisions to make, for example, with regard to expansion of lines in that area.

To satisfy requirements, performance management generally includes functions to do the following:

- Gather statistical information
- Maintain and examine logs of system state histories
- Determine system performance under natural and artificial conditions
- Alter system modes of operation for the purpose of conducting performance management activities

Security Management

Security management is concerned with generating, distributing, and storing encryption keys. Passwords and other authorization or access control information must be maintained and distributed. Security management is also concerned with monitoring and controlling access to computer networks and access to all or part of the network management information obtained from the network nodes. Logs are an important security tool, and therefore security management is very much involved with the collection, storage, and examination of audit records and security logs, as well as with the enabling and disabling of these logging facilities.

Security management provides facilities for protection of network resources and user information. Network security facilities should be available for authorized users only. Users want to know that the proper security policies are in force and effective and that the management of security facilities is itself secure.

The purpose of security management is to support the application of security policies by means of functions that include the following:

- The creation, deletion, and control of security services and mechanisms
- The distribution of security-related information
- The reporting of security-related events

Network Management Systems

A large network cannot be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools. The urgency of the need for such tools is increased, and the difficulty of supplying such tools is also increased, if the network includes equipment from multiple vendors. Moreover, the increasing decentralization of network services, as exemplified by the increasing importance of workstations and client/server computing, makes coherent and coordinated network management increasingly difficult. In such complex information systems, many significant network assets are dispersed far from network management personnel.

Components of a Network Management System

A network management system is a collection of tools for network monitoring and control that is integrated in the following senses:

- A single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks
- A minimal amount of separate equipment, as most of the hardware and software required for network management is incorporated into the existing user equipment

A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network

management tasks resides in the host computers and communications processors (for example, front-end processors, terminal cluster controllers, switches, routers). A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of each element and link known to the system. The active elements of the network provide regular feedback of status information to the network control center. In this context, the term element refers to network devices and end systems attached to the network.

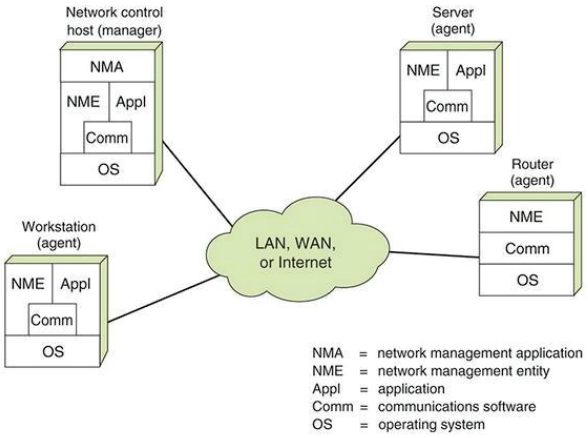


FIGURE 12.1 Components of a Network Management System

Figure 12.1 suggests the principal components of a network management system. Each network node contains a collection of software devoted to the network management task, referred to in the diagram as a network management entity (NME).

Each NME performs the following tasks:

- Collects statistics on communications and network-related activities
- Stores statistics locally
- Responds to commands from the network control center, including commands to do the following:
  - ✓ Transmit collected statistics to the network control center
  - ✓ Change a parameter (for example, a timer used in a transport protocol)
  - ✓ Provide status information (for example, parameter values, active links)
  - ✓ Generate artificial traffic to perform a test
- Sends messages to the NCC when local conditions undergo significant changes

At least one host in the network is designated as the network control host, or manager. In addition to the NME software, the network control host includes a collection of software called the network management application (NMA). The NMA includes an operator interface to allow an authorized user to manage the network. The NMA responds to user commands by displaying information and/or by issuing commands to NMEs throughout the network. This communication is carried out using an application-level network management protocol that employs the communications architecture in the same fashion as any other distributed application.

Every other node in the network that is part of the network management system includes an NME and, for purposes of network management, is referred to as an agent. Agents include end systems that support user applications as well as nodes that provide a communications service, such as front-end processors, cluster controllers, bridges, and routers.

As depicted in Figure 12.1, the network control host communicates with and controls the NMEs in other systems. For maintaining high availability of the network management function, two or more network control hosts are used. In normal operation, one of the hosts is actively used for control, while the others are idle or simply collecting statistics. If the primary network control host fails, the backup system is used.

Distributed Network Management Systems

In a traditional centralized network management scheme, one host in the configuration has the role of a network management station; there can be one or two other management stations in a backup role. The remainder of the devices on the network contain agent software and a local database to allow monitoring and control from the management station. As networks grow in size and traffic load, such a centralized system is unworkable. Too much burden is placed on the management station, and there is too much traffic, with reports from every single agent having to wend their way across the entire network to headquarters. In such circumstances, a decentralized, distributed approach works best (see the example in Figure 12.2). In a decentralized network management scheme, there can be multiple top-level management stations, which are referred to as management servers. Each such server can directly manage a portion of the total pool of agents. However, for many of the agents, the management server delegates responsibility to an intermediate manager. The intermediate manager plays the role of manager to monitor and control the agents under its responsibility. It also plays an agent role to provide information and accept control from a higher-level management server. This type of arrangement spreads the processing burden and reduces total network traffic.

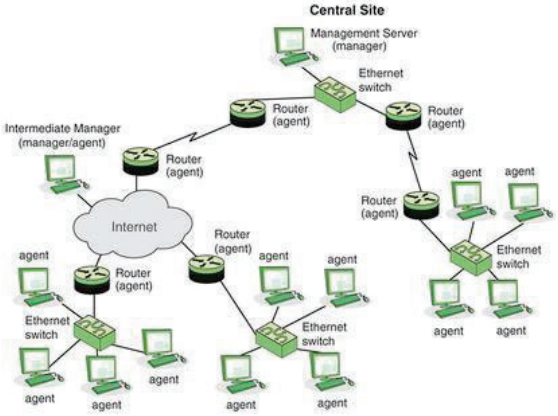


FIGURE 12.2 Example of a Distributed Network Management Configuration

Network Management Architecture

Cisco has developed a hierarchical network management architecture [CISC07] based on ITU M.3400, as shown in Figure 12.3.

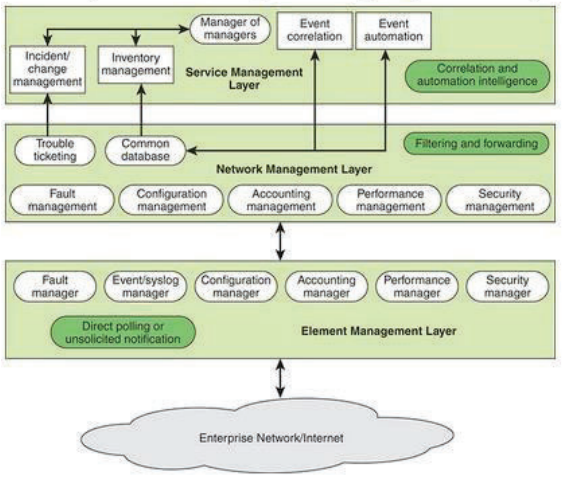


FIGURE 12.3 Network Management System Logical Architecture

The element management layer provides an interface to the network devices and communications links in order to monitor and control them. This layer captures events and fault occurrences through a combination of direct polling and unsolicited notification by network elements. Management function modules provide interfaces to specific elements, allowing elements from different manufacturers to be incorporated under a single network management system.

The network management layer (NML) provides a level of abstraction that does not depend on the details of specific elements. In terms of event management, this layer takes input from multiple elements (which in reality can be different applications), correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that occurred. The NML provides a level of abstraction above the element management layer in that operations personnel are not “weeding” through potentially hundreds of unreachable or node down alerts but instead are focusing on the actual event, such as failure of an area-border router. Thus, this layer performs a filtering function, only providing a more aggregated view of the network through a common database across all five functions as well as a trouble ticketing facility.

The service management layer is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems. The goal is to move traditional network management environments and the operations personnel from element management (managing individual alerts) to network management (managing network events) to service management (managing identified problems).

5.3 Firewalls

The firewall is an important complement to host-based security services such as intrusion detection systems. Typically, a firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing are imposed. Firewalls are also deployed internally in an enterprise network to segregate portions of the network.

A firewall provides an additional layer of defense, insulating internal systems from external networks or other parts of the internal network. This follows the classic military doctrine of "defense in depth," which is applicable to IT security.

Firewall Characteristics

"Network Firewalls" [BELL94] lists the following design goals for a firewall:

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
- Only authorized traffic, as defined by the local security policy, is allowed to pass. Various types of firewalls are used, and they implement various types of security policies, as explained later in this chapter.
- The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

In general terms, firewalls use four techniques that to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four techniques:

- Service control: Determines the types of Internet services that can be accessed—inbound or outbound. The firewall can filter traffic on the basis of IP address, protocol, or port number; provide proxy software that receives and interprets each service request before passing it on; or host the server software itself, such as a web or mail service.
- Direction control: Determines the direction in which particular service requests are initiated and allowed to flow through the firewall.
- User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It can also

be applied to incoming traffic from external users, though this requires some form of secure authentication technology, such as that provided in IP Security (IPsec).

- Behavior control: Controls how particular services are used. For example, the firewall can filter email to eliminate spam or enable external access to only a portion of the information on a local web server.

Before proceeding to the details of firewall types and configurations, let's consider the capabilities that are within the scope of a firewall:

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection against various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
- A firewall provides a location for monitoring security-related events. Audits and alarms are implemented on the firewall system.
- A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function, which audits or logs Internet usage.
- A firewall serves as a platform for implementing virtual private networks (as discussed in the following section).

Firewalls have limitations, including the following:

- A firewall cannot protect against attacks that bypass the firewall. Internal systems can have dial-out capability to connect to an ISP. An internal LAN can support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- A firewall does not fully protect against internal threats, such as disgruntled employees or employees who unwittingly cooperate with external attackers.
- An improperly secured wireless LAN can be accessed from outside the organization. An internal firewall that separates portions of an enterprise network does not guard against wireless communications between local systems on different sides of the internal firewall.
- A laptop, PDA, or portable storage device can be used and infected outside the corporate network and then attached and used internally.

Types of Firewalls

A firewall acts as a packet filter. It operates as a positive filter, allowing only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type, a firewall can examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. This section looks at the principal types of firewalls, shown in Figure 12.4.

Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing Internet Protocol (IP) packet and then forwards or discards the packet (see Figure 12.4b). This type of firewall is typically configured to filter packets going in both directions (from and to the internal network).

Filtering rules are based on information contained in a network packet:

- Source IP address: The IP address of the system that originated the IP packet (for example, 192.178.1.1)
- Destination IP address: The IP address of the system the IP packet is trying to reach (for example, 192.168.1.2)
- Source and destination transport-level addresses: The transport-level (for example, Transmission Control Protocol [TCP] or User Datagram Protocol [UDP]) port number, which defines applications such as Simple Network Management Protocol (SNMP) or Telnet
- IP protocol field: The transport protocol
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for

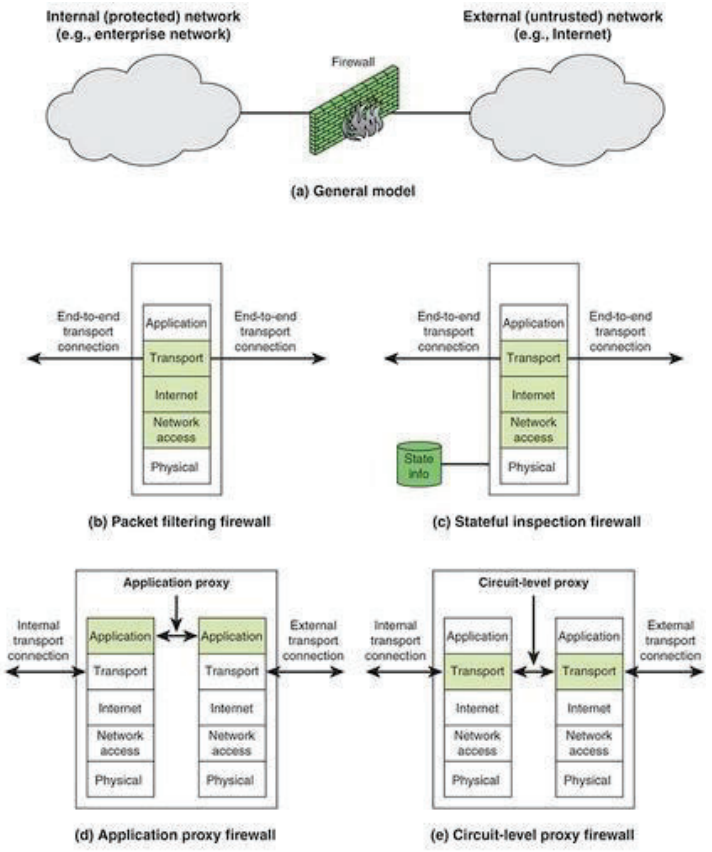


FIGURE 12.4 Types of Firewalls

A packet filter is typically set up as a list of rules, based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

The default = discard policy is the more conservative of the two. Initially, everything is blocked, and services are added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations. Further, visibility to users diminishes as rules are created. The default = forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known. This policy is used by generally more open organizations, such as universities.

Table 12.2 gives some examples of packet filtering rule sets. In each set, the rules are applied top to bottom. The * in a field is a wildcard designator that matches everything. Assume that the default = discard policy is in force with all these rule sets.

TABLE 12.2 Packet-Filtering Example

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	Port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set C

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Rule Set E

action	ourhost	port	theirhost	Port	comment
block	*	*	*	*	default

The rule sets can be described as follows:

- Rule set A: Inbound mail is allowed (port 25 is for Simple Mail Transfer Protocol [SMTP] incoming), but only to a gateway host. However, packets from a particular external host, SPIGOT, are blocked because that host has a history of sending massive files in email messages.
- Rule set B: This rule set is intended to specify that any inside host can send mail to the outside. A TCP packet with destination port 25 is routed to the SMTP server on the destination machine. The problem with this rule is that the use of port 25 for SMTP receipt is only a default; an outside machine can be configured to have some other application linked to port 25. As this rule is written, an attacker can gain access to internal machines by sending packets with TCP source port number 25.
- Rule set C: This rule set achieves the intended result that was not achieved in C. The rules take advantage of a feature of TCP connections. Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the other side. Thus, this rule set states that it allows IP packets where the source IP address is one of a list of designated internal hosts and the destination TCP port number is 25. It also allows incoming packets with source port number 25 that include the ACK flag in the TCP segment. Note that you explicitly designate source and destination systems to define these rules.
- Rule set D: This rule set is one approach to handling File Transfer Protocol (FTP) connections. With FTP, two TCP connections are used: a control connection to set up the file transfer and a data connection for the actual file transfer. The data connection uses a different port number that is dynamically assigned for the transfer. Most servers, and hence most attack targets, use low-numbered ports; most outgoing calls tend to use a higher-numbered port, typically above 1023. Thus, this rule set allows:
  - ✓ Packets that originate internally
  - ✓ Reply packets to a connection initiated by an internal machine
  - ✓ Packets destined for a high-numbered port on an internal machine

This scheme requires that the systems be configured so that only the appropriate port numbers are in use.

- Rule set E: This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

Rule set D points out the difficulty in dealing with applications at the packet filtering level. Another way to deal with FTP and similar applications is either to use stateful packet filters or an application-level gateway, both described subsequently in this section.

One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast. However, packet filters have the following weaknesses:

- Because packet filtering firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, if a packet filtering firewall cannot block specific application commands and if a packet filtering firewall allows a given application, all functions available within that application are permitted.
- Because of the limited information available to the firewall, the logging functionality present in packet filtering firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Most packet filtering firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality in the firewall.
- Packet filtering firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filtering firewalls cannot detect a network packet in which the OSI Layer 3 addressing information was altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.
- Finally, due to the small number of variables used in access control decisions, packet filtering firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filtering firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

Some of the attacks made on packet filtering firewalls and the appropriate countermeasures are as follows:

- IP address spoofing: The intruder transmits packets from the outside with a source IP address field containing an address of an internal host. The attacker hopes that the use of a spoofed address allows penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted. The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface. In fact, this countermeasure is often implemented at the router external to the firewall.
- Source routing attacks: The source station specifies the route for a packet to take as it crosses the Internet, in the hopes that this bypasses security measures that do not analyze the source routing information. The countermeasure is to discard all packets that use this option.

- Tiny fragment attacks: The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. This attack is designed to circumvent filtering rules that depend on TCP header information.

Typically, a packet filter makes a filtering decision on the first fragment of a packet. All subsequent fragments of that packet are filtered out solely because they are part of the packet whose first fragment was rejected. The attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through. A tiny fragment attack is defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter remembers the packet and discards all subsequent fragments.

Stateful Inspection Firewalls

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher-layer context. To understand what is meant by context and why a traditional packet filter is limited with regard to context, a little background is needed. Most standardized applications that run on top of TCP follow a client/server model. For example, for the SMTP, email is transmitted from a client system to a server system. The client system generates new email messages, typically from user input. The server system accepts incoming email messages and places them in the appropriate user mailboxes. SMTP operates by setting up a TCP connection between client and server, in which the TCP server port number, which identifies the SMTP server application, is 25. The TCP port number for the SMTP client is a number between 1024 and 65535 that is generated by the SMTP client.

In general, when an application that uses TCP creates a session with a remote host, it creates a TCP connection in which the TCP port number for the remote (server) application is a number less than 1024 and the TCP port number for the local (client) application is a number between 1024 and 65535. The numbers less than 1024 are the “well-known” port numbers and are assigned permanently to particular applications (for example, 25 for server SMTP). The numbers between 1024 and 65535 are generated dynamically and have temporary significance only for the lifetime of a TCP connection.

A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users.

A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 12.3. There is an entry for each currently established connection. The packet filter now allows incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

TABLE 12.3 Stateful Firewall Connection State Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.98.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall but also records information about TCP connections (refer to Figure 12.4c). Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols, such as FTP, instant messaging (IM), and Session Initiation Protocol (SIP) commands, in order to identify and track related connections.

Application-Level Gateway

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic (refer to Figure 12.4d). The user contacts the gateway by using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and is not forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable, while denying all other features.

Application-level gateways are more secure than packet filters. Rather than try to deal with the numerous possible combinations that are allowed and forbidden at the TCP and IP levels, the application-level gateway only needs to scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

A prime disadvantage of this type of gateway is the additional processing overhead on each connection. In effect, there are two spliced connections between the end users, and the gateway, which is at the splice point, must examine and forward all traffic in both directions.

Circuit-Level Gateway

A fourth type of firewall is the circuit-level gateway, or circuit-level proxy (refer to Figure 12.4e). This is either a standalone system or a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections are allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway is configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway incurs the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

Next-Generation Firewalls

Next-generation firewalls, which are implemented in either software or hardware, are capable of detecting and blocking complicated attacks by enforcing security measures at the protocol, port, and application levels. The difference between a standard firewall and a next-generation firewall is that the latter performs more in-depth inspection and in smarter ways. Next-generation firewalls also provide additional features such as Active Directory integration support, SSH (Secure Shell) and SSL (Secure Sockets Layer) inspection, and malware filtering based on reputation.

The common functionalities present in traditional firewalls—such as state inspection, virtual private networking, and packet filtering—are also present in next-generation firewalls. Next-generation firewalls are more capable of detecting application-specific attacks than standard firewalls and thus can prevent more malicious intrusions. Such a firewall does a full-packet inspection by checking the signatures and payload of packets for any anomalies or malware.

DMZ Networks

As shown in Figure 12.5, a firewall may be an internal or external firewall. An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or invite external connectivity, such as a corporate website, an email server, or a DNS (Domain Name System) server.

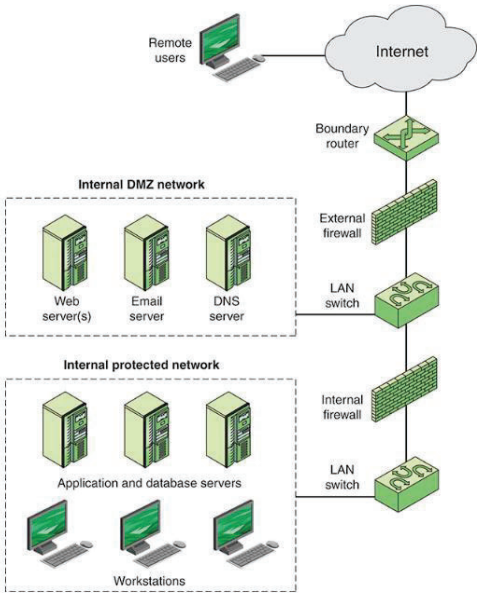


FIGURE 12.5 Firewall Configuration Example

An external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. An external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

- An internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
- An internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall protects the DMZ systems from attack from the internal protected network.
- Multiple internal firewalls are used to protect portions of the internal network from each other. For example, firewalls are configured so that internal servers are protected from internal workstations and vice versa. A common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks.

The Modern IT Perimeter

Traditionally, the enterprise network perimeter was defined by the physical interface between network devices, such as routers, and external networks, such as the Internet and private WANs. For today's enterprise, the perimeter is better defined by each node on the network and not the network itself. Key elements that break traditional network perimeter security are the following:

- Wireless access points (APs): Wi-Fi APs that are either unknowingly or maliciously deployed inside the enterprise network enable mobile devices on the premises or near the premises to gain access to resources on the enterprise network.

An IBM red paper [BUEC09] suggests that the following elements should comprise network perimeter defense in a wireless environment:

- The ability to globally enforce host-based security software deployed to the mobile systems known to access the enterprise network
- Scanning for, discovering, and blocking unknown devices
- Monitoring traffic patterns, communications, and transmitted data to discover how the enterprise network is being used and to uncover unwanted or threatening traffic from mobile devices

5.4 Virtual Private Networks and IP Security

This section introduces the concept of virtual private networks and examines IPsec, a common security mechanism used with VPNs.

Virtual Private Networks

A virtual private network (VPN) is a private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks that span large geographic areas, to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs. From the point of view of the provider, the pubic network facility is shared by many customers, and the traffic of each customer is segregated from other traffic. Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN. It is often the case that encryption and authentication facilities are provided for the VPN.

In today's distributed computing environment, the VPN offers an attractive solution to network managers. In essence, a VPN consists of a set of computers that interconnect by means of a relatively insecure network and that make use of encryption and special protocols to provide security. At each corporate site, workstations, servers, and databases are linked by one or more LANs. The LANs are under the control of the network manager and are configured and tuned for cost-effective performance. The Internet or some other public network is used to interconnect sites, providing a cost savings over the use of a private network and offloading the WAN management task to the public network provider. That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.

But the manager faces a fundamental requirement: security. Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, the manager can choose from a variety of encryption and authentication packages and products. Proprietary solutions raise a number of problems. First, how secure is the solution? If proprietary encryption or authentication schemes are used, there may be little reassurance in the

technical literature about the level of security provided. Second is the question of compatibility. No manager wants to be limited in the choice of workstations, servers, routers, firewalls, and so on by a need for compatibility with the security facility. This is the motivation for the IPsec set of Internet standards.

IPsec

IPsec is a set of Internet standards that augment both versions of IP that are in current use (IPv4 and IPv6) with security features. The principal feature of IPsec is that it encrypts and/or authenticates all traffic at the IP level. Thus, all distributed applications—including remote logon, client/server, email, file transfer, web access, and so on—are secured.

IPsec provides three main facilities: an authentication-only function referred to as Authentication Header (AH), a combined authentication/encryption function called Encapsulating Security Payload (ESP), and a key exchange function. For VPNs, both authentication and encryption are generally desired because it is important both to (1) ensure that unauthorized users do not penetrate the virtual private network and (2) ensure that eavesdroppers on the Internet cannot read messages sent over the VPN. Because both features are generally desirable, most implementations are likely to use ESP rather than AH. The key exchange function allows for manual exchange of keys as well as an automated scheme.

Figure 12.6a shows a simplified packet format for an IPsec option known as tunnel mode, using ESP and a key exchange function. Figure 12.6b shows a typical IPsec usage scenario. An organization maintains local area networks (LANs) at dispersed locations. Insecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPsec networking device typically encrypts and compresses all traffic going into the WAN and decrypts and decompresses traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial in to the WAN. Such user workstations must implement the IPsec protocols to provide security.

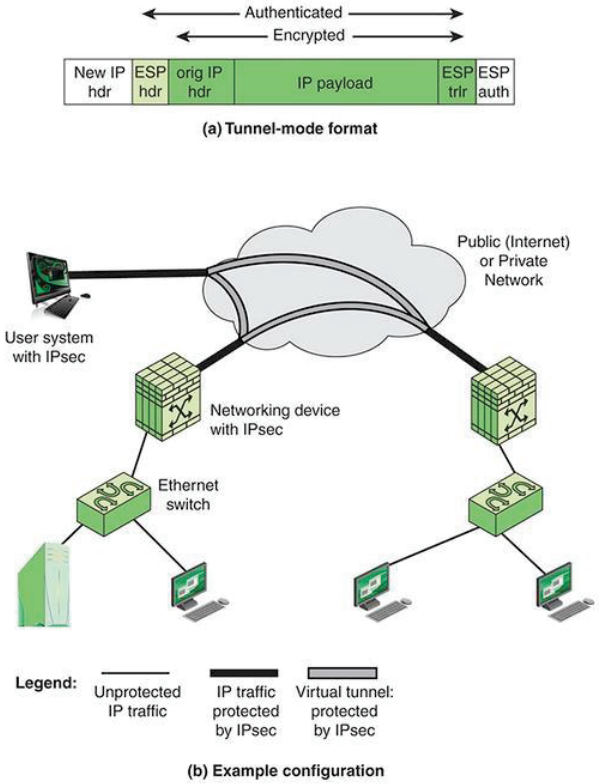


FIGURE 12.6 An IPsec Tunnel Mode Scenario

Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet, including the security fields, is treated as the payload of new outer IP packet, with a new outer IP header. The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet can have totally different source and destination addresses, which increases the security. Tunnel mode is used when

one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec. With tunnel mode, a number of hosts on networks behind firewalls can engage in secure communications without IPsec being implemented. The unprotected packets generated by such hosts are tunneled through external networks by tunnel mode SAs set up by the IPsec software in the firewall or secure router at the boundary of the local network.

Here is an example of how tunnel mode IPsec operates. Host A on a network generates an IP packet with the destination address of host B on another network. This packet is routed from the originating host to a firewall or secure router at the boundary of host A's network. The firewall filters all outgoing packets to determine the need for IPsec processing. If this packet from host A to host B requires IPsec, the firewall performs IPsec processing and encapsulates the packet with an outer IP header. The source IP address of this outer IP packet is this firewall, and the destination address can be a firewall that forms the boundary to B's local network. This packet is now routed to B's firewall, with intermediate routers examining only the outer IP header. At B's firewall, the outer IP header is stripped off, and the inner packet is delivered to B.

Firewall-Based VPNs

Figure 12.7 shows a typical scenario of IPsec usage. An organization maintains LANs at dispersed locations. Insecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPsec networking device typically encrypts and compresses all traffic going into the WAN and decrypts and decompresses traffic coming from the WAN; authentication can also be provided. These operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial in to the WAN. Such user workstations must implement the IPsec protocols to provide security. They must also implement high levels of host security, as they are directly connected to the wider Internet, which makes them an attractive target for attackers attempting to access the corporate network.

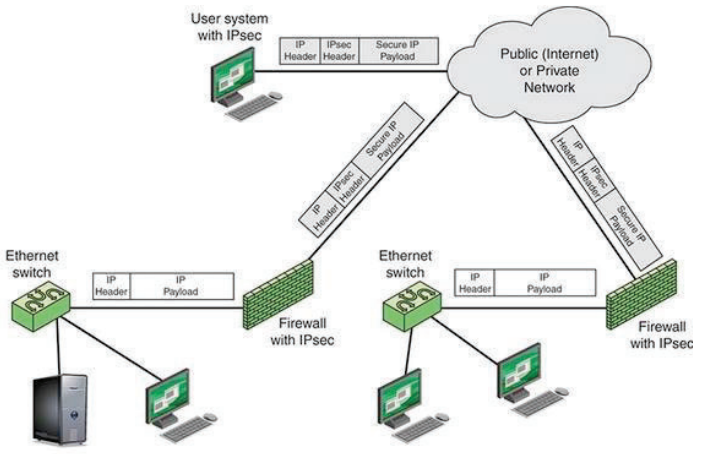


FIGURE 12.7 A VPN Security Scenario

A logical means of implementing IPsec is in a firewall, as shown in Figure 12.8. If IPsec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPsec can be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall and thus less desirable as an IPsec platform.

5.5 Security Considerations for Network Management

This section addresses the network management topics defined in the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP).

Network Device Configuration

The principal security objective related to network device configuration is to ensure that the configuration of network devices is accurate and does not compromise the security of the network.

The SGP recommends that policies and procedures for device configuration cover:

- Security architecture principles
- Standard security management practices
- Device configuration
- Restriction of access to network devices
- Vulnerability and patch management
- Changes to routing tables and settings in network devices
- Regular review of network device configuration and setup

Configuring network devices is a complex undertaking. As vendors build more features into their routers, switches, firewalls, and application delivery controllers, the command-line syntax required to configure those devices becomes increasingly loaded with options and syntactic choices. Web-based graphical user interfaces (GUIs) are often available as an alternative to a command-line interface (CLI), but they can be slow to navigate. Web GUIs also have a way of obfuscating functions by hiding them in unlikely pages, making accessing them require an annoying series of clicks.

Analyses by numerous IT experts have time and again revealed that the most common cause of network outages is faulty configuration changes [BANK14]. Even minor errors in configuration changes to the devices in production carry the risk of causing network outage. Therefore, skilled network administrators spend a significant part of their time configuring devices. They may find it hard to concentrate on strategic network engineering and administration tasks.

Most configuration changes are repetitive, labor-intensive tasks, such as changing passwords and access control lists. A number of tools and vendor offerings can automate repeatable and complex tasks related to device configuration, reducing the chance of human error. A Zoho Corp. white paper [BALA15] outlines the following important characteristics of automated network device configuration management tools:

- Multivendor device support: A tool should support all device types from all popular vendors.
- Discovery capability for device addition: A network can have thousands of network devices, and it is labor intensive to add each device manually. A tool should allow for discovering the devices in the network and automatically adding them, in addition to other device addition options.
- Communication protocols: A tool should support a wide range of protocols for establishing communication with the device and transferring configuration files.
- Secure storage: A tool should store configuration data in encrypted form, protected against intrusion.
- Inventory: A tool should provide an informative inventory of the devices being managed. It should provide various details, such as serial numbers, interface details, chassis details, port configurations, IP addresses, and hardware properties of the devices.
- Configuration operations and schedules: A tool should provide simple, intuitive options in the GUI to carry out various configuration operations, such as retrieving, viewing, editing, and

uploading configurations back to the device. It should include options to schedule the operations for automatic execution.

- Configuration versioning: A tool should associate a version number with the configuration of each device, incremented with each change.
- Baseline configuration: A tool should have a provision for labeling the trusted configuration version of each device as a baseline version to enable administrators to roll back a configuration to the baseline version in the event of a network outage.
- Approval mechanism: The security policies of many enterprises require certain types of changes carried out by certain levels of users to be reserved for review and approval by top administrators prior to the deployment of the changes.

Physical Network Management

Physical network management is one aspect of physical security. This section first lists some important aspects of physical network management and then introduces the TIA-492 infrastructure standard.

Network Aspects

Three aspects of physical network management are mentioned here:

- Telecommunication cables: Telecommunication cables both within a site and providing external access to a site need to be physically protected. This includes using armored conduit, locking inspection/termination points, and avoiding routes through publicly accessible areas.
- Network access points: It is important to store network access points in secure environments and make sure they are subject to physical security policies.
- Network documentation: It is important to clearly document network configuration and functionality.

TIA-492

The Telecommunications Industry Association (TIA) standard TIA-492, Telecommunications Infrastructure Standard for Data Centers, specifies the minimum requirements for telecommunications infrastructure of data centers.

The standard specifies function areas and helps define equipment placement based on the standard hierarchical design for regular commercial spaces. This architecture anticipates growth and helps create an environment where applications and servers can be added and upgraded with minimal downtime. This standardized approach supports high availability and a uniform environment for implementing security measures. TIA-942 specifies that a data center should include functional areas, as shown in Figure 12.8.

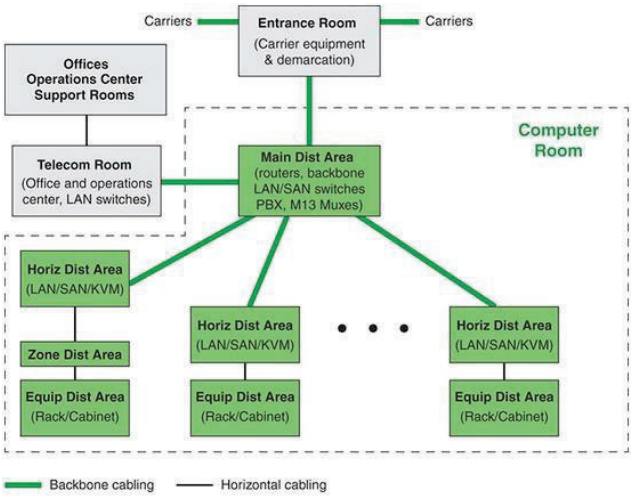


FIGURE 12.8 TIA-942-Compliant Data Center Showing Key Functional Areas

The functional areas are as follows:

- Computer room: This is the portion of the data center that houses data processing equipment.
- Entrance room: One or more entrance rooms house external network access provider equipment and provide the interface between the computer room equipment and the enterprise cabling systems. Physical separation of the entrance room from the computer room provides better security.
- Main distribution area: This centrally located area houses the main cross-connect as well as core routers and switches for LAN and SAN (storage area network) infrastructures.
- Horizontal distribution area (HDA): The HAD serves as the distribution point for horizontal cabling and houses cross-connects and active equipment for distributing cable to the equipment distribution area.
- Equipment distribution area (EDA): The EDA is the location of equipment cabinets and racks, with horizontal cables terminating with patch panels.
- Zone distribution area (ZDA): The ZDA is an optional interconnection point in the horizontal cabling between the HDA and EDA. The ZDA acts as a consolidation point for reconfiguration flexibility or for housing freestanding equipment such as mainframes.

An important part of TIA-942 that is especially relevant for computer security is the concept of tiered reliability. The standard defines four tiers, as shown in Table 12.4. For each of the four tiers, TIA-942 describes detailed architectural, security, electrical, mechanical, and telecommunications recommendations such that the higher the tier, the higher the availability.

TABLE 12.4 Data Center Tiers Defined in TIA-942

Tier	System Design	Availability/Annual Downtime
1	▪ This tier is susceptible to disruptions from both planned and unplanned activities. ▪ There is a single path for power and cooling distribution with no redundant components. ▪ It may or may not have a raised floor, a UPS, or a generator. ▪ It takes 3 months to implement. ▪ It must be shut down completely to perform preventive maintenance.	99.671%/28.8 hours
2	▪ Tier 2 is less susceptible than tier 1 to disruptions from both planned and unplanned activity. ▪ It has a single path for power and cooling distribution and includes redundant components. ▪ It includes a raised floor, a UPS, and a generator. ▪ It takes 3 to 6 months to implement. ▪ Maintenance of the power path and other parts of the infrastructure requires a processing shutdown.	99.741%/22.0 hours
3	▪ Tier 3 enables planned activity without disrupting computer hardware operation, but unplanned events still cause disruption. ▪ Multiple power and cooling distribution paths are available, though only one path is active; tier 3 includes redundant components. ▪ It takes 15 to 20 months to implement. ▪ It includes a raised floor and sufficient capacity and distribution to carry the load on one path while performing maintenance on the other.	99.982%/1.6 hours
4	▪ Planned activity does not disrupt critical load and data center can sustain at least one worst-case unplanned event with no critical load impact ▪ Multiple active power and cooling distribution paths, includes redundant components ▪ Takes 15 to 20 months to implement	99.995%/0.4 hours

Wireless Access

The security aspects of network management for wireless access have the objective of ensuring that only authorized individuals and computing devices gain wireless access to networks and minimizing the risk of wireless transmissions being monitored, intercepted or modified.

Dennis Kennedy's article "Best Practices for Wireless Network Security" provides a useful list of risks associated with wireless access and mitigation techniques including the following:

- Insufficient policies, training, and awareness: As with other areas, wireless security controls must include policies and user awareness training specifically for wireless access. These include procedures regarding uses of wireless devices and an understanding of relevant risks.

- Access constraints: A wireless access point transmits, at regular intervals, a signal containing is Service Set Identifier (SSID). This unique SSID identifies the access point and is used to announce that the access point is active. Because SSIDs are transmitted unencrypted, an unauthorized use could exploit the SSID to attempt an attack or intrusion. Countermeasures include the following:
    - ✓ Enable device security features.
    - ✓ Change default settings, such as default SSIDs set by the manufacturer.
    - ✓ Use static IP addresses for wireless access points. This avoids the use of the Dynamic Host Configuration Protocol (DHCP), which automatically provides an IP address to anyone attempting to gain access to your wireless network. again Static IP addresses make unauthorized penetration more difficult.
    - ✓ Track employees who have WLANs at home or at a remote site. Require that wireless networks be placed behind the main routed interface so the institution can shut them off if necessary. If WLANs are being used at home, require specific security configurations, including encryption and VPN tunneling.
- Rogue access points: Rogue access points are APs that users install without coordinating with IT. Access controls, encryption, and authentication procedures enable IT to maintain control.
- Traffic analysis and eavesdropping: To counter this threat, it is necessary to use a strong user authentication technique and to encrypt all traffic.
- Insufficient network performance: Poor performance is due to an imbalance in the use of access points, insufficient capacity planning, or a denial of service attack. The following steps can mitigate this risk.

1. Continually monitor network performance and investigate any anomalies immediately.
2. Segment the access point's coverage areas to reduce the number of people using each access point.
3. Apply a traffic-shaping solution to allow administrators to proactively manage traffic rather than react to irregularities.

- Hacker attacks: Hackers attempt to gain unauthorized access over wireless networks. Intrusion detection systems, anti-virus software, and firewalls are mitigation techniques.
- Physical security deficiencies: This is in the domain of physical security. Subject Both the network devices and mobile devices to physical security policies and procedures.

Employ VPNs as an additional security control.

External Network Connections

The principal security objective with respect to external network connections is to prevent unauthorized external users from gaining access to information systems and networks. The SGP includes the following guidelines:

- Restrict external network traffic to only specified parts of information systems and networks and defined entry points.
- Verify the sources of external connections.
- Limit access to devices that meet minimum security configuration requirements.
- Restrict access to only specific enterprise applications.
- Use firewalls to enforce security policies.

- Use a VPN for devices.

Firewalls

The security management of firewalls requires a clearly defined firewall policy that is compatible with an overall security policy and a plan for the implementation and operation of the organization's firewalls. The following subsections examine these two topics.

Firewall Policy

National Institute of Standards and Technology (NIST) SP 800-41, Guidelines on Firewalls and Firewall Policy, defines a firewall policy as a description of how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types, based on the organization's information security policies. SP 800-41 makes the following recommendations with respect to setting firewall policies:

- Base an organization's firewall policy on a comprehensive risk analysis.
- Base firewall policies on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Take into account the source and destination of the traffic in addition to the content.
- By default, block many types of IPv4 traffic, such as traffic with invalid or private addresses.
- Have policies for handling incoming and outgoing IPv6 traffic.
- Determine which applications in the organization send traffic into or out of its network and make firewall policies to block traffic for other applications.

Firewall Planning and Implementation

With respect to planning and implementation, SP 800-41 offers the following advice on the phases involved:

- Plan: The first phase of the process involves identifying all requirements for an organization to consider when determining what firewall to implement to enforce the organization's security policy.
- Configure: The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.

- Test: The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution and to identify any issues—such as interoperability—with components.
- Deploy: When testing is complete and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.
- Manage: After the firewall has been deployed, it is managed throughout its life cycle, including component maintenance and support for operational issues. This life cycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

Remote Maintenance

Remote maintenance refers to maintenance activities conducted by individuals who are external to an information system's security perimeter. Remote maintenance is a convenience to the enterprise; in some environments it is a necessity, as an Internet of Things (IoT) deployment or an industrial control system. The principal security objective in this area is to prevent unauthorized access to critical systems and networks through the misuse of remote maintenance facilities.

The U.S. Department of Homeland Security has compiled a list of requirements for remote maintenance of industrial control system [DHS11], but this list has general applicability to IT systems as well. The requirements for an organization are as follows:

- Authorize, monitor, and control remotely executed maintenance and diagnostic activities.
- Allow the use of remote maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system.
- Maintain records for remote maintenance and diagnostic activities.
- Terminate all sessions and remote connections when remote maintenance is completed.
- If password-based authentication is used to accomplish remote maintenance, change passwords following each remote maintenance session.
- Audit remote maintenance and diagnostic sessions and ensure that designated organizational personnel review the maintenance records of the remote sessions.
- Document the installation and use of remote maintenance and diagnostic links.
- Require that remote maintenance or diagnostic services be performed from a system that implements a level of security at least as high as that implemented on the system being serviced or remove the component to be serviced from the system and, prior to remote maintenance or diagnostic services, sanitize the component (for example, clearing of set points, embedded network addresses and embedded security validation information). After the service is performed and the component is returned to the facility, the organization should check or reinstall the authorized firmware code as specified by the configuration management plan and reset all authorized embedded configuration settings. Do this before reconnecting the component to the system to remove potentially malicious software that was added via "new" firmware.
- Require that remote maintenance sessions be protected by a strong authenticator tightly bound to the user.
- Require that maintenance personnel notify the system administrator when remote maintenance is planned (that is, date/time).

- Require that a designated organizational official with specific security/system knowledge approve the remote maintenance.
- Implement cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
- Employ remote disconnect verification at the termination of remote maintenance and diagnostic sessions.

Often the focus of enterprise security is protecting stored information and server facilities, as well as client/server communication from the wide variety of threats on the landscape. It is important not to overlook security related to electronic communications that may not involve server or database access but that is between individuals. This section looks at four types of electronic communications that need to be protected.

Email

It is useful to have a basic grasp of the Internet mail architecture, as defined in RFC 5598, Internet Mail Architecture. At its most fundamental level, the Internet mail architecture consists of a user world, in the form of message user agents (MUAs), and a transfer world, in the form of the Message Handling System (MHS), which is composed of message transfer agents (MTAs). The MHS accepts a message from one user and delivers it to one or more other users, creating a virtual MUA-to-MUA exchange environment. This architecture involves three types of interoperability. One is directly between users: Messages must be formatted by the MUA on behalf of the message author so that the message are displayed to the message recipient by the destination MUA. There are also interoperability requirements between the MUA and the MHS—first when a message is posted from an MUA to the MHS and later when it is delivered from the MHS to the destination MUA. Interoperability is required among the MTA components along the transfer path through the MHS.

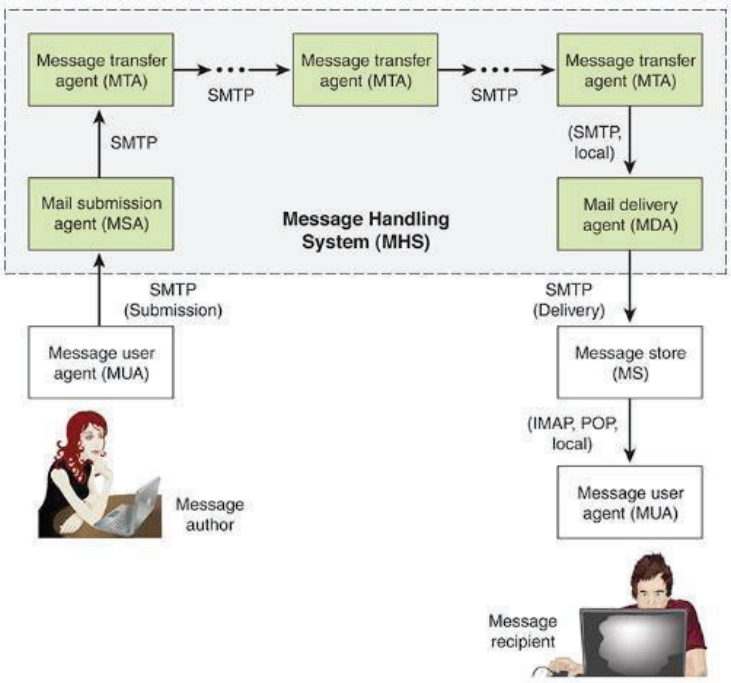


FIGURE 12.9 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

The key components include the following:

- Message user agent (MUA): The MUA operates on behalf of user actors and user applications. It is their representative within the email service. Typically, this function is housed in the user's computer and is referred to as a client email program or a local network email server. The author MUA formats a message and performs initial submission into the MHS via a MSA. The recipient MUA processes received mail for storage and/or display to the recipient user.
- Mail submission agent (MSA): The MSA accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards. This function is either located together with the MUA or as a separate functional model. In the latter case, Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.
- Message transfer agent (MTA): The MTA relays mail for one application-level hop. It is like a packet switch or an IP router in that its job is to make routing assessments and to move the message closer to the recipients. Relaying is performed by a sequence of MTAs until the

message reaches a destination MDA. An MTA also adds trace information to the message header. SMTP is used between MTAs and between an MTA and an MSA or MDA.

- Mail delivery agent (MDA): The MDA is responsible for transferring the message from the MHS to the MS, using SMTP.
- Message store (MS): The MUA employs a long-term MS, located on a remote server or on the same machine as the MUA. Typically, an MS retrieves messages from a remote MS using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

Trustworthy Email Standards

For both organizations and individuals, email is pervasive and vulnerable to a wide range of security threats. In general terms, email security threats are classified as follows:

- Authenticity-related threats: Can result in unauthorized access to an enterprise's email system. Another threat in this category is deception, in which case the purported author isn't the actual author.
- Integrity-related threats: Can result in unauthorized modification of email content.
- Confidentiality-related threats: Can result in unauthorized disclosure of sensitive information.
- Availability-related threats: Can prevent end users from being able to send or receive email.

To assist in addressing these threat categories, the National Institute of Standards and Technology (NIST) issued SP 800-177, Trustworthy Email, which provides recommendations and guidelines for enhancing trust in email. The document is both a survey of available standardized protocols and a set of recommendations for using these protocols to counter security threats to email usage. The following protocols and standards are described in and recommended by SP 800-177:

- STARTTLS: This SMTP security extension enables an SMTP client and server to negotiate the use of Transport Layer Security (TLS) to provide private, authenticated communication across the Internet.
- S/MIME: S/MIME provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption) of the message body carried in SMTP messages.
- DNS-based Authentication of Named Entities (DANE): DANE is designed to overcome problems in a certification authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC (DNS Security Extensions), with the result that the same trust relationships used to certify IP addresses are used to certify servers operating on those addresses.
- Sender Policy Framework (SPF): SPF enables a domain owner to specify the IP addresses of MTAs that are authorized to send mail on its behalf. SPF uses DNS to allow domain owners to create records that associate the domain name with a specific IP address range of authorized MTAs. It is a simple matter for receivers to check the SPF TXT record in DNS to confirm that the purported sender of a message is permitted to use that source address and reject mail that does not come from an authorized IP address.
- DomainKeys Identified Mail (DKIM): DKIM enables an email actor (author or operator) to affix a domain name to the message reliably, using cryptographic techniques, so that filtering engines develop an accurate reputation for the domain. The MTA is able to sign selected headers and the body of a message. This validates the source domain of the mail and provides message body integrity.

- Domain-based Message Authentication, Reporting and Conformance (DMARC): DMARC publishes a requirement for the author domain name to be authenticated by DKIM and/or SPF, for that domain's owner to request recipient handling of non-authenticated mail using that domain, and a reporting mechanism from recipients back to domain owners. DMARC lets senders know the proportionate effectiveness of their SPF and DKIM policies and signals to receivers what action should be taken in various individual and bulk attack scenarios.

An examination of these standards is beyond the scope of this book. For a detailed discussion, see Stallings's article "Comprehensive Internet Email Security" [STAL16]. A security manager must be aware of these standards and determine whether they should be required for email software products and services.

Another useful NIST document is SP 800-45, Guidelines on Electronic Mail Security, which complements SP 800-177. SP 800-45 recommends security practices for designing, implementing, and operating email systems on public and private networks. SP 800-177 focuses on the required Internet protocols and the use of digital signatures and encryption.

Acceptable Use Policy for Email

Many organizations provide email accounts for their employees that enable email to be sent and received within the organization as well as via the Internet. For such employees, it is recommended that an acceptable use policy be defined and agreed to by the employees. (See Section 4.3 for a general discussion of acceptable use policies.) As an example, an email acceptable use policy may include the following:

- Acceptable behavior: Use of email by employees is permitted and encouraged where such use supports the goals and objectives of the business.
- Unacceptable behavior: The following behavior by an employee is considered unacceptable:
  - ✓ Use of company communications systems to set up personal businesses or send chain letters
  - ✓ Forwarding of company confidential messages to external locations
  - ✓ Distributing, disseminating, or storing images, text, or materials that are considered indecent, pornographic, obscene, or illegal
  - ✓ Distributing, disseminating, or storing images, text, or materials that are considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or considered harassment
  - ✓ Accessing copyrighted information in a way that violates the copyright
  - ✓ Breaking into the company's or another organization's system or unauthorized use of a password/mailbox
  - ✓ Broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters
  - ✓ Transmitting unsolicited commercial or advertising material
  - ✓ Undertaking deliberate activities that waste staff effort or networked resources
  - ✓ Introducing any form of computer virus or malware into the corporate network
- Monitoring: The organization accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact on employee productivity and the reputation of the business. In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and

inspect any data recorded in those systems. In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check up on the use and content of emails. Such monitoring is for legitimate purposes only and is undertaken in accordance with a procedure agreed with employees.

- Sanctions: Where it is believed that an employee failed to comply with this policy, he or she faces the company's disciplinary procedure. An employee who has breached the policy faces a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied depends on factors such as the seriousness of the breach and the employee's disciplinary record.
- Agreement: All company employees, contractors, or temporary staff who are granted the right to use the company's email services are required to sign this agreement, confirming their understanding and acceptance of the policy.

Security Policy for Email

In addition to an acceptable use policy, an organization needs a security policy for email that specifies how email is to be handled, transmitted, and stored. ISO 27002, Code of Practice for Information Security Controls, includes the following considerations for protecting email:

- Protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization
- Ensuring correct addressing and transportation of the message
- Ensuring reliability and availability of the service
- Considering legal factors, such as requirements for electronic signatures
- Obtaining approval prior to using external public services such as instant messaging, social networking, or file sharing
- Specifying stronger levels of authentication to control access from publicly accessible networks

Instant Messaging

IM is a communications service in which short messages appear in pop-up screens as soon as they are received, thereby commanding the recipient's immediate attention. IM uses a shared software client between or among two or more people using personal computers, smartphones, or other devices. The communication is done over a network, often the Internet, and can include advanced modes with live voice or video. File transfers are also sometimes allowed but are limited in size. Most IM services offer presence information that indicates whether a user is online and available to send and receive messages. These services also provide buddy lists, which are groups of people the user has selected for frequent access, as well as group-based chat services. Enterprise IM provides real-time message passing within private and public networks.

Although included in the online chat category of technologies, IM differs in that the communicating parties are selected from the buddy list, and users are typically alerted when someone on their list is online. In contrast, online chat allows communication in a multiuser environment among users who are usually anonymous.

IM also differs from text messaging. The primary difference is that text messaging is a cellular phone service that is typically limited to 160 characters, whereas instant messaging is usually a computer session with a longer message size. After a text message is transmitted, the session is essentially ended even though the recipient can respond and keep the back-and-forth going all day. When an instant messaging session is started, it remains connected until the session is ended by one of the parties.

Acceptable Use Policy for IM

A template for an instant messaging acceptable use policy developed by InfoTech includes the following rules that comprise the policy:

1. Supported IM Solution: [Company Name] has selected [name IM solution] as its sole provider of corporate IM services. Non-sanctioned IM services could affect network security, so the corporate firewall has been configured to block them. Free IM services commonly used within the consumer market are NOT approved or supported by the IT department.
2. Instant Messaging Usage & Security Policy https://www.infotech.com/research/instant-messaging-usage-and-security-policy
3. Acceptable Use: IM services are to be used for business communications and for the purpose of fulfilling job duties, in accordance with corporate goals and objectives. Use of IM communications in this manner between [Company Name] employees and project teams is permitted and encouraged. It is expected that all employees will communicate professionally with colleagues, keeping in mind that foul language and slang terms are not allowed. [Note: If IT allows external IM communications with business partners or clients, these can be referred to here. However, this should only be done with added security features provided by IM security vendors.]
4. Confidentiality: The transmission of sensitive corporate information through IM for business purposes is not permitted. Truly sensitive communications should be conducted through encrypted email or in-person meetings. Employees are prohibited from sending client lists, personal information, credit card information, trade secrets, and other proprietary information through the corporate IM service. In addition, it is prohibited to discuss legal advice or questions through IM with corporate lawyers, as this can violate the attorney-client privilege.
5. File Sharing: Though many IM services support the transmission of files, this feature has been blocked for IM at [Company Name]. [Note: Although InfoTech recommends the banning of file sharing altogether, if advanced network-based security controls are in place, this section can be modified to include that file sharing is permitted and that all files will be automatically scanned for viruses and monitored by IT.]
6. Personal Use: Limited personal use of corporate IM services to communicate internally with colleagues at [Company Name] regarding non-work-related matters is permitted during designated work breaks and lunch hours only. Even during allotted personal IM usage periods, employees may not use the service for unsolicited mass mailings, non-[Company Name] commercial activity, operation of a privately owned business, solicitation of funds, dissemination of political causes, or promotion of religious/personal beliefs to others.
7. Compliance: IM use at [Company Name] will comply with, all [Company Name] policies, all [Company Name] contracts and all applicable laws.

8. Privacy: IM conversations and messages created on the corporate IM service and transmitted through corporate systems will be considered the property of [Company Name]. [Company Name] reserves the right to monitor, inspect, copy, review, store, and audit IM usage and messages generated by or for the enterprise. [Company Name] is also obligated to disclose IM messages and conversations when ordered to do so by auditors, courts, and law enforcement, with or without the employee's consent. Given these factors, employees do not have a reasonable expectation of privacy when using corporate IM services.

Security Policy for IM

IM is often poorly supervised, even though it introduces various risks to enterprise networks. Threats include IM-borne viruses, worms, spam over IM (SPIM), malware and phishing attacks, accidental or deliberate data leakage, inappropriate use, and regulatory noncompliance. A primary type of IM attack is to trick potential victims into installing a malicious program. IM-based attacks need some form of user interaction in order to launch, and attackers make use of social engineering to entice them to break security procedures or ignore common sense. These attacks usually exploit people's innate curiosity or natural desire to help. They also try to appeal to vanity or authority and other triggers, such as greed, fear, anger, or moral duty.

Thus, if an enterprise is going to enable employees to use IM, a corporate IM security policy is essential, and it needs to be backed up by user awareness training and an acceptable use policy.

Two basic approaches enable an enterprise to maintain security over IM. Both approaches limit employees to the use of the enterprise-mandated IM facility and further limit the group of employees that can use IM. One approach is to host an enterprise IM server in-house. This enables the enterprise to enforce its IM policies through traffic analysis and reporting, message keyword searches, and message archiving. The enterprise can also implement end-to-end encryption and user authentication, as well as configure content and URL filters and allow the controlled use of many collaboration features, such as integrated live voice, video, and data.

The enterprise may also opt for a cloud service, which means there is no need to install additional hardware or software. All IM messages sent to or from the enterprise network are routed through the cloud service, where they are scanned for viruses, worms, and malicious URLs. Messages are also matched against enterprise content control and acceptable IM use policies: Messages that are malicious or suspicious or that violate policies are automatically blocked. Also, all messages are logged and can be sent to the enterprise's existing archiving solution to satisfy legal discovery requirements and other relevant regulations. This type of service makes enterprise-grade control of IM accessible to organizations of all sizes.

Voice over IP (VoIP) Networks

VoIP has become increasingly prevalent in organizations of all sizes. In essence, VoIP involves the transmission of speech across IP-based network. VoIP works by encoding voice information into a digital format, which is carried across IP networks in discrete packets. VoIP has two main advantages over traditional telephony:

- A VoIP system is usually cheaper to operate than an equivalent telephone system with a PBX and conventional telephone network service. There are several reasons for this. Whereas

traditional telephone networks allocate dedicated circuits for voice communications using circuit switching, VoIP uses packet switching, allowing the sharing of transmission capacity. Further, packetized voice transmission fits well in the framework of the TCP/IP protocol suite, enabling the use of application- and transport-level protocols to support communications.

- VoIP readily integrates with other services, such as combining web access with telephone features through a single PC or terminal.

VoIP Signaling

Before voice is transferred using VoIP, a call must be placed. In a traditional phone network, the caller enters the digits of the called number. The telephone number is processed by the provider's signaling system to ring the called number. With VoIP, the calling user (program or individual) supplies the phone number of a URI (universal resource indicator, a form of URL), which then triggers a set of protocol interactions and results in the placement of the call.

The heart of the call placement process for VoIP is the Session Initiation Protocol (SIP), defined in RFC 3261, which is an application-level control protocol for setting up, modifying, and terminating real-time sessions between participants over an IP data network. SIP supports not only VoIP but also many multimedia applications. Associated with SIP is Session Description Protocol (SDP), defined in RFC 4566. SIP is used to invite one or more participants to a session, and the SDP-encoded body of a SIP message contains information about what media encodings (for example, voice, video) the parties can and will use. Once this information is exchanged and acknowledged, all participants are aware of the participants' IP addresses, available transmission capacity, and media type. Then data transmission begins, using an appropriate transport protocol. Typically, Real-Time Transport Protocol (RTP) is used. Throughout the session, participants can make changes to session parameters, such as new media types or new parties to the session, using SIP messages.

An alternative to the use of SIP is ITU-T H.323. The H.323 protocol has been available for several years, and carriers made a significant investment to build out many large, H.323-based networks. SIP is growing in popularity due to its ability to easily combine voice and Internet-based services. SIP interoperability and coexistence with H.323 is very important to maximize the return on current investments and to support new deployments that might use SIP as an alternative packet telephony signaling protocol.

VoIP Processing

In a VoIP system, when a called party responds, a logical connection is established between the two parties (or more parties, for a conference call), and voice data can be exchanged in both directions.

Figure 12.10 illustrates the basic flow of voice data in one direction in a VoIP system. On the sending side, the analog voice signal is first converted into a digital bit stream and then segmented into packets. The packetization is performed, typically, by RTP. This protocol includes mechanisms for labeling the packets so that they can be reassembled in the proper order at the receiving end, plus a buffering function to smooth out reception and deliver the voice data in a continuous flow. The RTP packets are then transmitted across the Internet or a private intranet using User Datagram Protocol (UDP) and IP.

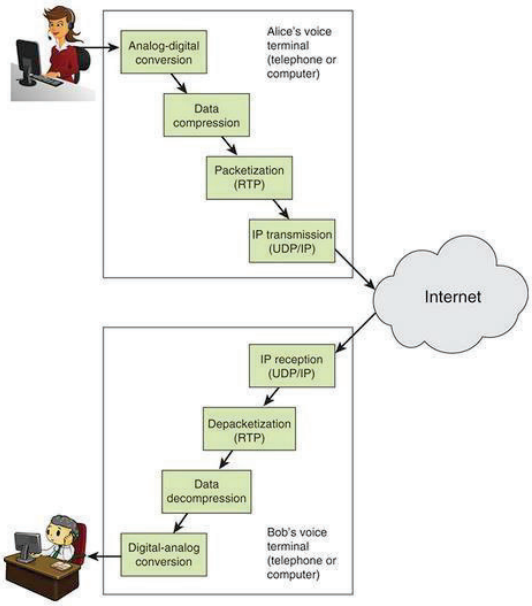


FIGURE 12.10 VoIP Processing

At the receiving end, the process is reversed. The packet payloads are reassembled by RTP and put into the proper order. The data are then decompressed, and the digitized voice is processed by a digital-to-analog converter to produce analog signals for the receiver's telephone or headset speaker.

VoIP Context

Ultimately, VoIP using IP-based networks may replace the public circuit-switched networks in use today. But for the foreseeable future, VoIP must coexist with the existing telephony infrastructure. Figure 12.11 shows some of the key elements involved in the coexistence of these older and newer technologies.

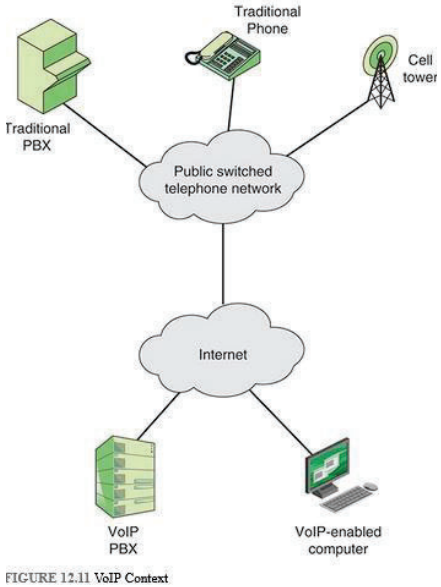


FIGURE 12.11 VoIP Context

The deployment of the VoIP infrastructure is accompanied by a variety of end-user products, including the following:

- Traditional telephone handset: These corded or cordless units function much like traditional telephones but are VoIP capable. They typically have many additional features, making use of a screen, and providing capabilities similar to those of smartphones.
- Conferencing units: These provide the same basic service as conventional conference calling phone systems and also allow users to coordinate other data communications services, such as text, graphics, video, and whiteboarding.
- Mobile units: Smartphones and other cellphones with VoIP capability can tie directly into a VoIP network without needing to go through any kind of gateway system.
- Softphone: The term softphone refers to software operating on a PC that implements VoIP. Typically, the PC is configured with a headset or with a telephone that makes use of a USB connection to the PC.

A wide variety of infrastructure equipment has been developed to support VoIP. There are two noteworthy types:

- IP PBX: The IP PBX is designed to support digital and analog phones and connect to IP-based networks using VoIP, as well as provide a connection to the public switched telephone network using traditional technology, if needed.
- Media gateway: The media gateway connects different physical networks in order to provide end-to-end connectivity. An important type of media gateway connects a VoIP network to a circuit-switched telephone network, providing the necessary conversion and signaling.

The VoIP environment continues to evolve, and a large number of products are being developed for providers, businesses, and residential/personal users.

VoIP Threats

As VoIP becomes mainstream, a number of security issues must be understood and addressed. Key areas of concern are as follows:

- VoIP traffic travels through the Internet. It is possible that a hacker could use a packet sniffer to listen to unencrypted VoIP traffic. The solution lies in setting up a VPN between the endpoints, but doing so also introduces additional complications.
- Many older firewalls may not recognize VoIP packets. In addition, some intrusion detection systems may try to inspect voice packets, thereby introducing delay and jitter. Bypassing the traffic inspection rules in the firewall may create additional vulnerability.
- Many older VoIP phones may require security patches for their software. Such patches are seldom applied as many administrators are not even aware that phone software needs to be patched. Some VoIP phones are set up to apply patches directly without even asking for authentication. Such phones can be very vulnerable to hackers.
- Phones also inherit the security flaws of the operating systems they use.
- Systems used out of the box may have default passwords and open ports that need to be managed and secured. In many cases, this is ignored.
- DoS attacks can be launched against a VoIP phone system, just as they can be launched against other computer applications.

The following are some specific threats to the use of VoIP:

- Spam over Internet telephone (SPIT): Unsolicited bulk messages may be broadcast over VoIP to phones connected to the Internet. Although marketers already use voicemail for commercial messages, IP telephony makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately.
- Eavesdropping: Interception of control packets enables an adversary to listen in on an unsecured VoIP call.
- Theft of service: This type of attack involves capturing access codes, allowing the adversary to get into the VoIP provider network and then use the facility.
- Man-in-the middle attack: This type of attack involves an adversary inserting as a relay point between two ends of a VoIP call. In addition to eavesdropping, the adversary could divert a call to a third party or generate simulated voice content to create misleading impressions or cause operational errors.

VoIP Security Measures

A number of security measures can be taken to protect VoIP traffic, including the following:

- Encryption: It is a good practice to encrypt all voice connections.
- VPNs: VPNs create segregated broadcast domains within the IP network infrastructure. By creating VPNs for voice, organizations provide an additional layer of protection that can potentially insulate voice communications from DoS attacks and other risks.
- Port administration: SIP applications tend to open multiple ports on network devices, creating additional exposure to hackers. Therefore, IT staff need to implement firewalls and other security administration tools that discover and close unnecessarily opened ports—and rigorously authenticate devices attempting to use those ports.
- Real-time antivirus scanner: An organization should scan the VoIP server continuously.
- Application-layer firewall: This protects assets associated with the VoIP server, such as a database devoted to logging calls or even recording the calls.
- Device authentication: Any user device that attempts to use the VoIP service should be authenticated.
- User authentication: Individual users should be authenticated to limit specific users or groups of users to specific VoIP services.
-

Telephony and Conferencing

The security objective with respect to telephony and conferencing is to prevent and detect unauthorized use or misuse of telephony and conferencing facilities. This is achieved with a combination of physical and logical controls. The SGP recommends that there should be policies that cover the following:

- Use of the organization's telephones
- Moves and changes of telephone users
- Registration and authentication of users with access to voicemail
- Protection of voicemail systems against unauthorized access (for example, by use of password protection)
- The use and setup of web-based conferencing facilities (including teleconferencing, videoconferencing, and online web-based collaboration)

5.7 Networks and Communications Best Practices

The SGP breaks down best practices in the networks and communication category into 2 areas and 10 topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Network management: The objectives of this area are to (1) design physical, wireless, and voice networks to be reliable and resilient; prevent unauthorized access; encrypt connections; and detect suspicious traffic and (2) configure network devices (including routers, firewalls, and wireless access points) to function as required and to prevent unauthorized or incorrect updates.

- ✓ Network device configuration: Lists the key practices to ensure that network devices (including routers, switches, and firewalls) are configured to function as required and to prevent unauthorized or incorrect updates.
- ✓ Physical network management: Addresses issues related to the physical protection of network devices and communications links.
- ✓ Wireless access: Provides a policy checklist for managing wireless access.
- ✓ External network connections: Provides a policy checklist for managing and protecting external network connections.
- ✓ Firewalls: Details the types of firewalls to be used and provides guidelines for firewall security policy.
- ✓ Remote maintenance: Lists measures to protect remote maintenance facilities from misuse.

- Electronic communications: The objectives of this area are to protect electronic communication systems by setting policy for their use; configuring security settings; and hardening the supporting technical infrastructure. Four topics are covered: email, instant messaging, VoIP, and telephone/conferencing. For each of these topics, the SGP provides checklists of policies and procedures to secure against misuse.

5.8 Review Questions / Case Studies / Projects

1. According to ISO 7498-4, what are the key functions of network management?
2. What are some of the key tasks performed by a network management entity?
3. How is a distributed network management system organized?
4. Explain the network management architecture defined by Cisco.
5. Name all the techniques that firewalls use to control access to a site and enforce the site's security policy.
6. What are some common types of firewalls?
7. What are some of the weaknesses of packet filters?
8. What are some of the important characteristics of automated network device configuration management tools?
9. According to TIA-942, which functional areas are included in a data center?
10. What are some of the key risks associated with wireless access?
11. According to SP 800-41, how are firewall planning and implementation phases defined?
12. In general, how can you classify email security threats?
13. According to ISO 27002, how can an organization protect email?
14. Describe two types of infrastructure equipment that support VoIP.
15. What are some of the principal threats to VoIP usage?
16. How does the Standards Customer Council define the key components of a cloud service agreement (CSA)?

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Appreciate the importance of security event logging to the event management process.**
- **Understand the nature and purpose of threat intelligence.**
- **Explain the typical nature of cyber attacks and strategies for preventing and responding to them.**
- **Understand the difference between a security event and a security incident.**
- **Present an overview of the security incident management process.**

6.1 Introduction

This chapter deals with detecting and responding to technical security attacks. The previous sections focus on the management of threats and vulnerabilities and the monitoring of events that may represent threats exploiting vulnerabilities. The remaining sections deal with responding to security incidents that constitute attacks or violations of security policy.

6.2 Technical Vulnerability Management

Technical vulnerability management, usually referred to simply as vulnerability management, is a security practice specifically designed to proactively mitigate or prevent the exploitation of technical vulnerabilities that exist in a system or an organization. The process involves the identification, classification, remediation, and mitigation of various vulnerabilities in a system. It is an integral part of cybersecurity and is practiced together with risk management as well as other security practices.

technical vulnerability

A hardware, firmware, communication, or software flaw that leaves an information processing system open to potential exploitation either externally or internally, resulting in risk for the system.

Figure 15.1 illustrates the five key steps involved in vulnerability management. The following sections examine each off these steps in detail.

Plan Vulnerability Management

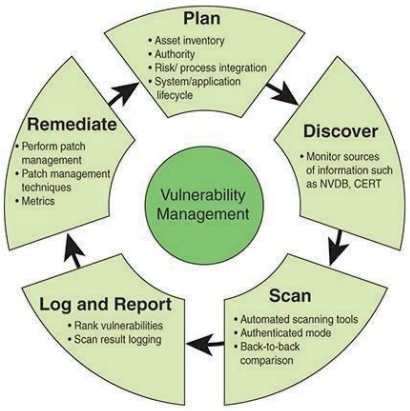


FIGURE 15.1 Vulnerability Management Steps

Effective management of technical vulnerabilities begins with planning. Key aspects of the planning process include the following:

- **Risk and process integration**: Technical vulnerability review is an operational aspect of an overall information security risk management strategy. A vulnerability analysis must consider the relative risk impacts, including those related to the potential for operational disruption. These risks must also have a clear reporting path that allows for appropriate management awareness of risk factors and exposure. Vulnerability management should also provide input into change management and incident management processes.
- **Integration with asset inventory:** As discussed in Chapter, "Information Risk Assessment," asset identification is an integral part of risk assessment. The resulting asset inventory allows for action to be taken once a technical vulnerability is reviewed and a mitigation strategy agreed on. By integrating the asset inventory with the vulnerability management system, an enterprise can prioritize high-risk systems where the impact of technical vulnerabilities can be greatest.
- **Establishment of clear authority to review vulnerabilities**: Because probing a network for vulnerabilities can disrupt systems and expose private data, an enterprise needs to have in place a policy and buy-in from top management before performing vulnerability assessments. The enterprise's acceptable use policy must have users and system managers consent to vulnerability scanning as a condition of connecting to the network. Awareness training should clarify that the main purpose of seeking vulnerabilities is to defend against attacks. There is also a need for policies and ethical guidelines for those who have access to data from vulnerability scans. These individuals need to understand the appropriate action when illegal materials are found on their systems during a vulnerability scan.
- **System and application life cycle integration:** The review of vulnerabilities must be integrated in system release and software development planning to ensure that potential weaknesses are identified early to both lower risks and manage costs of finding these issues prior to identified release dates.

Discover Known Vulnerabilities

The discover step involves monitoring sources of information about known vulnerabilities to hardware, software, and network equipment. Key sources of information include the following:

CERT Coordination Center https://www.sei.cmu.edu/about/divisions/cert/index.cfm

- National Institute of Standards and Technology (NIST) National Vulnerability Database (NVDB) and Common Vulnerability Scoring System (CVSS): This excellent source of information is discussed in some detail in Section 3.5.

- Computer emergency response (or readiness) team (CERT): Such a team is a cooperative venture that collects information about system vulnerabilities and disseminates it to systems managers. Hackers also routinely read CERT reports. Thus, it is important for system administrators to quickly verify and apply software patches to discovered vulnerabilities. One of the most useful of these teams is the U.S. Computer Emergency Readiness Team, which is a partnership between the Department of Homeland Security and the public and private sectors, intended to coordinate responses to security threats from the Internet. Another excellent resource is the CERT Coordination Center, which grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency. The CERT Coordination Center website provides good information on Internet security threats, vulnerabilities, and attack statistics.
- Packet Storm: Packet Storm provides around-the-clock information and tools to help mitigate both personal data and fiscal loss on a global scale. As new information surfaces, Packet Storm releases everything immediately through its RSS (Rich Site Summary) feeds, Twitter, and Facebook.
  Packet Storm https://packetstormsecurity.com
- SecurityFocus: This site maintains two important resources. BugTraq is a high-volume, full-disclosure mailing list for detailed discussion and announcement of computer security vulnerabilities. The SecurityFocus Vulnerability Database provides security professionals with up-to-date information on vulnerabilities for all platforms and services.
  SecurityFocus https://www.securityfocus.com
- Internet Storm Center (ISC): Maintained by the SANS Technology Institute, the ISC provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet service providers to fight back against the most malicious attackers.
  Internet Storm Center https://isc.sans.edu

Scan for Vulnerabilities

In addition to monitoring vulnerability reporting services, enterprises need to regularly scan software, systems, and networks for vulnerabilities and proactively address those that are found. The Center for Internet Security (CIS) recommends the following scanning regimen [CIS18]:

- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver a prioritized lists of the most critical vulnerabilities to each responsible system administrator, along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries, described in Section 3.5) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project, which is part of the NVDB).
- Perform vulnerability scanning in authenticated mode, either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans; this account should not be used for any other administrative activities, and it should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to users individually.

- Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Periodically review business risks for existing vulnerabilities to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions changed, increasing the risk.

Depending on the size and structure of the institution, the approach to vulnerability scanning can differ. Small institutions with a good understanding of IT resources throughout the enterprise can centralize vulnerability scanning. Larger institutions are more likely to have some degree of decentralization, so vulnerability scanning might be the responsibility of individual units. Some institutions have a blend of both centralized and decentralized vulnerability assessment. In any case, before starting a vulnerability scanning program, it is important to have authority to conduct the scans and to understand the targets to be scanned.

There are a number of free and commercial vulnerability scanners available for enterprise use. An example of a freeware package is the Open Vulnerability Assessment System (OpenVAS), which scans for thousands of vulnerabilities and supports concurrent scan tasks and scheduled scans. OpenVAS includes a daily updated feed of vulnerability tests. Perhaps the most widely used commercial scanner is Nessus. Nessus uses a variety of types of scans and looks for a broad range of vulnerabilities.

There are two challenges involved in scanning that an enterprise needs to address:

- **Scanning can cause disruptions.** The scanning process can impact performance. This is especially true with legacy systems, which can have problems even with simple network port scans. IT operations staff need to be in the loop. Make them aware of the importance and relevance of scans. Also, timing needs to be resolved to ensure that scanning does not conflict with regular maintenance schedules.

- **Scanning can generate huge amounts of data and numerous false positives.** Technical vulnerability management practices produce very large data sets. Accordingly, use frequent follow-up evaluations to validate the findings. Reviewing all these vulnerabilities is infeasible. Develop a vulnerability prioritization plan before initiating a large number of scans. The vulnerability prioritization plan must be aligned with the IT infrastructure and application plan to support the overall IT strategic plan; there should not be too much focus on legacy infrastructure and legacy applications that may be retired shortly.

Log and Report

When a vulnerability scan is completed, the organization should log the results so that personnel can verify the activity of the regular vulnerability scanning tools.

An organization should rank discovered vulnerabilities, such as attaching a score to each vulnerability that reflects the following:

- The skill required to exploit the vulnerability
- The availability of the exploit to potential attackers

- The privilege gained upon successful exploitation
- The risk and impact of this vulnerability if exploitation is successful

The resulting vulnerability scoring and metrics provide a valuable guide in the remediation process.

The reporting process includes keeping track of the number and risk levels of vulnerabilities discovered over time and the effectiveness of remediation efforts in removing vulnerabilities.

With respect to logging, The CIS Critical Security Controls for Effective Cyber Defense [CIS18] recommends that event logs be correlated with information from vulnerability scans. This has three objectives. First, verify that the activity of the regular vulnerability scanning tools is itself logged. Second, correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. Third, monitor the scan logs to ensure that this activity is limited to the time frames of legitimate scans. This latter objective is important both because the enterprise wants to avoid conflict with other activities, such as routine maintenance, and because vulnerability scanning itself is a form of attack that must be detected.

Remediate Vulnerabilities

An organization should deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. It should apply patches to all systems—even systems that are properly air-gapped (that is, physically not accessible from the Internet).

NIST SP 800-40, Guide to Enterprise Patch Management Technologies, provides a very detailed list of recommendations for patch management. This chapter provides a brief summary of those recommendations, which are grouped into three categories: performing patch management, patch management technologies, and patch management metrics.

Performing Patch Management

There are a number of issues to consider related to performing patch management. One is the relationship between timing, prioritization, and testing. Ideally, every discovered vulnerability should be patched as soon as discovered. But, because resources are limited, enterprises need to prioritize patching. Further, there is a risk of installing a patch throughout an enterprise without testing it, so the resources involved in testing need to be taken into account. An organization should consider the impact of a patch on operational systems, such as rebooting or changing configurations. It should also take special care if it uses multiple automated means of patching, such as self-patching software, third-party services, and network-based capability. An organization should anticipate and resolve conflicts and maintain a policy to verify that patches are effective on all relevant systems.

Patch Management Technologies

Table 15.1 shows three types of patch management techniques: agent-based scanning, agentless scanning, and passive network monitoring.

TABLE 15.1 Comparison of Patch Management Techniques

Characteristic	Agent-Based Scanning	Agentless Scanning	Passive Network Monitoring
Admin privileges needed on hosts?	Yes	Yes	No
Supports unmanaged hosts?	No	No	Yes
Supports remote hosts?	Yes	No	No
Supports appliances?	No	No	Yes
Bandwidth needed for scanning?	Minimal	Moderate to excessive	None
Potential range of applications detected?	Comprehensive	Comprehensive	Only those that generate unencrypted network traffic

Details of the three patch management techniques are as follows:

- Agent-based scanning: Requires an agent to be running on each host to be patched, with one or more servers managing the patching process and coordinating with the agents. Each agent is responsible for determining what vulnerable software is installed on the host, communicating with the patch management servers, determining what new patches are available for the host, installing those patches, and executing any state changes needed to make the patches take effect.
- Agentless scanning: Uses one or more servers that perform network scanning of each host to be patched and determine what patches each host needs. Generally, agentless scanning requires that servers have administrative privileges on each host so that they can return more accurate scanning results and so they have the ability to install patches and implement state changes on the hosts.
- Passive network monitoring: Monitors local network traffic to identify applications (and, in some cases, operating systems) that are in need of patching. Unlike the other techniques, this technique identifies vulnerabilities on hosts that don't permit direct administrator access to the operating system, such as some Internet of Things (IoT) devices and other appliances. However, the passive monitoring must be linked to system management software that has the ability to install patches.

Common features of patch management capabilities include identifying which patches are needed, bundling and sequencing patches for distribution, allowing administrators to select which patches may or may not be deployed, and installing patches and verifying installation. Many patch management technologies also allow patches to be stored centrally (within the organization) or downloaded as needed from external sources.

A supplementary approach to traditional patch management is virtual patching. Virtual patching is implemented in a hardware device or software module that sits between incoming traffic and an application, a database, a server, or an endpoint. The virtual patch capability scans all traffic for exploits and blocks specific communications and resource usage, based on several factors. Virtual patching is an interim measure when it is difficult to immediately install needed patches.

Patch Management Metrics

As with other aspects of security, management needs metrics to evaluate the use of patch management. SP 800-40 gives the following examples of possible implementation measures:

- What percentage of the organization's desktops and laptops are being covered by the enterprise patch management technologies?
- What percentage of the organization's servers have their applications automatically inventoried by the enterprise patch management technologies?

SP 800-40 gives the following examples of possible effectiveness/efficiency measures:

- How often are hosts checked for missing updates?
- How often are asset inventories for host applications updated?
- What is the minimum/average/maximum time to apply patches to X% of hosts?
- What percentage of the organization's desktops and laptops are patched within X days of patch release? Y days? Z days? (In this case, X, Y, and Z are different values, such as 10, 20, and 30.)
- On average, what percentage of hosts are fully patched at any given time? What percentage of high impact moderate impact, and low impact hosts are fully patched??
- What percentage of patches are applied fully automatically, versus partially automatically, versus manually?

SP 800-40 gives the following examples of possible impact measures:

- What cost savings has the organization achieved through its patch management processes?
- What percentage of the organization's information system budget is devoted to patch management?

6.3 Security Event Logging

This section begins with a discussion of the distinction between security events and security incidents and then examines the key objective in performing security event logging. The remainder of this section deals with details of the security event logging function.

In the information security field, a distinction is commonly made between events and incidents:

- Security event: An occurrence considered by an organization to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity. Events sometimes provide indications that incident are occurring.
- Security incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

A related concept is an indicator of compromise (IoC). IoCs are specific techniques used in the course of an attack, which may appear as anomalous behavior. SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, defines IoCs as forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that were compromised. IOCs for the discovery of compromised hosts include for example, the creation of registry key values. IOCs for network traffic include, for example, uniform resource locators (URLs) or protocol elements

that indicate malware command-and-control servers. The rapid distribution and adoption of IOCs improve information security by reducing the time during which information systems and organizations are vulnerable to the same exploit or attack.

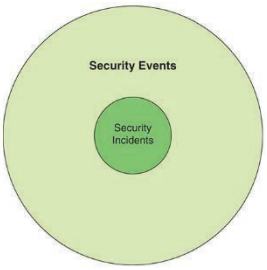


FIGURE 15.2 Security Events and Incidents

The term security event covers both events that are security incidents and those that are not, as shown in Figure 15.2.

In a certification authority workstation, for example, a list of security events can include the following:

- Logging an operator into or out of the system
- Performing a cryptographic operation, such as signing a digital certificate or certificate revocation list
- Performing a cryptographic card operation (creation, insertion, removal, or backup)
- Performing a digital certificate life cycle operation (rekey, renewal, revocation, or update)
- Posting a digital certificate to an X.500 directory
- Receiving a key compromise notification
- Receiving an improper certification request
- Detecting an alarm condition reported by a cryptographic module
- Failing a built-in hardware self-test or a software system integrity check

Only the final four events in this list are security incidents. This section and the following one address issues related to security events. Sections 15.6 and 15.7 discuss the management of security incidents.

Security Event Logging Objective

The objectives of security event logging are to help identify threats that may lead to an information security incident, maintain the integrity of important security-related information, and support forensic investigations. Effective logging enables an enterprise to review events, interactions, and changes that are relevant to security. With a record of events such as anomalies, unauthorized access attempts, and excessive resource usage, an enterprise can perform an analysis to determine the cause.

Potential Security Log Sources

A wide variety of sources of security events can be logged, including the following:

- Server and workstation operating system logs

Log: A record of the events occurring within an organization’s systems and networks.

- Application logs (for example, web server, database server)
- Security tool logs (for example, antivirus, change detection, intrusion detection/prevention system)
- Outbound proxy logs and end-user application logs
- Firewalls and other perimeter security devices for traffic between local user and remote database or server (referred to as north–south traffic)

- Security devices between data center storage elements that communicated across a network (referred to as east–west traffic), which may involve virtual machines and software-based virtual security capabilities

The abundance of log sources present a considerable challenge to enterprise security management. An organization should create a central repository to store logs in a standardized format. This may require conversion software and consolidation software to keep the amount of log information manageable.

What to Log

In determining what types of events to log, an organization must take into consideration a number of factors, including relevant compliance obligations, institutional privacy policies, data storage costs, access control needs, and the ability to monitor and search large data sets in an appropriate time frame. The following are examples of potential security-related events that that could be logged:

- Operating system logs: Successful user logon/logoff; failed user logon; user account change or deletion; service failure; password changes; service started or stopped; object access enied; object access changed
- Network device logs: Traffic allowed through firewall, traffic blocked by firewall; bytes transferred; protocol usage; detected attack activity; user account changes; administrator access
- Web servers: Excessive access attempts to nonexistent files; code (for example, SQL [Structured Query Language] or HTML [Hypertext Markup Language]) seen as part of the URL; attempted access to extensions not implemented on the server; web service stopped/started/failed messages; failed user authentication; invalid request; internal server error

Protection of Log Data

An organization needs to protect log data in terms of confidentiality, data integrity, availability, and authenticated usage. Logs can contain sensitive information, such as a user's password or the content of emails. This presents security and privacy risks. In addition, if logs are altered or deleted, malicious activity might not be noticed or the identity of the malicious party might be concealed.

Role-based access controls are used to partition the ability to read and modify log data based on business needs and position responsibilities.

Log Management Policy

NIST SP 800-92, Guide to Computer Security Log Management, recommends addressing the following questions in a log management policy:

log management

The process for generating, transmitting, storing, analyzing, archiving, and disposing of log data.

- Log generation:

  - Which types of hosts perform logging?
  - Which host components perform logging (for example, operating system, service, application)?
  - Which types of events each component logs (for example, security events, network connections, authentication attempts)?
  - Which data characteristics are logged for each type of event (for example, username and source IP address for authentication attempts)?
  - How frequently each type of event is logged (for example, every occurrence, once for all instances in x minutes, once for every x instances, every instance after x instances)?
- Log transmission:
  - Which types of hosts transfer logs to a log management infrastructure?
  - Which types of entries and data characteristics are transferred from individual hosts to a log management infrastructure?
  - How is log data transferred (for example, which protocols are permissible), including out-of-band methods, where appropriate (for example, for standalone systems)?
  - How frequently is log data transferred from individual hosts to a log management infrastructure (for example, in real time, every five minutes, every hour)?
  - How are the confidentiality, integrity, and availability of each type of log data protected while in transit, and is a separate logging network used?
- Log storage and disposal:
  - How often are logs rotated or archived?
  - How are the confidentiality, integrity, and availability of each type of log data protected while in storage (at both the system level and the application level)?
  - How long is each type of log data preserved (at both the system level and the infrastructure level)?
  - How is unneeded log data disposed of (at both the system level and the infrastructure level)?
  - How much log storage space is available (at both the system level and the infrastructure level)?
  - How are log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records, handled (for example, how the impacted logs must be marked, stored, and protected)?
- Log analysis:
  - How often is each type of log data analyzed (at both the system level and the infrastructure level)?
  - Who is able to access the log data (at both the system level and the infrastructure level), and how are accesses logged?
  - What should happen when suspicious activity or an anomaly is identified?
  - How are the confidentiality, integrity, and availability of the results of log analysis (for example, alerts, reports) protected while in storage (at both the system level and the infrastructure level) and in transit?
  - How does the organization handle inadvertent disclosures of sensitive information recorded in logs, such as passwords or the contents of emails?

6.4 Security Event Management

Security event management (SEM) is the process of identifying, gathering, monitoring, analyzing, and reporting security-related events. The objective of SEM is to extract from a large volume of security events those events that qualify as incidents. SEM takes data input from all devices/nodes and other similar applications, such as log management software. The collected events data is analyzed with security algorithms and statistical computations to trace out any vulnerability, threat, or risk, as shown in Figure 15.3.

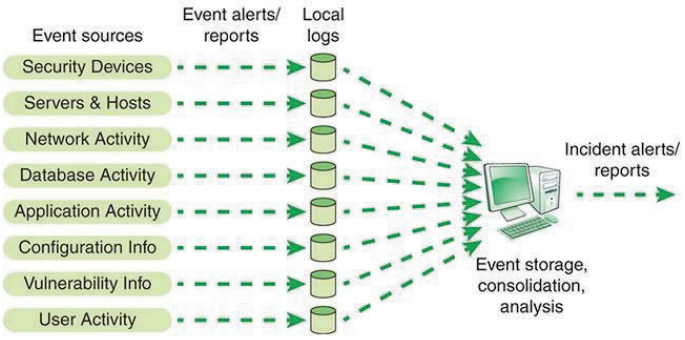


FIGURE 15.3 Security Event Management

SEM Functions

The first phase of event management is the collection of event data in the form of logs, as discussed in the preceding section. As event data are generated, they are generally stored in logs local to the devices that generate them. A number of steps need to be taken at this point:

1. Normalization: For effective management, the log data needs to be in a common format to enable further processing.
2. Filtering: This step includes assigning priorities to various types of events. On the basis of priority, large number of events can be set aside and not subject to further analysis, or they can be archived in case there is a need to review them later.
3. Aggregation: The IT facility of a large enterprise generates millions of events per day. It is possible to aggregate them by categories into a more manageable amount of data. For example, if a particular type of traffic is blocked a number of times, it is sufficient to record as a single aggregate event the type of traffic and the number of times it was blocked over a particular time frame.

These preliminary steps reduce the volume of data. The objective of the next steps is to analyze the data and generate alerts of security incidents.

Analysis includes the following aspects:

- Pattern matching: It is important to look for data patterns within the fields of stored event records. A collection of events with a given pattern can signal a security incident.
- Scan detection: Often, an attack begins with a scan of IT resources by the attacker, such as port scans, vulnerability scans, or other types of pings. A substantial number of scans being found from a single source or a small number of sources can signal a security incident.
- Threshold detection: A straightforward form of analysis is the detection of a threshold being crossed. For example, if the number of occurrences of a type of event exceeds a given threshold in a certain time period, that constitutes an incident.
- Event correlation: Correlation consists of using multiple events from a number of sources to determine that an attack or suspicious activity occurred. For example, if a particular type of attack proceeds in multiple stages, the separate events that record those multiple activities need to be correlated in order to see the attack. Another aspect of correlation is to correlate

particular events with known system vulnerabilities, which might result in a high-priority incident.

SEM Best Practices

Because SEM systems interact with virtually all other systems in an IT environment, deployment of SEM system is a large and complex project and needs to be planned and implemented carefully.

Plan

- SEM planning begins with understanding the scope of the project, in the context of the enterprise. The blog post “Preparing for Security Event Management” [HUTT07] lists the following considerations in planning an SEM system:
- Depending on such factors as the complexity of the infrastructure, SEM tools, and configured pattern/logic, the deployment of an implementation can take from a month up to a year.
- The load generated by SEMS may require the use of several dedicated servers.
- The real-time nature of alerts may result is substantial volumes of data. Thus the SEM planners need to carefully consider performance and sizing requirements.
- A large, distributed installation requires careful network planning, that includes consideration of bandwidth demands and modes of failure.
- Some systems require the installation of agents to relay information to SEM collectors, while others are agentless.
- Any return on investment (ROI) from SEM is proportional to the care and attention spent training analysts in its proper use.

With an understanding of the scale of a SEM project, a management team assigns responsibilities and authority for aspects of the project and determines which IT and IT security staff need to be involved in development, deployment, and use of SEM. At this point, it is important to address more specific questions about the SEM to guide acquisition and development, including the following:

- Which systems should be monitored?
- Which events are important, and what information should be collected from the local logs?
- Where should the central event log be stored, and how will it be protected and accessed?
- How long should log data be retained?
- How will the event data be analyzed to generate meaningful alerts and metrics?
- How will the performance of the SEM system be monitored?

Assess

The current security status of an IT system needs to be assessed. This involves performing a baseline vulnerability assessment on existing systems. At minimum, a team should remedy the most serious vulnerabilities for the most valuable assets. Once this is done, the team needs to assess the SEM requirements for the enterprise. The blog post “Preparing for Security Event Management” [HUTT07] lists the following objectives:

- Understand your priorities. What systems should you plug into the SEM first, and what part of your IT is subject to the most attacks?

- Determine which portions of the IT infrastructure are critical. This will dictate the level of alert level settings configure within the SEM for various IT infrastructure components.
- Determine which events are logged and which are not, as well as the level of detail of the logging for each logged event.
- Develop an inventory of all security products, their intended use, and whether or not each product is being used properly.
- Understand where you need vulnerability remediation before event management. SEM software works best when used to monitor well-configured systems; it does not fix things that are currently insecure or broken.

Simplify

A simplification of the overall security infrastructure has benefits in and of itself and also makes the task of SEM easier. There are several considerations in this regard:

- Over time, the security infrastructure can contain elements that are either no longer needed because they duplicate other functions or that are configured or deployed ineffectively. Remove, reconfigure, or redeploy these elements.
- As much as feasible, retire legacy software and equipment and consolidate external routes into the enterprise network.
- Consider grouping high-value assets together for highest security.
- Deploy a default deny policy as broadly as possible. For example, perhaps only user actions that are specifically allowed are performed, and all others are prohibited. Or maybe applications on a whitelist are allowed to run, and all others are automatically blocked. Default deny makes for short and elegant configuration, fewer events that need investigation, and greater overall security.

Another aspect of simplification is to configure and deploy systems in such a way as to reduce the number of alerts and especially the number of false positives. For example, logically group servers so that sensors selectively ignore Windows attacks directed at UNIX systems and vice versa.

6.5 Threat Intelligence

Threat intelligence, also known as cyber threat intelligence (CTI), or cyberintelligence, is the knowledge established as a result of analyzing information about potential or current attacks that threaten an organization. The information is taken from a number of internal and external sources, including application, system, and network logs; security products such as firewalls and intrusion detection systems; and dedicated threat feeds.

Threat Taxonomy

In order to effectively use threat intelligence and respond to attacks, it is important to have a clear understanding of the types of threats faced by the enterprise. This entails understanding the potential sources of threats as well as the types of threats that may occur.

Threat Sources

The nature of threats depends to a great extent on the type of source. Threat sources can be categorized as follows:

- Adversarial: Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (that is, information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)
- Accidental: Erroneous actions taken by individuals in the course of executing their everyday responsibilities
- Structural: Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters
- Environmental: Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization
-

Types of Threats

A number of organizations have published taxonomies or catalogs of threat types. NIST provides a catalog consisting of 83 adversarial threat events and 18 non-adversarial threat events in SP 800-30, Guide for Conducting Risk Assessments. The adversarial threats are organized based on the cyber attack kill chain, discussed in Section 15.5. The non-adversarial threat events include user error, hardware failures, and environmental events. The European Union Agency for Network and Information Security (ENISA) Threat Taxonomy [ENIS16] lists 177 separate threats. The Web Application Security Consortium (WASC) Threat Classification [WASC10] lists 34 threat types. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) list 22 adversarial threats, 11 accidental threats, and 13 environmental threats; Table 15.2 shows the SGP's lists of threats.

TABLE 15.2 Threats Defined in the SGP

Adversarial Threats	Accidental Threats
Session hijacking	User error (accidental)
Unauthorized access to legitimate authentication credentials	Mishandling of critical and/or sensitive information by authorized users
Exploit vulnerable authorization mechanisms	User error (negligence)
Unauthorized monitoring and/or modification of communications	Loss of information systems
Denial of service (DoS) attack	Undesirable effects of change
Exploit insecure disposal of an organization's information assets	Resource depletion
Introduce malware to information systems	Misconfiguration
Exploit misconfigured organizational information systems	Maintenance error
Exploit design or configuration issues in an organizations remote access service	Software malfunction (internally produced software)
Exploit poorly-designed network architecture	Software malfunction(externally acquired software)
Misuse of information systems	Accidental physical damage
Unauthorized physical access to information systems	**Environmental Threats**
Physical damage to or tampering with information systems	Pathogen (e.g., disease outbreak)
Theft of information system hardware	Storm (hail, thunder, blizzard)
Conduct physical attacks on organizational facilities or their supporting infrastructure	Hurricane
Unauthorized network scanning and/or probing	Tornado
Gathering publicly-available information about an organization	Earthquake
Phishing	Volcanic eruption
Insert subversive individuals into organizations	Flooding
Interpersonal manipulation	Tsunami
Exploit vulnerabilities in an organization's information systems	Fire (wild)
Compromise supplier or business partner of target organization	Power failure or fluctuation
	Damage to or loss of external communications
	Failure of environmental control systems
	Hardware malfunction or failure

It is useful to study these various lists to gain an appreciation of the breadth of threats confronting the enterprise.

phishing
A digital form of social engineering that attempts to acquire sensitive data, such as bank account numbers or passwords, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

The Importance of Threat Intelligence

The primary purpose of threat intelligence is to help organizations understand the risks of the most common and severe external threats, such as advanced persistent threats (APTs), exploits, and zero-day threats. Although threat actors also include internal (or insider) and partner threats, the emphasis

is on the types of external threats that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself against the types of attacks that could do them the most damage.

advanced persistent threat (APT): A network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry. APTs differ from other types of attacks in their careful target selection and persistent, often stealthy, intrusion efforts over extended periods.

Exploit: An attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders.

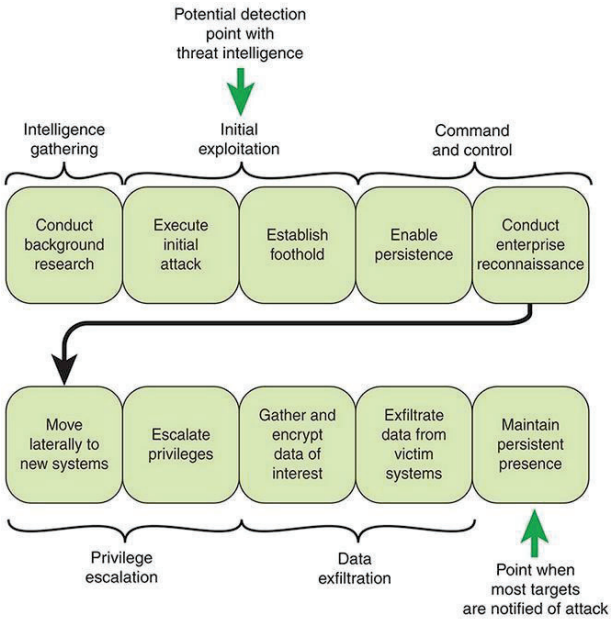


FIGURE 15.4 Potential Benefit of Threat Intelligence

zero-day threat: The threat of an unknown security vulnerability in a computer software or application for which either a patch has not been released or the application developers are unaware or have not had sufficient time to address the issue. A zero-day attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

As an example of the importance of threat intelligence, Figure 15.4, based on one in the Information Systems Audit and Control Association's (ISACA's) Responding to Targeted Cyberattacks [ISAC13], illustrates the impact of threat intelligence on an APT attack.

A typical APT attack proceeds through the following steps:

1. Conduct background research. An APT attack begins with research on potential targets to identify specific avenues of attack. This maximizes the chance of the target reacting as desired.

2. Execute the initial attack. Typically, the initial attack targets one or more specific individuals through some form of social engineering: embedding a link to malicious content into an email message, an instant message, or a social media posting or another attack vector and then persuading the target to open an attachment or click on a link to infect one or more devices with malicious software.

3. Establish a foothold. The APT establishes an initial foothold into the target environment by using customized malware. In almost every case, that custom software does not trigger any antivirus alert, but it does let the APT know about the successful attack. The initial infection tool, sometimes called first-stage malware, can have very little malicious functionality, but it generally is able to beacon home and download additional functionality, sometimes called second-stage malware.

4. Enable persistence. One of the primary objectives of the APT is to establish persistent command and control over compromised computers in the target environment—meaning control and access that survives a reboot of the targeted device and provides the APT with regular connectivity to the target environment. In most cases, this persistence is established simply by installing new services (including the attacker's command-and-control software) on the target computer that automatically start when the computer boots.

5. Conduct enterprise reconnaissance. After establishing persistent access to the target environment, the APT typically attempts to find the servers or storage facilities holding the targeted information. In most cases, the reconnaissance uses the tools available on the compromised computers. In some cases, the APT uploads scanning tools to search for specific types of systems (for example, identity and access management, authentication, virtual private networks [VPNs], database or email servers).

6. Move laterally to new systems. Part of enterprise reconnaissance necessarily includes moving laterally to new systems to explore their contents and understand the new parts of the enterprise accessed from the new systems. The APT can directly install command-and-control software on new systems to expand persistent access to the environment.

7. Escalate privileges. As the attackers conduct reconnaissance and move around the network using the compromised credentials of their first few targets, they inevitably seek to escalate from local user to local administrator to higher levels of privilege in the environment so that they are not constrained to any specific part of the environment. In enterprises where access to information is tightly controlled, compromising all the credentials in the environment allows the attackers to masquerade as anyone in the environment and access any resource they desire.

8. Gather and encrypt data of interest. Having found the data of interest to the attackers, the APT generally gathers the data into an archive and then compresses and encrypts the archive. This enables the APT to hide the contents of the archive from technologies that include deep packet inspection and data loss prevention (DLP) capabilities at the enterprise boundary.

9. Exfiltrate data from victim systems. The APT uses a variety of tools and protocols to surreptitiously transfer data from the target systems.

10. Maintain persistent presence. An APT seeks to attain what its controllers have tasked it to do: maintain access to the target environment. It is not uncommon for the APT to sit undetected in an enterprise network for lengthy periods of time before being activated.

As Figure 15.4 indicates, threat intelligence enables a security team to become aware of a threat well before the point of typical notification, which is often after the real damage is done. Even if an early opportunity is lost, threat intelligence reduces the time it takes to discover that an attack has already succeeded and therefore speeds up remediation actions to limit the damage.

Gathering Threat Intelligence

The starting point for using threat intelligence is, of course, to gather that intelligence. This section looks at the wide variety of sources available to assist security personnel in this task.

External Sources

While it is possible to assign the threat intelligence task to one or more employees whose job it is to engage in research on existing and evolving threats, a more effective approach is to subscribe to a regular feed of threat data from a threat intelligence subscription service. One commercial example is Wapack Labs Cyber Threat Analysis Center.

Wapack Labs Cyber Threat Analysis Center http://www.wapacklabs.com/

There are a number of cyberintelligence vendors whose services can be employed. In addition, many of the sources of vulnerability information, such as CERTs, discussed in Section 15.1, are useful sources of threat intelligence.

Another useful source of threat intelligence is information sharing and analysis centers (ISACs). An ISAC is a nonprofit organization, generally sector specific, that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector. In the United States, the National Council of ISACs is a central home for many ISACs. Although U.S. based, these ISACs generally have global significance.

National Council of ISACs https://www.nationalisacs.org

Internal Sources

Various activities in the IT infrastructure of an enterprise signal that an attack is imminent or that a threat is developing. The SGP lists the following examples:

- Event logs from technical infrastructure, such as operating system logs (for example, from servers and mobile devices; authentication and DNS [Domain Name System] logs; service and application logs; and network device logs)
- Alerts from security systems such as firewalls, malware protection, DLP, network-based intrusion detection systems (NIDSs), gateway proxy servers, and physical security systems
- Direct feeds from security event management utilities, such as those produced by security event logging software or a security information and event management (SIEM) system
- security information and event management (SIEM)
- An application or set of tools that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
- Dedicated teams that perform information security–related activities (for example, those responsible for incident management, IT help desk functions, and forensic investigations)
- Business support functions (for example, legal, human resources, audit, physical security, facilities)

Threat Analysis

Threat analysis includes the task of describing the type of possible attacks, potential attackers, and their methods of attack and the consequences of successful attacks. It involves the following:

- Identifying the vulnerabilities of the system
- Analyzing the likelihood of threats aimed at exploiting these vulnerabilities
- Assessing the consequences that would occur if each threat were to be successfully carried out
- Estimating the cost of each attack
- Costing out potential countermeasures
- Selecting the security mechanisms that are justified (possibly by using cost/benefit analysis)

An organization should carry out this analysis as a regular part of risk management. Then, when the security team is alerted to a new threat, there is already a plan in place to deal with that threat. If the threat is one that has not been anticipated, then the previously mentioned analytical steps need to be carried out with reference to this new threat.

6.6 Cyber Attack Protection

The National Information Assurance Glossary [CNSS10] defines cyber attack as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Attack Kill Chain

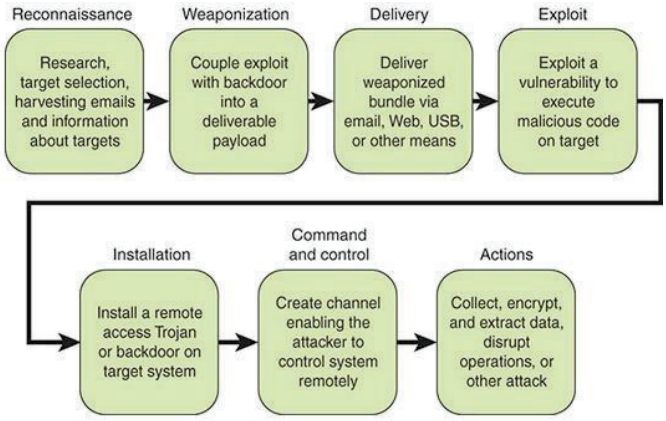


FIGURE 15.5 Cyber Attack Kill Chain

The concept of a cyber attack kill chain was introduced in Chapter and is illustrated in Figure 15.5. Note that APTs, discussed earlier in this chapter, are a form of cyber attack (refer to Figure 15.4). The following sections consider each of the phases of a cyber attack kill chain in turn.

Reconnaissance

In the first stage of a typical cyber attack, the attacker decides whether the potential target is in fact a promising target and, if so, the best means of attack. Ideally, the attacker looks for a target that exhibits both serious vulnerabilities and valuable data. If the target is particularly high value, the attacker can attempt the attack even if there are few vulnerabilities.

There are a number of potential sources of information about a target:

- Names and contact details of employees online: Even if these are not provided on the enterprise website, they may be available through social networks. This information may be used for social engineering purposes.

social engineering

The process of attempting to trick someone into revealing information (for example, a password) or performing an action that can be used to attack an enterprise or into performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

- Details about enterprise web servers or physical locations online: These details are used for social engineering or to narrow down a list of possible exploits that could be used break into the enterprise's environment.
- Emails and other network traffic: This information may be used for social engineering or to gain insight into possible avenues of attack.

The means of performing reconnaissance include the following:

- Perform perimeter network reconnaissance/scanning

- Perform network sniffing of exposed networks
- Gather information using open source discovery of organizational information
- Perform surveillance of targeted organizations over time to examine and assess organizations and ascertain points of vulnerability
- Perform malware-directed internal reconnaissance

Weaponization

At this stage, an attacker prepares an attack payload and crafts a tool to deliver the attack, using the gathered information. This step happens at the attacker side, without contact with the victim.

SP 800-30 lists the following types of attack tools:

- Phishing attacks
- Spear phishing attacks
  spear phishing: Phishing that is targeted against a group, a company, or individuals within a company.
- Attacks specifically based on deployed information technology environment
- Counterfeit/spoof website
- Counterfeit certificates

Delivery

During the delivery phase, the attacker sends the malicious payload to the victim by one of many intrusion methods. Possible methods of delivery include email, web traffic, instant messaging, and File Transfer Protocol (FTP). The payload can also be placed on removable media (for example, flash drives) and social engineering techniques can be used to persuade an employee to install the malware from the media to the enterprise's information systems. SP 800-30 lists a number of other delivery techniques, including the following:

- Insert malware into common freeware, shareware, or commercial IT products. This technique does not target a specific organization but is a way to find targets of opportunity.
- Insert malware into organizational information systems and information system components (for example, commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
- Replace critical information system components with modified or corrupted components. This is done through the supply chain, a subverted insider, or some combination thereof.
- Place individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.

Exploit

During the exploit phase, the delivered payload is triggered and takes action on the target system to exploit a vulnerability. This phase is concerned with gaining entry to the system in order to begin the actual attack. This phase can make use of a vulnerability known to the attacker, or the initially delivered payload can search for and discover vulnerabilities that enable continuing and expanding the attack.

A wide variety of attacks are possible at this stage, encompassing all the threat categories discussed in this book (for example, exfiltrating data, modifying data, compromising availability).

Installation

During the installation phase, the attacker installs components that permit permanent control of the target system. The objective is to mount further attacks on the enterprise. At this stage, the attacker can also elevate user privileges of installed malware and install persistent payload.

Command and Control

The attacker creates a command-and-control channel in order to continue to operate the internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed. Among other actions at this stage, the adversary can take actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations. The adversary can adapt behavior in response to surveillance and organizational security measures.
Actions

The attacker performs the steps to achieve his or her goals inside the victim's network—to obtain information, destroy information, or disrupt systems or networks. This can be an elaborate active attack process that takes months and thousands of small steps to achieve.
Protection and Response Measures

The following sections describe the steps an organization can take to reduce its vulnerability to each of the phases of the cyber attack kill chain described in the preceding section.
Dealing with the Reconnaissance Phase

A number of techniques can be used to detect reconnaissance attempts. For websites, web analytics can detect behavior that is more in line with an attacker than a benign user. For any type of traffic, scanning the source IP addresses for those with known bad reputations is fruitful. Multiple events occurring from the same address in a small time frame may indicate a reconnaissance effort.

web analytics

The process of analyzing the behavior of visitors to a website. This process involves extracting and categorizing qualitative and quantitative data to identify and analyze onsite and offsite patterns and trends.

Prevention methods include the use of firewalls, especially if a default deny policy is used, whitelisting, and segmenting enterprise networks.

Dealing with the Weaponization Phase

As defined here, weaponization is a process that occurs at the attacker site and thus cannot be detected by the target. However, rapid patching and updating in addition to a regular routine of vulnerability fixing can thwart a weaponization effort by eliminating the vulnerability before it is exploited. This highlights the necessity of obtaining and acting on threat intelligence in a timely manner.

Dealing with the Delivery Phase

They key to preventing delivery is to maintain a robust security training and awareness program so that social engineering efforts are more likely to fail.

A variety of technical tools are used to prevent delivery, including the following:

- Antivirus software: Antivirus software is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. It is important to continuously run antivirus software to identify, trap, and destroy incoming known viruses. If a virus is detected, the antivirus software is configured to trigger a scan of the rest of the IT infrastructure for indicators of compromise associated with this outbreak.
- Firewall: A firewall blocks delivery attempts from known or suspected hostile sources.
- Intrusion prevention system (IPS): An IPS is a system that detects an intrusive activity and also attempts to stop the activity—ideally before it reaches its targets. It is similar to an intrusion detection system but is proactive in attempting to block the intrusion.

Dealing with the Exploit Phase

Countermeasures at the exploit stage include the following:

- Host-based intrusion detection systems (HIDS): Once an exploit is inside the enterprise network and attacking hosts, a HIDS detects and alerts on such attempts.
- Regular patching: Patching discovered vulnerabilities helps contain the damage.
- Data restoration from backups: Once an exploit is discovered and removed, it may be necessary to restore a valid copy of data from a backup.

Dealing with the Installation Phase

Tools that detect suspicious software or behavior, such as antivirus software and HIDS, are appropriate at the installation stage. These tools include specific actions such as the following:

- An organization should remediate any malware infections as quickly as possible before they progress. Scan the rest of the enterprise network for indicators of compromise associated with this outbreak.
- Sometimes a distributed denial-of-service (DDoS) attack is used to divert attention away from another, more serious, attack attempt. Increase monitoring, investigate all related activity, and work closely with the enterprise Internet service provider (ISP) or other service provider.

  distributed denial-of-service (DDoS) attack
  A DoS attack in which multiple systems are used to flood servers with traffic in an attempt to overwhelm available resources (transmission capacity, memory, processing power, and so on), making them unavailable to respond to legitimate users.
- An organization should detect, monitor, and investigate unauthorized access attempts, giving priority to those that are mission critical and/or contain sensitive data.
- An organization should identify the privileged user accounts for all domains, servers, apps, and critical devices. Monitoring should be enabled for all systems, and for all system events, and the monitoring system should feed the log monitoring infrastructure.
- An organization should configure critical systems to record all privileged escalation events and set alarms for unauthorized privilege escalation attempts.

Dealing with the Command-and-Control Phase

Countermeasures at the command-and-control stage include the following:

- Network-based intrusion detection systems (NIDS): A NIDS can detect and alert on attempts to use an unauthorized or suspicious channel.

- Firewall: A firewall blocks communication with known or suspected hostile sources and also blocks suspicious activity or packet content.
- Tarpit: This is a service on a computer system (usually a server) that delays incoming connections for as long as possible. Tarpits were developed as a defense against computer worms, based on the idea that network abuses such as spamming or broad scanning are less effective if they take too long. A tarpit is used for incoming traffic that is not on an approved source whitelist.

Dealing with the Actions Phase

If an attack gets to the stage of ongoing advanced attacks, a critical aspect of security is a backup policy. An organization should regularly back up all critical data and systems; test, document, and update system recovery procedures; and, during a system compromise, capture evidence carefully and document all recovery steps as well as all evidentiary data collected.

Incident management, discussed in Sections 15.6 and 15.7, is relevant for this stage.

Non-Malware Attacks

An increasingly important category of cyber attacks is referred to as non-malware attacks. The chief characteristic of a non-malware attack is that it does not involve downloading any malicious files or code onto target devices. Rather, the attacker uses existing software on target machines, whitelisted applications, and authorized protocols to carry out malicious activities. Non-malware attacks can appear at several points along the cyber kill chain. Among the most common types of non-malware attacks are the following:

- Remote logins
- **Windows Management Instrumentation (WMI)**–based attacks: Windows Management Instrumentation (WMI)- A protocol to pull system metadata from Microsoft Windows devices, most notably operating system and software version data.
- **PowerShell-based attacks:** PowerShell - A scripting language and related facilities that provides rich access to Window systems, including access to security settings.
- Attacks leveraging Office macros

When dealing with security events other than malware, the difficulty of automating the process of responding is significantly greater. When antivirus software or other incident monitoring software encounters malware, the malware can be automatically removed or isolated for further analysis. But an intrusion or another indicator of compromise may require both automated tools for recognition and human involvement for response. The article “Restoring Machine Learning’s Good Name in Cybersecurity” [CHES17] gives the following example: For a typical scenario in a medium-to-large company, the security analyst’s procedure for confronting a potential breach consists of the following:

- Identify a security event.
- Try to identify the attack intent based on the event name and description (which is rarely satisfactory, as the event name is usually too generic and the description too vague to accurately represent the intent).
- Search for and collect relevant, potentially useful data from third-party threat centers, security blogs, intelligence reports, and similar sources.
- Begin analyzing data.

- Determine event intent and possible impact on the organization, based on associated threat information.

But an analyst's job doesn't end there. All such events in an organization must be aggregated in an effort to find cause-and-effect correlations to reveal potential coordinated attack campaigns. When there are numerous security events to process in a short time, which is typical, the task becomes impossible.

An increasingly popular approach to overcoming this problem is to use artificial intelligence (AI) and machine learning (ML) software:

- Artificial intelligence: Technology that appears to emulate human performance, typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance (also known as cognitive computing), or replacing people on execution of nonroutine tasks. AI implies the capability to learn and adapt through experience and to come up with solutions to problems without using rigid, predefined algorithms, which is the approach of non-AI software.
- Machine learning: AI software that modifies its own algorithms in order to become more intelligent and improve future results. Unlike the static logic ("if this, do that") in regular programs, machine learning continues to refine its logic so that the next operation is more effective than the preceding one.

A number of vendors now offer ML and AI products to support cyber response efforts. However, this technology has not reached the level of maturity required to significantly improve protection. A recent report by Carbon Black [CARB17] aggregates insight from more than 400 interviews with leading cybersecurity researchers, summarized as follows:

- Non-malware attacks are considered more threatening than malware- based attacks.
- Non-malware attacks are increasingly leveraging native system tools, such as WMI and PowerShell, to conduct nefarious actions.
- Confidence in the ability of legacy antivirus software to prevent non-malware attacks is low.
- AI is considered by most security researchers to be in its nascent stages and not yet able to replace human decision making in cybersecurity.
- Researchers say attackers can bypass ML-driven security solutions.
- Cybersecurity talent, resourcing, and trust in executives continue to be top challenges plaguing many businesses.

6.7 Security Incident Management Framework

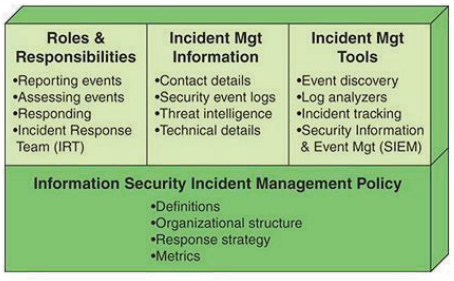


FIGURE 15.6 Security Information Management Framework

The ISO 27000 suite defines information security incident management as consisting of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. This section examines the management framework for security information management, which comprises the relevant individuals, information, and tools required by the organization's information security incident management process. Figure 15.6 highlights the four key elements of an incident response framework, which are discussed subsequently in this section. The purpose of the framework is to ensure the availability of resources that are required to help resolve information security incidents quickly and effectively. Section 15.7 examines the security incident management process.

A number of standards are relevant to the implementation of security incident management, including the following:

- ISO 27002, Code of Practice for Information Security Controls: Provides a comprehensive checklist of management practices for incident response.
- ISO 27035-1, Information Security Incident Management—Part 1: Principles of Incident Management: Presents basic concepts and phases of information security incident management and how to improve incident management. This part combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents and applying lessons learned.
- ISO 27035-2, Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Response: Describes how to plan and prepare for incident response. Provides a very detailed discussion of what should go into an information security incident management plan.
- ITU-T X.1056, Security Incident Management Guidelines for Telecommunications Organizations: Provides practical guidance on how to respond to incidents effectively and efficiently.
- NIST SP 800-61, Computer Security Incident Handling Guide: Provides detailed guidance for planning, managing, and implementing an incident response plan.
- RFC 2350, Expectations for Computer Security Incident Response: Describes issues and requirements for managing incident response.

It is the responsibility of the security managers to review all these documents.

Objectives of Incident Management

ISO 27035-1 lists the following as the objectives for security incident management:

- Information security events are detected and dealt with efficiently, in particular deciding when they are to be classified as information security incidents.
- Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
- The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
- A link is established with relevant elements from crisis management and business continuity management through an escalation process.
- Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents.
- Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism increases the chances of preventing future information security incidents from occurring, improves the implementation and use of information security controls, and improves the overall information security incident management plan.

Relationship to Information Security Management System

Figure 15.7, adapted from figures in ISO 27035-1, indicates the relationship between information security incident management and an information security management system (ISMS) (refer to Figure 2.1). The upper part of the figure, bounded by dashed lines, illustrates the relationships among objects in an information security incident. A threat causes a security event by exploiting a vulnerability, which enables the threat to create the event. The event is potentially an incident that impacts information assets exposed by vulnerabilities and compromises the operations supported by the information assets. In the upper part of the figure, the shaded objects are preexisting and affected by the unshaded objects.

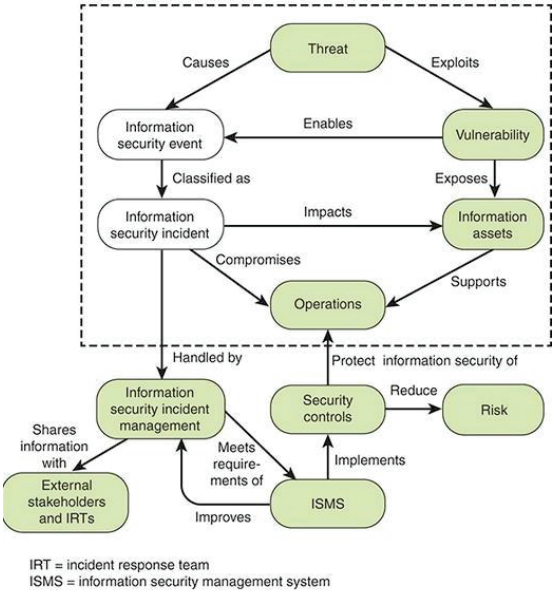


FIGURE 15.7 Security Incident Management in Relation to ISMS and Applied Controls

The lower part of Figure 15.7 indicates the bigger picture, showing how security incident management relates to risk management and an ISMS.

Incident Management Policy

Essential to successful incident management is a documented incident management policy. Such a policy should have sections that deal with overall management, including the following topics:

- A specification of internal and external interested parties
- An agreed-on definition of incident and guidelines to identify a security incident
- A definition of incident response/handling and its overall objectives and scope
- A statement of management intent, supporting the goals and principles of incident response/handling
- A brief explanation of the incident response/handling policies, principles, standards, and compliance requirements that are of particular importance to the enterprise
- A definition of general and specific responsibilities for incident response/handling, including handling of evidence and reporting
- References to documentation that supports the policy, such as detailed incident response/handling, incident triage, and computer forensic policies and procedures
- User awareness training pertaining to incident identification and reporting
- Metrics for measuring the incident response capability and its effectiveness

The policy should also cover the strategy for dealing with incidents, including the following topics:

- Identification of an incident and response (for example, shutdown, containment, quarantine)
- Acquisition of volatile and static data
- Retention and analysis of data
- Remediation
- Referral to law enforcement
- Handling of forensic data
- Escalation of incidents

- Reporting of findings
- Definition of the learning process from incidents to upgrade systems and processes

Roles and Responsibilities

The information security incident management framework defines the roles and responsibilities of the information security incident management team and others involved in responding to incidents. ISO 27035-2 lists the following incident management responsibilities for which personnel need to be assigned:

- Detecting and reporting information security events. (This is the responsibility of any permanent or contracted personnel in an organization and its companies.)
- Assessing and responding to information security events and incidents and being involved in post-incident resolution activities. These activities include learning and improving information security and the information security incident management plan itself. These activities are the responsibility of members of the point of contact team, the incident response team, management, public relations personnel, and legal representatives.
- Reporting information security vulnerabilities and dealing with them. (This is the responsibility of any permanent or contracted personnel in an organization and its companies.)

Most organizations want to create a formal information security incident response team (IRT). X.1056 defines an IRT as a team of appropriately skilled and trusted members of the organization, which handles security incidents during their life cycle. At times, external experts may supplement this team. Members of the team should have the following backgrounds/skill sets:

- Understanding of known threats, attack signatures, and vulnerabilities
- Understanding of the enterprise network, security infrastructure, and platforms
- Experience in security response and/or troubleshooting techniques
- Experience in forensic techniques and best practices
- Understanding of regulations and laws as they pertain to privacy and disclosure and evidentiary requirements
- Understanding of systems, threats, and vulnerabilities, and remediation methods in their area of business responsibility

Part-time or liaison members of the IRT should be well versed in the following key areas:

- Information technology
- Information security
- Corporate communications
- Human resources
- Legal
- Business unit management and technology specialists
- Corporate security (including physical security)

The IRT's primary responsibility is to respond to incidents throughout the incident response life cycle, as described in Section 15.7. The IRT is also involved in making recommendations for improving security practices and implementing new security controls.

Incident Management Information

The information security incident management framework is responsible for detailing the types of information needed to assist information security incident management. The SGP lists the following information types needed for incident management:

- Contact details for relevant parties, such as business managers, technical experts (such as those in a security operations center [SOC] or equivalent), and external suppliers
- Security-related event logs (for example, those produced by applications, systems, network devices, and security products)
- Details about affected business environments, such as processes, operations, and applications
- Technical details, such as network diagrams, system configurations, and external network connections
- Threat intelligence and the results of threat analysis

Incident Management Tools

The information security information management framework specifies the tools needed to assist information security incident management (for example, checklists, e-discovery software, log analyzers, incident tracking software, forensic analysis software).

One of the most important incident management tools is a SIEM system. SIEM is a broader term than SEM and refers to a more comprehensive system of information collection and subsequent action. Capabilities of a typical SIEM include the following, according to ISACA's Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives [ISAC10]:

- Data collection: In a typical use case, a SIEM solution must be able to touch a number of different systems: firewalls, proxy servers, databases, intrusion detection and prevention systems, operating systems, routers, switches, access control systems, and so on. Some of these share similar logging and alert functions, but frequently there is significant variation in the format, protocol, and information provided.
- Data aggregation: The aggregator serves as a consolidating resource before data is sent to be correlated or retained.
- Data normalization: Normalization is the process of resolving different representations of the same types of data into a similar format in a common database.
- Correlation: Event correlation is the function of linking multiple security events or alerts, typically within a given time window and across multiple systems, to identify anomalous activity that is not evident from any singular event.
- Alerting: When data that trigger certain responses (such as alerts or potential security problems) are gathered or identified, SIEM tools activate certain protocols to alert users, such as notifications sent to the dashboard, an automated email, or text message.
- Reporting/compliance: Protocols in a SIEM are established to automatically collect data necessary for compliance with company, organizational, and government policies. Both custom reporting and report templates (generally for common regulations such as the Payment Card Industry Data Security Standard [PCI DSS] and the U.S. Sarbanes-Oxley Act) are typically part of a SIEM solution.
- Forensics: The ability to search log and alert data for indicators of malicious or otherwise anomalous activities is the forensic function of the SIEM. Forensics, which is supported by the event correlation and normalization processes, requires highly customizable and detailed query capabilities and drill-down access to raw log files and archival data. Working in concert, these technologies greatly enhance the investigative capabilities of security analysts, just as

data collection, aggregation, and correlation technologies enhance their ability to detect and respond to real-time events.

- Retention: Data need to be stored for long periods so that decisions can be made based on more complete data sets.
- Dashboards: Dashboards are used to analyze and visualize data in an attempt to recognize patterns or target activity or data that do not fit into a normal pattern.

6.8 Security Incident Management Process

Many organizations react in an ad hoc manner when a security incident occurs. Because of the potential cost of security incidents, it is cost-beneficial to develop a standing capability for quick discovery and response to such incidents. This capability also serves to support the analysis of past security incidents with a view to improving the ability to prevent and respond to incidents.

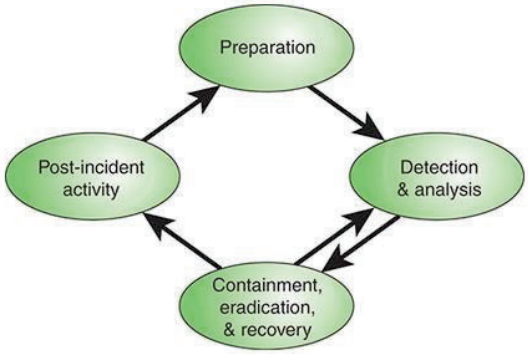


FIGURE 15.8 Incident Response Life Cycle

SP 800-61 defines a four-phase incident management process, as shown in Figure 15.8, that serves as a useful way of structuring the discussion.

Preparing for Incident Response

An effective incident response capability requires the participation of a number of people within the organization. Making the right planning and implementation decisions is key to establishing a successful incident response program. Tasks involved in preparing for incident response include the following:

- Develop an organization-specific definition of the term incident so that the scope of the term is clear
- Create an incident response policy
- Develop incident response and reporting procedures
- Establish guidelines for communicating with external parties
- Define the services that will be provided by the IRT
- Select an organizational structure and staffing model for incident response
- Staff and train the IRT
- Establish and maintain accurate notification mechanisms
- Develop written guidelines for prioritizing incidents
- Have a plan for the collection, formatting, organization, storage, and retention of incident data

Detection and Analysis

Perhaps the most challenging phase of the incident response life cycle is detection and analysis, which consists of determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

Incident Detection

Sections 15.2 and 15.3 discuss event logging and management in some detail. As part of the incident response life cycle, security incidents must be detected from among the numerous security events logged and recorded.

Key aspects of incident detection include the following:

- All IT personnel and users need to be trained and comfortable regarding procedures for reporting failures, weaknesses, and suspected incidents; methods to recognize and detect problems with security protections; and how to escalate reporting appropriately.
- Technical controls must be implemented for the automated detection of security incidents from event logs, coupled with reporting that is as near real time as possible. Key technical tools include IDSs and continuously monitoring antivirus software.
- Situational awareness information needs to be collected from internal and external data sources, including local system and network traffic and activity logs; news feeds concerning ongoing political, social, or economic activities that might impact incident activity; and external feeds on incident trends, new attack vectors, current attack indicators, and new mitigation strategies and technologies.
- Digital evidence needs to be gathered and stored securely, and its secure preservation must be continually monitored in case the evidence is required for legal prosecution or internal disciplinary action.

Analysis

Once an incident is detected, it is appropriate to move immediately to the next phase of the life cycle, which deals with removing the threat and recovery from any damage. Most enterprises choose to do a more in-depth analysis at this point. Typical actions include the following:

- Determine the magnitude of the impact. Consider the number of users affected or the number of devices or the segments of the network.
- Assess the severity. What is the sensitivity of the data involved? What is the criticality of the service, or system, or application? What is the potential for damage or liability?
- Assess the urgency of the event. Is it an active problem, a threat, or an event-in-progress? Was the problem discovered after the fact? Is the intrusion dormant or completed? Does this involve use of an account rather than a system? Does this involve the safety or privacy of individuals?

The analysis also needs to determine whether immediate action is needed to remove the vulnerability or to block the action that enabled the incident to occur. Such analysis may also be part of the post-incident activity phase.

Containment, Eradication, and Recovery

The containment, eradication, and recovery phase is the central task of incident management. If prevention measures failed and an incident occurs, the enterprise needs to stop the attack if it is ongoing and recover from the attack. Actions taken during this phase can conceivably uncover another incident, which feeds back to the detection and analysis phase, as shown in Figure 15.8.

Containment

Most incidents require some sort of containment. The objective is to prevent the spread of the effects of the incident before they overwhelm resources or in some other way increase damage.

Strategies for dealing with various types of incidents must be planned well in advance. The strategy varies depending on the type of incident. For example, email-borne virus, DoS attacks, and intrusion coupled with escalation of privileges require different strategies. In some cases, a system may need to be isolated from the network until it is cleaned. User or system-level accounts may need to be disabled or changed. Active sessions may need to be terminated.

The nature of the strategy and the magnitude of resources devoted to containment depends on criteria developed ahead of time. Examples of criteria include potential damage to and theft of resources, the need to preserve evidence, the effectiveness of the strategy, the time and resources needed to implement the strategy, and the duration of the solution.

Eradication

Once the ongoing damage has been stopped, it may be necessary to perform some sort of eradication to eliminate any residual elements of the incident, such as malware and compromised user accounts.

Recovery

During recovery, IT personnel restore systems to normal operation to the extent possible and, if applicable, harden systems to prevent similar incidents. Possible actions include the following:

- Restoring systems with clean versions from the latest backup
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (for example, firewall rule sets)

Post-Incident Activity

Incident logging capability allows for recording incidents and notes about an incident. After an incident is dealt with in the containment, eradication, and recovery phase, the organization should initiate an evaluation process. This includes lessons-learned meetings and after-action reports. Depending on the type of incident and the security policy, a comprehensive forensic investigation may be warranted, as discussed in Section 15.9, or a comprehensive loss analysis may be undertaken.

Once the incident, its effects, and the magnitude of the effort required to recover are reviewed and analyzed, further action may be needed, such as the following:

- The incident handling process should be reviewed to determine whether the process must be modified and/or more resources committed. Such changes depend on the novelty and severity of the incident.
- Policy and process changes may be warranted. Questions to consider include the following: Were any procedures missing, were communications unclear, or were any stakeholders not appropriately considered? Did the technical staff have appropriate resources (information as well as equipment) to perform the analysis and/or the recovery?
- Other improvements outside the incident management process may be needed, including new or revised technical security controls, updates to awareness and acceptable use policies, and improvements in the areas of threat intelligence and vulnerability assessment.

Table 15.3, from SP 800-61, is a useful checklist for assuring implementation of all phases of the incident response life cycle.

TABLE 15.3 Incident Handling Checklist

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (for example, search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (for example, new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
Post-Incident Activity	
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)

6.9 Emergency Fixes

Security incident emergencies must be handled with a greater sense of urgency than other security incidents. An emergency response may entail making an emergency fix to temporarily eliminate ongoing damage until a more permanent response is provided. Implementing an emergency fix can also require that an information security officer be temporarily given access privileges not normally authorized.

To get a feel for what constitutes an emergency, consider a classification scheme for security incidents suggested in ISO 27035:

- **Emergency**: Severe impact. These are incidents that:
  - Act on especially important information systems and
  - Result in especially serious business loss or
  - Lead to especially important social impact
- Critical: Medium impact. These are incidents that:

    - Act on especially important information systems or important information systems and
    - Result in serious business loss or
    - Lead to important social impact
- Warning: Low impact. These are incidents that:
    - Act on especially important information systems or ordinary information systems and
    - Result in considerable business loss or
    - Lead to considerable social impact
- Information: No impact. These are incidents that:
    - Act on ordinary information systems and
    - Result in minor business loss or no business loss or
    - Lead to minor social impact or no social impact

Table 15.4 provides examples of the types of security incidents that can result in different levels of impact.

TABLE 15.4 Examples of Incident Categories and Severity Classes

	Severity Class			
Incident Category	Information	Warning	Critical	Emergency
Technical attacks	Failed attempts	Single ordinary (user compromise)	Multiple (user compromise) (application privileged access compromise)	Mass (application privileged access compromise)
Technical attacks		Annoyance (scratch the surface)	Disturbance (throughput impact)	Unavailability (stop in service)
Malware	Single known (detected and blocked by antivirus protection)	Single unknown	Multiple infections Server infections	Mass infections

A security policy should include a section related to contingency plans for security incidents that require emergency fixes. It should include the following:

- Procedures for determining that an emergency fix is required
- Emergency contact information
- A summary of methods to be used related to hardware
- A summary of methods to be used related to software
- Procedures for approving emergency fixes and for logging the incident
- Procedures for revoking any emergency access required for the fix
- Procedures for documenting the incident, reviewing the response, and removing the fix
- A list of assets and resources that are most important to protect, with relative priorities assigned

A key aspect of responding to an emergency incident is that one or more individuals must have the authority to make fixes. Security officers must order emergency actions to protect information assets and override administrator privileges and roles to allow emergency access. A good security practice is to share system administrator access privileges with someone other than the system administrator, if for no other reason than to have emergency system access if the administrator is unavailable. But, having said this, such total access also requires total accountability and must be limited to the fewest

number of staff necessary to keep the system secure because each person with total system access has the ability to override any and all security features.

6.10 Forensic Investigations

NIST SP 800-96, Guide to Integrating Forensic Techniques into Incident Response, defines computer forensics, or digital forensics, as the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Computer forensics seeks to answer several critical questions, including the following:

- What happened?
- When did the events occur?
- In what order did the events occur?
- What was the cause of these events?
- Who caused these events to occur?
- What enabled these events to take place?
- What was affected? How much was it affected?

Computer forensic analysis is used for a number of reasons, including the following:

- To investigate crimes
- To investigate suspicious employee behavior
- To reconstruct serious security incidents
- To troubleshoot operational problems
- To support due diligence for audit record maintenance
- To recover from accidental system damage

Most security incidents do not require a forensic investigation but are dealt with using the ordinary incident management process. However, more serious incidents can warrant the more in-depth analysis of a forensic investigation. For example, if an external party such as a customer or supplier suffers a loss as a result of an incident involving the enterprise, forensic analysis can help the enterprise avoid or mitigate liability. As another example, when an employee is fired as a result of an incident but claims that his or her dismissal was unfair or unfounded, improperly processed evidence can make it more difficult to justify the decision and defend against the unfair dismissal claims. Without evidence, the enterprise could be in a potentially costly situation if the employee sues.

Figure 15.9 illustrates the typical phases in the digital forensics process, which are discussed in detail in the following sections.

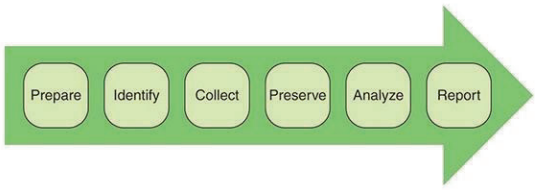


FIGURE 15.9 Phases of Digital Forensics Process

Prepare

Preparation involves the planning and policy-making activities related to forensic investigation. A section of the security policy should deal with computer forensics. SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, recommends the following considerations:

- Ensure that policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures
- Create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations

- Ensure that policies and procedures support the reasonable and appropriate use of forensic tools
- Ensure that IT professionals are prepared to participate in forensic activities

In addition, an organization should establish guidelines on how to manage evidence. Such guidelines help ensure that evidence is preserved throughout the entire investigation process.

The preparation phase also covers other activities, such as staff training, staff recruitment, tool validation, and quality assurance measures.

A vital aspect of preparation is to ensure that the data sources needed for forensic analysis are created and securely stored. Key actions include the following:

- Creating a file system baseline to help detect changes
- Utilizing a central system log server
- Maintaining network-level logging at key control points on the network
- Synchronizing system clocks and log timestamps using central Network Time Protocol (NTP) servers for systems that generate logs

Network Time Protocol (NTP): A protocol that assures accurate local timekeeping on computer systems, network devices, and other system components, with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

- Maintaining protocol activity tables, which are useful when responding to certain types of incidents

The advantage of creating centralized logs is that they are easier to protect than local logs distributed throughout the network, which present a greater attack surface.

Identify

The identification phase is initiated when there is a request for a forensic analysis. This phase involves understanding the purpose of the request and the scope of the investigation, such as type of case, subjects involved, and system involved. A forensic analyst must determine if a request contains sufficient information to start the process. If not, the analyst must coordinate with the requester to determine the next step.

The identification phase determines where the data of interest are stored and what data can be recovered and retrieved. Another task of this phase is to set up and validate forensic hardware and software and create system configuration as needed.

Collect

Once the location or locations of data are identified, the forensic process needs to ensure that the data are collected in a manner that preserves the integrity of the evidence. Typically, enterprise policy requires the use of special-purpose forensic hardware and software to ensure that the original data are never altered and that the evidence collected stands up to legal scrutiny. Once the data are collected, they are verified and backed up to ensure that a valid image exists.

The data collection process includes one or more of the following, depending on the purpose of the forensic analysis:

- Capturing data from system logs, event logs, and incident logs
- Discovering data on computer systems
- Recovering deleted, encrypted, or damaged file information
- Monitoring online activity
- Making a bit-image copy of an affected system's hard drive
- Detecting violations of corporate policy

For this phase, as well as the preservation phase, an organization should use forensic software tools that are well known in the computer forensics community, such as Forensic Tool Kit (FTK) and EnCase.

Preserve

Several actions comprise the preservation of data process, including the following:

- Creating a log that documents when, from where, how, and by whom data were collected
- Storing the data in a secure fashion to prevent tampering or contamination
- Logging each access to the data made for forensic analysis

Analyze

Analysis depends on the specifics of each job. The examiner usually provides feedback to the client during analysis, and from this dialogue the analysis may take a different path or be narrowed to specific areas.

Examples of analysis tasks include:

- Checking for changes to the system such as new programs, files, services, and users
- Looking at running processes and open ports for anomalous behavior
- Checking for Trojan horse programs and toolkits
- Checking for other malware
- Looking for illegal content
- Looking for indicators of compromise
- Determining the who, when, where, what, and how details of a security incident

Numerous forensic analysis tool can assist an analyst, including the following:

- Disk and data capture tools
- File viewers
- File analysis tools
- Registry analysis tools
- Internet analysis tools
- Email analysis tools
- Mobile devices analysis tools
- macOS analysis tools
- Network forensic tools
- Database forensic tools

A helpful resource is the NIST Computer Forensics Tool Testing Program. This program tests available forensic tools and maintains a catalog. It enables practitioners to find tools that meet their specific technical needs. The catalog provides the ability to search by technical parameters based on specific digital forensics functions, such as disk imaging or deleted file recovery.

NIST Computer Forensics Tool Testing Program https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Report

The nature of any report resulting from a forensic investigation depends on the original purpose of the investigation. In general, SP 800-86 lists the following factors that affect reporting for any type of investigation:

- Alternative explanations: The available information may not provide a definitive explanation of the cause and nature of an incident. The analyst should present the best possible conclusions and highlight alternative explanations.
- Audience consideration: An incident requiring law enforcement involvement requires highly detailed reports of all information gathered and can also require copies of all evidentiary data obtained. A system administrator might want to see network traffic and related statistics in great detail. Senior management might simply want a high-level overview of what happened, such as a simplified visual representation of how the attack occurred and what should be done to prevent similar incidents.
- Actionable information: Reporting also includes identifying actionable information gained from data that allows an analyst to collect new sources of information. For example, a list of contacts may be developed from the data that can lead to additional information about an incident or a crime. Also, information that is obtained might help prevent future events, such as learning about a backdoor on a system that is to be used for future attacks, a crime that is being planned, a worm scheduled to start spreading at a certain time, or a vulnerability that could be exploited.

6.11 Threat and Incident Management Best Practices

The SGP breaks down the best practices in the threat and incident management category into two areas and nine topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Cybersecurity resilience: The objective of this area is to manage threats and vulnerabilities associated with business applications, systems, and networks by scanning for technical vulnerabilities, maintaining up-to-date patch levels, performing continuous security event monitoring, acting on threat intelligence, and protecting information against targeted cyber attacks.
- Technical vulnerability management: This topic deals with establishing a process for the identification and remediation of technical vulnerabilities in business applications, systems, equipment, and devices. The objective is to address technical vulnerabilities quickly and effectively, thus reducing the likelihood of their being exploited and preventing serious security incidents.

    - Security event logging: This topic deals with procedures for recording security-related events in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.

    - Security event management: This topic deals with management guidelines for reviewing and analyzing security-related event logs. The objective is to detect known vulnerabilities, detect unusual or suspicious activity, and respond to events that need to be investigated in a timely manner.
    - Threat intelligence: The objective of this topic is to promote situational awareness about current and emerging threats, supporting information risk-related decisions and activities, based on analysis of a range of sources. The SGP discusses internal and external sources of threat information, details that should be included in threat information, analysis policy, and threat intelligence sharing.
    - Cyber attack protection: This topic provides checklists for protecting enterprise assets during all phases of a cyber attack.
- Security incident management: The objective of this area is to develop a comprehensive and documented strategy for managing security incidents, which is supported by a process for the identification, response, recovery, and post-implementation review of information security incidents.
    - Security incident management framework: This topic lists considerations for defining an information security incident management framework, including relevant individuals, information, and tools required by the organization's information security incident management process.
    - Security incident management process: This topic provides a checklist of actions related to detecting, analyzing, containing, recovering from, and learning from security incidents.
    - Emergency fixes: This topic provides a checklist of actions for applying emergency fixes, responding to emergencies in a timely and secure manner, and reducing disruption to the organization.
    - Forensic investigations: This topic provides a checklist of actions for dealing with information security incidents or other events (for example, e-discovery requests) that require forensic investigation.

6.12 Review Questions / Case Studies / Projects

1. Explain the term technical vulnerability. What are five key steps involved in vulnerability management?
2. What are key sources for discovering vulnerabilities?
3. Describe two difficulties, or challenges, that result from the use of vulnerability scans
4. What are some of the common patch management techniques used in organizations?
5. Differentiate between a security event and a security incident.
6. For security event logging, what events should be captured in operating system logs, network device logs, and web server logs?
7. What kind of analysis can you do on cleaned SEM data?
8. How can you categorize threat sources?
9. Briefly describe an APT attack and list the steps in a typical APT attack.
10. What are the steps to prevent delivery of malicious payload in a cyber attack kill chain?

LEARNING OUTCOMES

After reading this Section of the guide, the learner should be able to:

- **Present the X.816 model of security audit and alarms.**
- **List useful information to collect in security audit trails.**
- **Discuss security audit controls.**
- **Understand the use of metrics in security performance monitoring.**
- **Describe the essential elements of information risk reporting.**
- **Discuss what is involved in information security compliance monitoring.**

7.1 Introduction

This chapter looks at two aspects of security monitoring that lead to improvement in organizational security: the security audit and security performance.

7.2 Security Audit

In general terms, an audit in an enterprise is an independent inspection of enterprise records to determine compliance with a standard or policy. More specifically, a security audit relates to security policies and the mechanisms and procedures used to enforce that policy. A security audit trail is an important component of a security audit.

Security Audit

An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

Security Audit Trail

A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

X.816, Security Audit and Alarms Framework, lists the following objectives for a security audit:

- Allows the adequacy of the security policy to be evaluated
- Aids in the detection of security violations
- Facilitates making individuals accountable for their actions (or for actions by entities acting on their behalf)
- Assists in the detection of misuse of resources
- Acts as a deterrent to individuals who might attempt to damage the system

Security audit mechanisms are not involved directly in the prevention of security violations. Rather, they are concerned with the detection, recording, and analysis of events. The basic objective of a security audit is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate security violations.

Security Audit and Alarms Model

X.816 has developed a model that shows the elements of the security auditing function and their relationships to security alarms (see Figure 18.1).

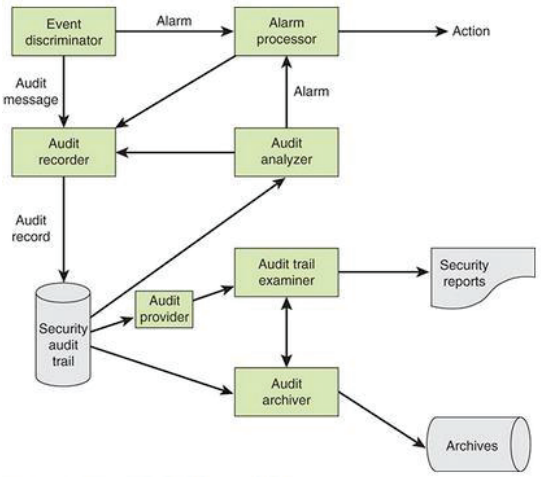


FIGURE 18.1 Security Audit and Alarms Model

The key elements of this model are as follows:

- Event discriminator: This logic embedded in the software of the system monitors system activity and detects security-related events that it was configured to detect.
- Audit recorder: For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission in the form of a message. The audit could also be done by recording the event in a shared memory area.
- Alarm processor: Some of the events detected by the event discriminator are defined to be alarm events. For such events, an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm. This action is itself an auditable event and so is transmitted to the audit recorder.
- Security audit trail: The audit recorder creates a formatted record of each event and stores it in the security audit trail.
- Audit analyzer: The security audit trail is available to the audit analyzer, which, based on a pattern of activity, may define a new auditable event that is sent to the audit recorder and may generate an alarm.
- Audit archiver: This software module periodically extracts records from the audit trail to create a permanent archive of auditable events.
- Archives: The audit archives are a permanent store of security-related events on this system.
- Audit provider: The audit provider is an application and/or user interface to the audit trail.

- Audit trail examiner: The audit trail examiner is an application or a user who examines the audit trail and the audit archives for historical trends, for computer forensic purposes, and for other analyses.
- Security reports: The audit trail examiner prepares human-readable security reports.

As shown, the auditing process begins with the detection of security-related events, which may in turn be determined to be security incidents that produce alarms. Refer to Figure 15.3 in Chapter, "Threat and Incident Management," for details of this process.

Data to Collect for Auditing

The choice of what data to collect should be based on a number of requirements. One issue is the amount of data to collect, which is determined by the range of areas of interest and by the granularity of data collection. There is a trade-off here between quantity and efficiency. The more data collected, the greater the performance penalty on the system. Larger amounts of data may also unnecessarily burden the various algorithms used to examine and analyze the data. Further, the presence of large amounts of data creates a temptation to generate security reports excessive in number or length.

With these cautions in mind, the first order of business in security audit trail design is the selection of data items to capture, including the following:

- Events related to the use of the auditing software (that is, all the components in Figure 18.1)
- Events related to the security mechanisms on the system
- Any events that are collected for use by the various security detection and prevention mechanisms, including items related to intrusion detection and items related to firewall operation
- Events related to system management and operation
- Events related to operating system access (for example, via system calls)
- Events related to application access for selected applications
- Events related to remote access

X.816 suggests the auditing the following:

- Security events related to a specific connection:
  - ✓ Connection requests
  - ✓ Connection confirmed
  - ✓ Disconnection requests
  - ✓ Disconnection confirmed

  Statistics appertaining to the connection
- Security events related to the use of security services:
  - ✓ Security service requests
  - ✓ Security mechanisms usage
  - ✓ Security alarms
- Security events related to management:
  - ✓ Management operations
  - ✓ Management notifications

The list of auditable events should include at least the following:

- Deny access

- Authenticate
- Change attribute
- Create object
- Delete object
- Modify object
- Use privilege

In terms of the individual security services, the following security-related events are important:

- Authentication: Verify success and verify fail
- Access control: Decide access success and decide access fail
- Non-repudiation: Non-repudiable origination of message, non-repudiable receipt of message, unsuccessful repudiation of event, and successful repudiation of event
- Integrity: Use of shield, use of unshield, validate success, and validate fail
- Confidentiality: Use of hide and use of reveal
- Audit: Select event for auditing, deselect event for auditing, and change audit event selection criteria

The standard points out that both normal and abnormal conditions may need to be audited; for instance, each connection request, such as a Transmission Control Protocol (TCP) connection request, may be a subject for a security audit trail record, whether or not the request was abnormal and regardless of whether the request was accepted. This is an important point. Data collection for auditing goes beyond the need to generate security alarms or to provide input to a firewall module. Data representing behavior that does not trigger an alarm are used to identify normal versus abnormal usage patterns and thus serve as input to intrusion detection analysis. Also, in the event of an attack, an analysis of all the activity on a system may be needed to diagnose the attack and arrive at suitable countermeasures for the future.

As a security administrator designs an audit data collection policy, it is useful to organize the audit trail into categories for purposes of choosing data items to collect. The following sections look at categories for audit trail design.

System-Level Audit Trails

System-level audit trails are generally used to monitor and optimize system performance but serve a security audit function as well. The system enforces certain aspects of security policy, such as access to the system itself. A system-level audit trail captures data such as login attempts (both successful and unsuccessful), devices used, and operating system functions performed. Other system-level functions may be of interest for auditing, such as system operation and network performance indicators.

Application-Level Audit Trails

Application-level audit trails are used to detect security violations in an application or to detect flaws in the application's interaction with the system. For critical applications, or those that deal with sensitive data, an application-level audit trail provides the desired level of detail to assess security threats and impacts. For example, for an e-mail application, an audit trail records sender and receiver, message size, and types of attachments. An audit trail for a database interaction using Structured

Query Language (SQL) queries records the user, type of transaction, and even individual tables, rows, columns, or data items accessed.

User-Level Audit Trails

A user-level audit trail traces the activity of an individual user over time. It is used to hold a user accountable for his or her actions. Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior.

A user-level audit trail records user interactions with the system, such as commands issued, identification and authentication attempts, and files and resources accessed. The audit trail also captures the user's use of applications.

Network-Level Audit Trails

Network-level audit trails encompass a wide variety of network activity. Enterprises use such audit trails to evaluate system performance and perform load balancing. These audit trails can also include security-related data, such as that generated by firewalls, virtual private network managers, and IPsec traffic.

Physical Access Audit Trails

Physical access audit trails are generated by equipment that controls physical access and are then transmitted to a central host for subsequent storage and analysis. Examples are card-key systems and alarm systems. The following are examples of the types of data of interest:

- Log the date and time the access was attempted or made as well as the gate or door through which the access was attempted or made, as well as the individual (or user ID) making the attempt to access the gate or door.
- Monitor and log invalid attempts by non-computer audit trails just as you would for computer system audit trails. Make sure management is aware that someone is attempting to gain access during unauthorized hours.
- Log information that also includes attempts to add, modify, or delete physical access privileges (for example, granting a new employee access to the building or granting transferred employees access to their new office—and, of course, deleting their old access, as applicable).
- As with system and application audit trails, implement auditing of non-computer functions to send messages to security personnel indicating valid or invalid attempts to gain access to controlled spaces. A guard or monitor may be desensitized if all access results in messages being sent to a screen. Therefore, it is best to highlight only exceptions, such as failed access attempts, to those monitoring access.

Where appropriate, the log data can include digital archives of video surveillance contemporaneous with a logged event.

Internal and External Audit

A sound auditing policy includes both internal security audits and external security audits. Internal audits are carried out by the organization itself, typically on a quarterly basis or after a significant security event. External audits are carried out by someone from outside, typically on annual basis.

internal security audit

An audit conducted by personnel responsible to the management of the organization being audited.

external security audit

An audit conducted by an organization independent of the one being audited.

The objectives of an internal security audit include the following:

- Identify security weaknesses
- Provide an opportunity to improve the information security management system
- Provide management with information about the status of security
- Deliver information about the status of security to management
- Review compliance of security systems with the information security policy of the organization
- Find and resolve noncompliance

The objectives of the external security include the following:

- Assess the process of the internal audit
- Determine the commonality and frequency of recurrence of various types of security violations
- Identify the common causes of various types of security violations
- Provide advisory and training inputs to tackle the neglect of procedures
- Review and update the policy

Security Audit Controls

A useful guide to developing a security audit program is the family of audit controls defined in SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. The controls are designed to be flexible and customizable and implemented as part of an organizationwide process to manage risk.

The audit and accountability family consists of 16 base controls. Some of the base controls include one or more control enhancements, which add functionality or specificity to a base control or increase the strength of a base control. The control enhancements are labeled with numbers in parentheses in the following list and table. In the following list some numbers associated with control enhancements are missing; these are withdrawn enhancements. The 16 base controls are:

- Audit and accountability policy and procedures: Defines the governance strategy for a security audit policy.
- Audit events: This control includes specifying the type of events to be audited. Additional guidance for this control includes the following: Specify the event types to be audited; Verify that the system can audit the selected event types; provide a rationale for why the auditable event types are deemed to be adequate to support after-the-fact investigations of security and privacy incidents; and coordinate the security audit function with other organizational entities requiring audit-related information.

- (3) Periodically review and update the set of events to be audited.
- Content of audit records: Deals with the content of audit records, including the following issues:
    - Specify the content of an audit record, such as what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
    - Provide centralized management and configuration of the content to be captured.
    - Limit the personally identifiable information contained in audit records.
- Audit storage capacity: Deals with allocating sufficient storage capacity to accommodate record retention requirements.
    - Periodically offload audit records onto a different system or media.
- Response to audit processing failures: Provides guidance on alerting specific personnel about an audit processing failure and what additional actions to take. The following control enhancements are covered:
    - Provide warning when allocated storage is exhausted.
    - Provide an alert to designated personnel or locations when specified audit failure events occur.
    - Enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity.
    - Invoke a specified full system shutdown, partial system shutdown, or degraded operational mode with limited mission/business functionality available in the event of specified audit processing failures.
- Audit review, analysis, and reporting: Deals with reviewing and analyzing security audit records at a specified frequency, with reports to specified individuals. Enhancement include:
    - Employ automated mechanisms to integrate audit review, analysis, and reporting.
    - Analyze and correlate audit records across different repositories to gain organizationwide situational awareness.
    - Provide and implement the capability to centrally review and analyze audit records from multiple components in the system.
    - Integrate analysis of audit records with other security analysis and monitoring efforts.
    - Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.
    - Specify permitted actions for system processes, roles, and/or users associated with the review, analysis, and reporting of audit records.
    - Require a distinct environment for the dedicated analysis of audit information related to privileged users.
    - Correlate information from nontechnical sources with audit information to enhance organizationwide situational awareness.
- Audit reduction and report generation: Deals with providing summary information from audit records that is meaningful to analysts. May also include:
    - Provide and implement the capability to process audit records for events of interest ased on specified criteria.
    - Provide and implement the capability to sort and search audit records for events of interest based on selected audit fields.
- Time stamps: Deals with recording time stamps from internal system clocks. Enhancements include:

    - Synchronize with an authoritative time source.
    - Identify a secondary authoritative time source to be used if the primary source is not available.
- Protection of audit information: Deals with providing technical or automated protection of audit information. Enhancements include:
    - For initial generation and backup of audit trails, use hardware-enforced, write-once media.
    - Store audit information in a repository separate from the audited system or system component.
    - Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
    - Authorize access to management of audit functionality to only selected privileged users.
    - For executing selected actions, require the approval of two authorized individuals.
    - Authorize read-only access to audit information to a selected subset of privileged users.
    - Store audit information on a component running a different operating system than the system or component being audited.
- Non-repudiation: Deals with protecting against an individual falsely denying having performed selected audit-related activities. Enhancements include:
    - Provide organizational personnel with the means to identify who produced specific information in the event of an information transfer.
    - Prevent the modification of information between production and review.
    - Maintain reviewer or releaser identity and credentials within the established chain of custody for all information reviewed or released.
    - Prevent the modification of information between review and transfer/release.
- Audit record retention: Provides guidance for developing a record retention policy.
    - Employ organization-defined measures to ensure that long-term audit records generated by the system can be retrieved.
- Audit generation: Provides guidance for defining an audit record generation capability for the auditable event types. Enhancements include:
    - Compile audit records from organization-defined system components into a systemwide audit trail that is time-correlated to within the organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.
    - Produce a systemwide (logical or physical) audit trail composed of audit records in a standardized format.
    - Extend or limit auditing, as necessary, to meet organizational requirements. Auditing that is limited to conserve system resources may be extended to address certain threat situations.
    - Audit query parameters within systems for data sets that contain personally identifiable information; this augments an organization's ability to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.
- Monitoring for information disclosure: Discusses monitoring open source information (for example, from social networking sites) for evidence of unauthorized disclosure of organizational information. Enhancements include:

    - Employ automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.
    - Review the open source information sites being monitored.
- Session audit: Deals with providing and implementing the capability for authorized users to select a user session to capture/record or view/hear. Enhancements include:
    - Initiate session audits automatically at system startup.
    - Provide and implement the capability for authorized users to capture, record, and log content related to a user session.
    - Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.
- Alternate audit capability: Deals with providing an alternate audit capability in the event of a failure in primary audit capability that implements organization-defined alternate audit functionality.
- Cross-organizational audit: When organizations use systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. This control provides for such a capability. Enhancements include:
    - Require that the identity of individuals be preserved in cross-organizational audit trails.
    - Provide cross-organizational audit information to organization-defined organizations based on organization-defined cross-organizational sharing agreements.

This set of controls provides comprehensive guidance for planning and implementing an effective security auditing function.

Table 18.1 lists the recommended set of minimum security controls, called a control baseline. Table 18.1 provides additional guidance for an organization in selecting controls based on risk assessment.

TABLE 18.1 Audit and Accountability Control Baseline

Control		Control Baselines		
		Low	Moderate	High
AU-1	Audit and accountability policy and procedures	AU-1	AU-1	AU-1
AU-2	Audit events	AU-2	AU-2(3)	AU-2(3)
AU-3	Content of audit records	AU-3	AU-3(1)	AU-3(1)(2)
AU-4	Audit storage capacity	AU-4	AU-4	AU-4
AU-5	Response to audit processing failures	AU-5	AU-5	AU-5(1)(2)
AU-6	Audit review, analysis, and reporting	AU-6	AU-6(1)(3)	AU-6 (1)(3)(5)(6)
AU-7	Audit reduction and report generation	—	AU-7(1)	AU-7(1)
AU-8	Time stamps	AU-8	AU-8(1)	AU-8(1)
AU-9	Protection of audit information	AU-9	AU-9(4)	AU-9 (2)(3)(4)
AU-10	Non-repudiation	—	—	AU-10
AU-11	Audit record retention	AU-11	AU-11	AU-11
AU-12	Audit generation	AU-12	AU-12	AU-12(1)(3)
AU-13	Monitoring for information disclosure	—	—	—
AU-14	Session audit	—	—	—
AU-15	Alternate audit capability	—	—	—
AU-16	Cross-organizational audit	—	—	—

7.3 Security Performance

Security performance is the measurable result of security controls applied to information systems and supporting information security programs. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) defines the security performance function as comprising three areas:

- Security monitoring and reporting: Consists of monitoring security performance regularly and reporting to specific audiences, such as executive management
- Information risk reporting: Consists of producing reports relating to information risk and presenting reporting to executive management on a regular basis
- Information security compliance monitoring: Consists of information security controls derived from regulatory and legal drivers and contracts, used to monitor security compliance

An essential element of security performance assessment is the selection of security performance metrics. This section looks first at the topic of security performance metrics and then treats the three areas previously listed.

Security Performance Measurement

Two terms are relevant to this discussion:

- Security performance: The measurable result of security controls applied to information systems and supporting information security programs.
- Security performance metric: A variable related to security performance to which a value is assigned as the result of measurement. Also called a security performance measure.

National Institute of Standards and Technology (NIST) IR 7564, Directions in Security Metrics Research, lists the following as the main broad uses of security metrics:

- Strategic support: Assessments of security properties can be used to aid in different kinds of decision making, such as program planning, resource allocation, and product and service selection.
- Quality assurance: Security metrics can be used during the software development life cycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying vulnerabilities that are likely to exist, and tracking and analyzing security flaws that are eventually discovered.
- Tactical oversight: Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (for example, policies, procedures, regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.

Yee's article "Security Metrics: An Introduction and Literature Review" [YEE17] states that a security metrics should do the following:

- Measure quantities that are meaningful for establishing the security posture of a computer system or of an organization
- Be reproducible
- Be objective and unbiased
- Be able to measure a progression toward a goal over time

Sources of Security Metrics

A security officer or a group responsible for developing a set of metrics for security performance assessment draws on several authoritative sets, some of which are described here.

Chapter 1, "Best Practices, Standards, and a Plan of Action," discusses the organization of COBIT 5 into 5 domains and 37 processes. Relevant for the discussion of this chapter is the Monitor, Evaluate, and Assess (MEA) domain, which deals with a company's strategy in assessing the needs of the company and whether the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. Three processes comprise this domain:

- Performance and conformance: Collect, validate, and evaluate business, IT, and process goals and metrics. Monitor to ensure that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.
- System of internal control: Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize, and maintain standards for internal control assessment and assurance activities.
- Compliance with external requirements: Evaluate whether IT processes and IT-supported business processes are compliant with laws, regulations, and contractual requirements. Obtain assurance that the requirements were identified and complied with and integrate IT compliance with overall enterprise compliance.

Table 18.2 lists the metrics defined for these three processes.

TABLE 18.2 Suggested Security Performance Metrics (COBIT 5 for Information Security)

Goal	Metrics
Performance and Conformance	
Information security performance is monitored on an ongoing basis	▪ Percentage of business processes that meet defined information security requirements
Information security and information risk practices conform to internal compliance requirements.	▪ Percentage of information security practices that satisfy internal compliance requirements
System of Internal Control	
Information security controls are deployed and operating effectively	▪ Percentage of processes that satisfy information security control requirements ▪ Percentage of controls in which information security control requirements are met
Monitoring processes for information security controls are in place and results are reported	▪ Percentage of information security controls appropriately monitored and results reported and reviewed
Compliance with External Requirements	
Information security and information risk practices conform to external compliance requirements	▪ Percentage of information security practices that satisfy external compliance requirements
Monitoring is conducted for new or revised external requirements with an impact on information security	▪ Number or percentage of projects initiated by information security to implement new external requirements

SP 800-55, Performance Measurement Guide for Information Security, lists a number of candidate metrics that organizations can tailor, expand, or use as models for developing other metrics (see Table 18.3). The recommended metrics focus on the SP 800-53 security controls. In essence, the metrics measure the effectiveness of the implementation of the security controls.

TABLE 18.3 Examples of Security Performance Metrics (NIST 800-55)

Area	Metric
Security budget	Percentage of the agency's information system budget devoted to information security
Vulnerability management	Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
Access control	Percentage of remote access points used to gain unauthorized access
Awareness and training	Percentage of information system security personnel that have received security training
Audit and accountability	Average frequency of audit records review and analysis for inappropriate activity
Certification, accreditation, and security assessments	Percentage of new systems that have completed certification and accreditation (C&A) prior to their implementation
Configuration management	Percentage approved and implemented configuration changes identified in the latest automated baseline configuration
Contingency planning	Percentage of information systems that have conducted annual contingency plan testing
Identification and authentication	Percentage of users with access to shared accounts
Incident response	Percentage of incidents reported within the required time frame, per applicable incident category
Maintenance	Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
Media protection	Percentage of media that passes sanitization procedures testing for FIPS 199 high-impact systems
Physical and environmental	Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems
Planning	Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior
Personnel security	Percentage of individuals screened before being granted access to organizational information and information systems
Risk assessment	Percentage of vulnerabilities remediated within organization-specified time frames
System and services acquisition	Percentage of system and service acquisition contracts that include security requirements and/or specifications
System and communication protection	Percentage of mobile computers and devices that perform all cryptographic operations using FIPS 140-2–validated cryptographic modules operating in approved modes of operation
System and information integrity	Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

There is one metric for each system control. For each metric, SP 800-55 provides detailed guidance in a number of categories. For example, for the maintenance metric, these are the category values:

- Goal: Strategic Goal: Accelerate the development and use of an electronic information infrastructure. Information Security Goal: Perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- Measure: Percentage (%) of system components that undergo maintenance in accordance with formal maintenance schedules.
- Measure Type: Effectiveness/Efficiency
- Formula: (Number of system components that undergo maintenance according to formal maintenance schedules/total number of system components) × 100.
- Target: This should be a high percentage defined by the organization.
- Implementation Evidence: (1) Does the system have a formal maintenance schedule? (2) How many components are contained within the system? (3) How many components underwent maintenance in accordance with the formal maintenance schedule?
- Frequency: Collection Frequency: Organization-defined (example: quarterly); Reporting Frequency: Organization-defined (example: annually)
- Responsible Parties: Information Owner: Organization-defined (example: System Owner); Information Collector: Organization-defined (for example, system administrator); Information Customer: Chief information officer (CIO), information system security officer (ISSO), senior agency information security officer (SAISO) (for example, chief information security officer [CISO])
- Data Source: Maintenance schedule, maintenance logs
- Reporting Format: Pie chart comparing the percentage of system components receiving maintenance in accordance with the formal maintenance schedule versus the percentage of system components not receiving maintenance in accordance with the formal maintenance schedule over the specified period

Chapter 1 discusses the critical security controls defined by the Center for Internet Security (CIS) (refer to Table 1.10). The CIS has also published a companion document that provides a number of security

metrics for each control [CIS15]. Each metric includes a set of three risk threshold values (lower, moderate, higher). The risk threshold values reflect the consensus of experienced practitioners. They are offered as a way for adopters of the controls to think about and choose metrics in the context of their own security improvement programs.

For example, Table 18.4 shows the metrics defined for the Maintenance, Monitoring, and Analysis of Audit Logs control.

TABLE 18.4 Metrics for the CIS Maintenance, Monitoring, and Analysis of Audit Logs Control

Metric	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard (by business unit)?	Less than 1%	1%–4%	5%–10%
What percentage of the organization's systems are not currently configured to centralize their logs to a central log management system (by business unit)?	Less than 1%	1%–4%	5%–10%
How many anomalies/events of interest have been discovered in the organization's logs recently (by business unit)?	—	—	—
If a system fails to log properly, how long does it take for an alert about the failure to be sent (time in minutes, by business unit)?	60 minutes	1 day	1 week
If a system fails to log properly, how long does it take for enterprise personnel to respond to the failure (time in minutes, by business unit)?	60 minutes	1 day	1 week

Information Security Metric Development Process

Figure 18.2, from SP 800-55, illustrates the process of developing information security metrics. It shows how this process takes place within a larger organizational context and demonstrates that information security metrics are used to progressively measure implementation, efficiency, effectiveness, and the business impact of information security activities within organizations or for specific systems.

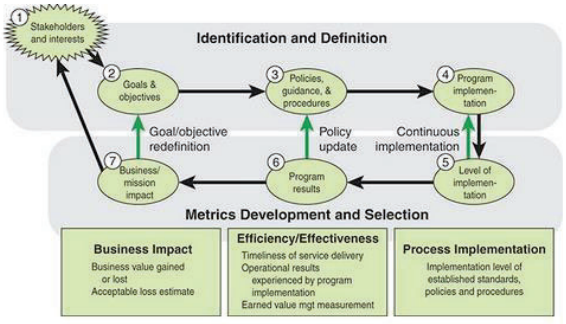


FIGURE 18.2 Information Security Metrics Development Process

The information security metric development process consists of two major activities:

1. Identifying and defining the current information security program
2. Developing and selecting specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls

The first four phases shown in Figure 18.2 summarize the information security program development process discussed earlier in this book. Based on inputs from stakeholders and other interests, security goals and objectives are developed. The goals and objectives lead to the development of security policies, which in turn guide security program implementation.

Phases 5, 6, and 7 in Figure 18.2 involve developing metrics that measure process implementation, effectiveness and efficiency, and mission impact. The organization selects metrics that measure performance, identify causes of unsatisfactory performance, and identify areas for improvement. The metrics also provide guidance for the security manager to facilitate consistent policy implementation, effect information security policy changes, and refine goals and objectives.

Figure 18.2 shows the manner in which the development of a set of metrics interacts with the system program development process. Payne's "A Guide to Security Metrics" [PAYN06] provides guidance on implementing a metrics program consisting of the following steps:

1. Define the metrics program goal(s) and objectives. For example, a goal could be expressed as "Provide metrics that clearly and simply communicate how efficiently and effectively our company is balancing security risks and preventive measures, so that investments in our security program can be appropriately sized and targeted to meet our overall security objectives."

The objectives could include the following:

- "To base the security metrics program on process improvement best practices within our company."
- "To leverage any relevant measurements currently being collected."
- "To communicate metrics in formats custom-tailored to various audiences."
- "To involve stakeholders in determining what metrics to produce."

2. Decide which metrics to generate. Security officials can use the guidance provided by COBIT 5, NIST, and the CIS, as described earlier.
3. Develop strategies for generating the metrics. These strategies should specify the source of the data, the frequency of data collection, and who is responsible for raw data accuracy, data compilation into measurements, and generation of the metric.
4. Establish benchmarks and targets. Benchmarking is the process of comparing one's own performance and practices against peers within the industry. An organization should compare the metric values it is achieving against industry norms to determine areas where best practices suggests that improvement in the security program is needed. For example, BitSight is one company that provides this service, enabling an organization to compare its security posture to others in their industry.
    - good information on Internet security threats, vulnerabilities, and attack statistics.
5. Determine how the metrics will be reported. The metrics program planner should determine the context, format, frequency, distribution method, and responsibility for reporting metrics so that the end product can be visualized early on by those who will be involved in producing the metrics and those who will be using them for decision making.
6. Create an action plan and act on it. The plan should detail the steps that need to be taken to launch the security metrics program, along with time tables and assignments.
7. Establish a formal program review/refinement cycle. The security metrics plan should include formal, regular review of the program.

BitSight https://www.bitsighttech.com/

Security Monitoring and Reporting

The objective of security monitoring and reporting is to provide each audience with a relevant, accurate, comprehensive, and coherent assessment of information security performance.

COBIT 5 provides specific guidance on security monitoring and reporting based on the three processes defined earlier in this section: performance and conformance, system of internal control, and compliance with external requirements. This subsection deals with the first two processes; the last subsection of Section 18.2 discusses the final process.

For the performance and conformance process, COBIT 5 defines the following steps:

1. Establish a monitoring approach. Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope, and method for measuring business

solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.

2. Set performance and conformance targets. Work with stakeholders to define, periodically review, update, and approve performance and conformance targets within the performance measurement system.
3. Collect and process performance and conformance data. Collect and process timely and accurate data aligned with enterprise approaches.
4. Analyze and report performance. Periodically review and report performance against targets, using a method that provides a succinct all-around view of IT performance and fits within the enterprise monitoring system.
5. Ensure the implementation of corrective actions. Assist stakeholders in identifying, initiating, and tracking corrective actions to address anomalies.

For the system of internal control process, COBIT 5 defines the following steps:

1. Monitor internal controls. Continuously monitor, benchmark, and improve the IT control environment and control framework to meet organizational objectives.
2. Review business process controls effectiveness. Review the operation of controls, including a review of monitoring and test evidence, to ensure that controls in business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous control monitoring, independent assessments, command and control centers, and network operations centers.
3. Perform control self-assessments. Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies, and contracts.
4. Identify and report control deficiencies. Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
5. Ensure that assurance providers are independent and qualified. Ensure that the entities performing assurance are independent from the function, groups, or organizations in scope.
6. Plan assurance initiatives. Plan assurance initiatives based on enterprise objectives and strategic priorities, inherent risk, resource constraints, and sufficient knowledge of the enterprise.
7. Scope assurance initiatives. Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
8. Execute assurance initiatives. Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance, and internal control system residual risk.

SP 800-55 provides a view of implementing the monitoring and reporting function based on the security performance metrics, shown in Figure 18.3.

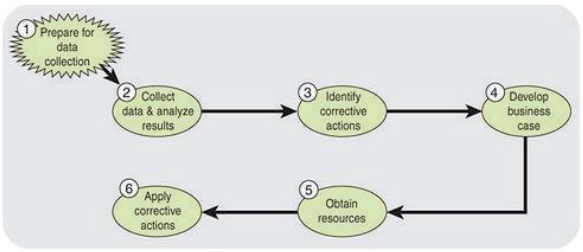


FIGURE 18.3 Information Security Metrics Program Implementation Process

This process proceeds in six steps:

1. Prepare for data collection. In essence, this step involves the metrics development process shown in Figure 18.2.
2. Collect data and analyze results. The analysis should identify gaps between actual and desired performance, identify reasons for undesired results, and identify areas that require improvement.
3. Identify corrective actions. Based on step 2, determine appropriate corrective actions and prioritize them based on risk mitigation goals.
4. Develop business case. This involves developing a cost model for each corrective action and making a business case for taking that action.
5. Obtain resources. Obtain the needed budget and resource allocation.
6. Apply corrective actions. These actions may include adjustments in management, technical, and operational areas.

Information Risk Reporting

Risk reporting is a process that produces information systems reports that address threats, capabilities, vulnerabilities, and inherent risk changes. Risk reporting describes any information security events that the institution faces and the effectiveness of management's response to and resilience in the face of those events. An organization needs to have a method of disseminating those reports to appropriate members of management. The contents of the reports should prompt action, if necessary, in a timely manner to maintain appropriate levels of risk.

One objective of information risk reporting is to provide executive management with an accurate, comprehensive, and coherent view of information risk across the organization. The second objective is to obtain approval from executive management for risk treatment options.

The Information Systems Audit and Control Association (ISACA) has developed useful guidance on information risk reporting, based on COBIT 5 [ISAC09]. The guidance makes use of two key concepts in COBIT 5:

- Process: A collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs, and produces outputs (for example, products, services). Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.
- Activity: The main action taken to operate the process, which provides guidance to achieve management practices for successful governance and management of enterprise IT. Activities:
  - ✓ Describe a set of necessary and sufficient action-oriented implementation steps to achieve a governance practice or management practice
  - ✓ Consider the inputs and outputs of the process
  - ✓ Are based on generally accepted standards and good practices
  - ✓ Support establishment of clear roles and responsibilities
  - ✓ Are nonprescriptive and need to be adapted and developed into specific procedures appropriate for the enterprise

Using these concepts, ISACA outlines the goals and metrics for processes and activities that contribute to the risk reporting function, as well as the risk reporting function itself (see Table 18.5).

TABLE 18.5 Risk Reporting Goals and Metrics

Category	Goals	Metrics
Process	▪ Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response	▪ Percentage of risk issues inappropriately distributed too high or too low in the enterprise hierarchy ▪ Number of IT-related events with business impact not earlier reported as in IT risk ▪ Percentage of critical assets/resources covered by monitoring activities ▪ Timeliness of reports on IT exposures relative to the next expected threat or loss event. ▪ Potential business impact of exposures discovered by assurance groups
Activity	▪ Communicate IT risk analysis results ▪ Report IT risk management activities and state of compliance ▪ Interpret independent IT assessment findings	▪ Percentage of risk analysis reports accepted on initial delivery ▪ Percentage of on-time risk management reports ▪ Frequency of risk management activity reporting ▪ Number of IT-related events with business impact not previously reported as an IT risk. ▪ Number of IT risk issues identified by outside parties yet to be interpreted and mapped into the risk profile
Risk reporting	▪ Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities	▪ The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

Information Security Compliance Monitoring

The objective of information security compliance monitoring is to ensure that information security controls are consistently prioritized and addressed according to information security obligations associated with legislation, regulations, contracts, industry standards, or organizational policies.

COBIT 5 Guidelines

COBIT 5 provides specific guidance on security monitoring and reporting for compliance with external requirements.

For the process of ensuring compliance with external requirements, COBIT 5 defines the following steps:

1. Identify external compliance requirements. On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that the organization must comply with from an IT perspective.
2. Optimize response to external requirements. Review and adjust policies, principles, standards, procedures, and methodologies to ensure that legal, regulatory, and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and good practice guidance for adoption and adaptation.
3. Confirm external compliance. Confirm compliance of policies, principles, standards, procedures, and methodologies with legal, regulatory, and contractual requirements.
4. Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures, and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Compliance Strategy

The following steps constitute a general approach to information security compliance monitoring:

1. Identify key stakeholders and/or partners across the organization who regularly deal with institutional compliance issues (for example, legal, risk management, privacy, audit).
2. Identify key standards, regulations, contractual commitments, and other areas that address specific requirements for security and privacy.
3. Perform a high-level gap analysis of each compliance requirement that is applicable to determine where progress needs to be made.
4. Develop a prioritized action plan that will help organize remedial efforts.
5. Develop a compliance policy, standard, roles and responsibilities, and/or procedures in collaboration with other key stakeholders.

7.4 Security Monitoring and Improvement Best Practices

The SGP breaks down the best practices in the security monitoring and improvement category into two areas and eight topics and provides detailed checklists for each topic. The areas and topics are as follows:

- Security audit: This area provides guidance for conducting thorough, independent, and regular audits of the security status of target environments (critical business environments, processes, applications, and supporting systems/networks).
- Security audit management: The objective of this topic is to ensure that security controls have been implemented effectively and that risk is being adequately managed and to provide the owners of target environments and executive management with an independent assessment of their security status.
    - ✓ Security audit process—planning: Provides guidance on a methodology for security audits.
    - ✓ Security audit process—fieldwork: Provides a checklist of actions related to collecting relevant background material, performing security audit tests, and recording the results of the tests.
    - ✓ Security audit process—reporting: Provides a checklist of items that should be in the security audit report, as well as guidance on the reporting process.
    - ✓ Security audit process—monitoring: Provides a checklist of actions to ensure the risks identified during security audits are treated effectively, compliance requirements are being met, and agreed security controls are being implemented within agreed time scales.
- Security performance: This area provides guidance for monitoring information risks; compliance with the security-related elements of legal, regulatory, and contractual requirements; and the overall information security condition of the organization on a regular basis, reporting the results to specific audiences, such as executive management.
- Security monitoring and performance: The objective of this topic is to ensure that there is a reporting function that provides selected audiences with a relevant, accurate, comprehensive, and coherent assessment of information security performance.

- Information risk reporting: The objective of this topic is to ensure that there is a reporting function that provides executive management with an accurate, comprehensive, and coherent view of information risk across the organization.
- Information security compliance monitoring: This topic provides guidelines for a security management process that should be established, which comprises information security controls derived from regulatory and legal drivers and contracts.

7.5 Review Questions / Case Studies / Projects

1. Briefly define the terms security audit and security audit trail.
2. What are the key elements of the X.816 security audit model's relationship with security alarms?
3. What are some of the auditable items suggested in the X.816 model of security audits and alarms?
4. What are the four different types of audit trails?
5. What are the key objectives of an external security audit?
6. How does the SGP define the security performance function?
7. NIST IR 7564 defines three broad uses of security metrics. Enumerate them.
8. What are the three key processes for the COBIT 5 Monitor, Evaluate, and Assess domain?
9. What guidelines does COBIT 5 define for the performance and conformance process?
10. Describe the monitoring and reporting function, as per SP 800-55.
11. ISACA's guidance on information risk reporting is based on which two concepts of COBIT 5?
12. What are the generic steps for security compliance monitoring?

References and Standards

References

The references listed here is a compilation of the references cited within the chapters.

ARMY10: Department of the Army. Physical Security. Field Manual FM 3-99.32, August 2010.

ASHO17: Ashok, I. "Hackers spied and stole from millions by exploiting Word flaw as Microsoft probed bug for months." International Business Times, April 27, 2017.

BALA15: Balasubramanian, V. Conquering the Operational Challenges of Network Change & Configuration Management through Automation. Zoho Corp. White Paper, 2015. https://www.manageengine.com/network-configuration-manager/network-configuration-management-overview.html

BANK14: Banks, E. "Automating Network Device Configuration." Network World, July 2014.

BAYL13: Baylor, K. "Top 8 DRM Best Practices." NSS Labs Research Report. 2013. https://www.nsslabs.com/linkservid/A59EC3DC-5056-9046-9336E175181E14C9/

BEHL12: Behl, A. Securing Cisco IP Telephony Networks. Indianapolis, IN: Cisco Press, 2012.

BELL94: Bellovin, S., and Cheswick, W. "Network Firewalls." IEEE Communications Magazine, September 1994.

BEUC09: Buecker, A., Andreas, P., & Paisley, S., Understanding IT Perimeter Security. IBM red paper REDP-4397-00, November 2009.

BONN12: Bonneau, J. "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords." IEEE Symposium on Security and Privacy, 2012.

BOSW14: Bosworth, S.; Kabay, M.; and Whyne, E., Editors. Computer Security Handbook. New York: Wiley, 2014.

BSA03: Business Software Alliance. Information Security Governance: Toward a Framework for Action. 2003. https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf

BUEC09: Buecker, A.; Andreas, P.; and Paisley, S. Understanding IT Perimeter Security. IBM Redpaper REDP-4397-00, November 2009.

BURK12: Burkett, J. "Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA." Information Security Journal, February 15, 2012

BURN15: Burnett, M. "Today I Am Releasing Ten Million Passwords." February 9, 2015. https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

CARB17: Carbon Black. Beyond the Hype: Security Experts Weigh in on Artificial Intelligence, Machine Learning and Non-malware Attacks. March 2017 https://www.carbonblack.com/wp-content/uploads/2017/03/Carbon_Black_Research_Report_NonMalwareAttacks_ArtificialIntelligence_MachineLearning_BeyondtheHype.pdf

CIS15: Center for Internet Security. A Measurement Companion to the CIS Critical Security Controls. October 2015. https://www.cisecurity.org/white-papers/a-measurement-companion-to-the-cis-critical-controls/

CIS18: Center for Internet Security. The CIS Critical Security Controls for Effective Cyber Defense version 7. 2018. https://www.cisecurity.org/controls/

CSCC15: Cloud Standards Customer Council. Practical Guide to Cloud Service Agreements. April 2015. http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

CSCC16: Cloud Standards Customer Council. Public Cloud Service Agreements: What to Expect and What to Negotiate. August 2016. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf

CEB15: CEB/Gartner. Information Security Strategy on a Page. 2015. https://www.cebglobal.com/information-technology/it-risk/information-security-strategic-plan.html

CGTF04: Corporate Governance Task Force. Information Security Governance: A Call to Action. U.S. Department of Homeland Security, 2004.

CHES17: Chesla, A. "Restoring Machine Learning's Good Name in Cybersecurity." Forbes Community Voice, July 25, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/07/25/restoring-machine-learnings-good-name-in-cybersecurity/#18be0e1168f4

CICE14: Cicerone, R., and Nurse, P., Editors. Cybersecurity Dilemmas: Technology, Policy, and Incentives. National Academy of Sciences, 2014.

CISC07: Cisco Systems. Cisco Advanced Services Network Management Systems Architectural Leading Practice. White Paper C07-400447-00, September 2007. https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb4c.pdf

CIS09: Center for Internet Security. Security Benchmark for Multi-Function Devices. April 2009. https://www.cisecurity.org

CIS18: Center for Internet Security. CIS Controls Version 7. 2018. https://www.cisecurity.org

CLAR14: Clark, D.; Berson, T.'; and Lin, H., Editors. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. National Research Council, 2014.

CLEE09: van Cleeff, A.; Pieters, W.; and Wieringa, R. "Security Implications of Virtualization: A Literature Study." International Conference on Computational Science and Engineering, IEEE, 2009.

CMU03: Carnegie-Mellon University. Handbook for Computer Security Incident Response Teams (CSIRTs). CMU Handbook CMU/SEI-2004-HB-002, 2003.

CNSS10: Committee on National Security Systems. National Information Assurance (IA) Glossary. April 2010.

COCS14: Council on CyberSecurity. Cybersecurity Workforce Handbook: A Practical Guide to Managing Your Workforce. 2014. http://pellcenter.org/tag/council-on-cybersecurity/

COGE16: Cogent Communications, Inc. Network Services Service Level Agreement Global. September 2016. http://www.cogentco.com/files/docs/network/performance/global_sla.pdf

CREN17: Crenshaw, A. "Hacking Network Printers." Retrieved June 26, 2017 from http://www.irongeek.com/i.php?page=security/networkprinterhacking

DHS10: U.S. Department of Homeland Security and the U.K. Centre for the Protection of National Infrastructure. Cyber Security Assessments of Industrial Control Systems. November 2010.

DHS11: U.S. Department of Homeland Security. Catalog of Control Systems Security: Recommendations for Standards Developers. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, April 2011.

DHS15: U.S. Department of Homeland Security. Seven Steps to Effectively Defend Industrial Control Systems. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, December 2015.

DHS16: U.S. Department of Homeland Security. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Report, September 2016.
DHS17: U.S. Department of Homeland Security. Study on Mobile Device Security. DHS Report, April 2017.

EAPA17: The EA Pad. "Basic Elements of Federal Enterprise Architecture." https://eapad.dk/gov/us/common-approach/basic-elements-of-federal-enterprise-architecture/retrieved April 15, 2017.

ENGE14: Engel, G. "Deconstructing the Cyber Kill Chain." DarkReading, November 18, 2014. http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

ENIS07: European Union Agency for Network and Information Security. Information Security Awareness Initiatives: Current Practice and the Measurement of Success. July 2008. https://www.enisa.europa.eu

ENIS08: European Union Agency for Network and Information Security. The New Users' Guide: How to Raise Information Security Awareness. July 2008 https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

ENIS10: European Union Agency for Network and Information Security. ENISA IT Business Continuity Management: An Approach for Small and Medium Sized Organizations. January 2010. https://www.enisa.europa.eu/publications/business-continuity-for-smes/at_download/fullReport

ENIS14: European Union Agency for Network and Information Security. Algorithms, Key Size and Parameters—2014. November 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

ENIS16: European Union Agency for Network and Information Security. ENISA Threat Taxonomy—A Tool for Structuring Threat Information. January 2016. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

ENIS18: European Union Agency for Network and Information Security. ENISA Threat Landscape Report 2017. January 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

EO13: Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." Federal Register, February 19, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

FEMA09: Federal Emergency Management Agency. Continuity Guidance for Non-Federal Entities (States, Territories, Tribal and Local Government Jurisdictions, and Private Sector Organizations). Continuity Guidance Circular 1 (CGC 1), January 21, 2009.

FFIE02: Federal Financial Institutions Examination Council. Information Security. December 2002.

FFIE15: Federal Financial Institutions Examination Council. Business Continuity Planning. February 2015.

FIRS15: First.org, Inc. Common Vulnerability Scoring System v3.0: Specification Document. 2015.

GADS06: Gadsden, R. MUSC Information Security Guidelines: Risk Management. Medical University of South Carolina, 2006. https://mainweb-v.musc.edu/security/guidelines/

GAO04: Government Accountability Office. Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity. GAO-04-394G, March 2004.

GAO12: United States Government Accountability Office. Portfolio Management Approach Needed to Improve Major Acquisition Outcomes. GAO-12-918, September 2012.

GARR10: Garretson, C. "Pulling the Plug on Old Hardware: Life-Cycle Management Explained." ComputerWorld, April 22, 2010.

GOBL02: Goble, G.; Fields, H.; and Cocchiara, R. Resilient Infrastructure: Improving Your Business Resilience. IBM Global Service White Paper. September 2002.

GOOD12: Goodin, D. "Why Passwords Have Never Been Weaker—and Crackers Have Never Been Stronger." Ars Technica, August 20, 2012.

GOUL15: Gould, L. "Introducing Application Lifecycle Management." Automotive Design and Production Magazine, November 2015.

GRAH12: Graham-Rowe, D. "Ageing Eyes Hinder Biometric Scans." Nature, May 2, 2012.

HABI17: Habib, H., et al. "Password Creation in the Presence of Blacklists." 2017 Workshop on Usable Security (USEC '17), 2017.

HAYD08a: Haydamack, C. "Strategic Planning Processes for Information Technology." BPTrends, September 2008

HAYD08b: Haydamack, C., and Sarah Johnson. Aligning IT with Business Goals through Strategic Planning. Intel Information Technology White Paper, December 2008.

HEIS14a: Higher Education Information Security Council. "Records Retention and Disposition Toolkit." Information Security Guide, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Records+Retention+and+Disposition+Toolkit

HEIS14b: Higher Education Information Security Council. "Cloud Computing Security." Information Security Guide, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Cloud+Computing+Security

HEIS14c: Higher Education Information Security Council. "Identity and Access Management." Information Security Guide, 2014. https://spaces.internet2.edu/display/2014infosecurityguide/Identity+and+Access+Management

HERL12: Herley, C., and Oorschot, P. "A Research Agenda Acknowledging the Persistence of Passwords." IEEE Security&Privacy, January/February 2012.

HERN06: Hernan, S.; Lambert, S.; Ostwald, T.; and Shostack, A. "Uncover Security Design Flaws Using The STRIDE Approach." MSDN Magazine, November 2006.

HIRT15: Hirt, R. "Review of Enterprise Security Risk Management." Slideshare, 2015. https://www.slideshare.net/randhirt/review-of-enterprise-security-risk-management

HUTT07: Hutton, N. "Preparing for Security Event Management." 360is Blog, February 28, 2017. http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf

IAIT12: The International Association of Information Technology Asset Managers. What is IT Asset Management? White Paper, 2012.

IFIT09: The International Foundation for Information Technology. System Development Management. 2009 https://www.if4it.com/SYNTHESIZED/DISCIPLINES/System_Development_Management_Home_Page.html

IBM14: IBM. "IBM Predictive Maintenance and Quality (Version 2.0)." IBM Redbooks Solution Guide, 2014.

INFO14: INFOSEC Institute. Information Security Policies. April 16, 2014. http://resources.infosecinstitute.com/information-security-policies/

ISAC08: ISACA. Defining Information Security Management Position Requirements: Guidance for Executives and Managers. 2008. www.isaca.org

ISAC09: ISACA. The Risk IT Framework. 2009. www.isaca.org

ISAC10: ISACA. Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives. 2008. www.isaca.org

ISAC11: ISACA. Creating a Culture of Security. 2011. www.isaca.org

ISAC13: ISACA. Responding to Targeted Cyberattacks. 2008. www.isaca.org

ITGI06: IT Governance Institute. Information Security Governance Guidance for Boards of Directors and Executive Management. 2006. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

ITUT12: ITU-T. Focus Group on Cloud Computing Technical Report Part 5: Cloud Security. FG Cloud TR, February 2012.

ITUT15: ITU-T. Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of existing ITU-T Recommendations for Secure Telecommunications. September 2015.

JOHN09: Johnston, A., and Hale, R. “Improved Security through Information Security Governance.” Communications of the ACM, January 2009.

JUDY14: Judy, H., et al. “Privacy in Cyberspace.” In [BOSW14].

JUER13: Juergens, M.; Donohue, T.; and Smith, C. “End-User Computing: Solving the Problem.” CompAct, April 2013. https://www.soa.org/News-and-Publications/Newsletters/Compact/2013/april/End-User-Computing--Solving-the-Problem.aspx
JUIZ15: Juiz, C., and Toomey, M. “To Govern IT, or not to Govern IT?” Communications of the ACM, February 2015.

KABA14: Kabay, M., and Robertson, B. “Employment Practices and Policies.” In [BOSW14].

KEIZ17: Keizer, G. “Experts Contend Microsoft Canceled Feb. Updates to Patch NSA Exploits.” ComputerWorld, April 18, 2017.

KELL12: Kelley, P., et al. “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms.” IEEE Symposium on Security and Privacy, 2012

KENN03: Kennedy, S. “Best Practices for Wireless Network Security.” ComputerWorld, November 23, 2003.

KINA16: Kinast, K. “10 key facts businesses need to note about the GDPR.” European Identity & Cloud Conference, 2016.

KOMA11: Komanduri, S. “Of Passwords and People: Measuring the Effect of Password-Composition Policies.” CHI Conference on Human Factors in Computing Systems, 2011.

KOWA12: Kowall, J., and Cappelli, W. Magic Quadrant for Application Performance Monitoring. Gartner Report, 2013. https://www.gartner.com/doc/2125315/magic-quadrant-application-performance-monitoring

LAMB06: Lambo, T. “ISO/IEC 27001: The Future of Infosec Certification.” ISSA Journal, November 2006.

MAAW10: Messaging Anti-Abuse Working Group. Overview of DNS Security - Port 53 Protection. MAAWG Paper, June 2010. https://www.m3aawg.org

MAZU13: Mazurek, M., et al. “Measuring Password Guessability for an Entire University.” Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, November 2013.

MCFA83: McFarlan, F. “The Information Archipelago—Plotting a Course.” Harvard Business Review, January 1983.

MICR15: Microsoft. Enterprise DevOps. Microsoft White Paper, 2015.

MILL17: Millet, L.; Fischhoff, B.; and Weinberger, P., Editors. Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. National Academies of Sciences, Engineering, and Medicine, 2017.

MINI14: Minick, E.; Rezabek, J.; and Ring, C. Application Release and Deployment for Dummies. Hoboken, NJ: Wiley, 2014.

MOGU07: Mogull, R. Understanding and Selecting a Data Loss Prevention Solution. SANS Institute White Paper, December 3, 2007. https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf

MOOR06: Moore, D., et al. “Inferring Internet Denial-of-Service Activity.” ACM Transactions on Computer Systems, May, 2006.

MOUL11: Moulds, R. Key Management for Dummies. Hoboken, NJ: Wiley, 2011.

MYER13: Myers, L. “The practicality of the Cyber Kill Chain approach to security.” CSO, October 4, 2013. https://www.cio.com/article/2381947/security0/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

NAYL09: Naylor, J. Acceptable Use Policies—Why, What, and How. MessageLabs White Paper, 2009. http://esafety.ccceducation.org/upload/file/Policy/AUP%20Legal%20advice.pdf

NCEM12: National Emergency Crisis and Disasters Management Authority. Business Continuity Management Standard and Guide. United Arab Emirates Supreme Council for National Security Standard AE/HSC/NCEMA 7000, 2012. https://www.ncema.gov.ae/content/documents/BCM%20English%20NCEMA_29_8_2013.pdf

NILE15: Niles, S. Physical Security in Mission Critical Facilities. White Paper 82. Schneider Electric. March 2015. http://it-resource.schneider-electric.com/h/i/55734850-wp-82-physical-security-in-mission-critical-facilities

NIST15: NIST. Measuring Strength of Authentication. December 16, 2015. https://www.nist.gov/sites/default/files/nstic-strength-authentication-discussion-draft.pdf

NIST17: NIST. Strength of Function for Authenticators – Biometrics (SOFA-B): Discussion Draft Open for Comments. November 14, 2017. https://pages.nist.gov/SOFA/SOFA.html

NIST18: NIST. Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NSTC11: National Science and Technology Council. The National Biometrics Challenge. September 2011.

OECH03: Oechslin, P. “Making a Faster Cryptanalytic Time-Memory Trade-Off.” Proceedings, Crypto 03, 2003.

OHKI09: Ohki, E., et al. “Information Security Governance Framework.” First ACM Workshop on Information Security Governance (WISG), November 2009.

OMB10: Office of Management and Budget; NIST; and Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile. 2010.

OMB13: Office of Management and Budget, and Federal Chief Information Officers Council. Federal Enterprise Architecture Framework. 2013.

OPEN15: Openwall.com. John the Ripper Password Cracker. http://www.openwall.com/john/doc/

OWAS17: The OWASP Foundation. OWASP Top 10 2017: The Ten Most Critical Web Application Security Risks. 2017 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

PAYN06: Payne, S. A Guide to Security Metrics. SANS Institute White Paper. June 19, 2006. https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

PETE12: Peters, C., and Schuman, B. Achieving Intel’s Strategic Goals with IT. Intel Information Technology White Paper, February 2012.

POLL12: Poller, A., et al., “Electronic Identity Cards for User Authentication—Promise and Practice.” IEEE Security & Privacy, January/February 2012.

RATH01: Ratha, N.; Connell, J.; and Bolle, R. “Enhancing security and privacy in biometrics-based authentication systems.” IBM Systems Journal, Vol 30, No 3, 2001.

RITC13: Ritchie, S. “Security Risk Management.” ISACA document, August 20, 2013. http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Security%20Risk%20Management.pdf

ROE10: Roe, D. “6 Ways Document Management and Records Management Differ.” CMS Wire, January 25, 2010.

ROY15: Roy, A., et al. “Secure the Cloud: From the Perspective of a Service-Oriented Organization.” ACM Computing Surveys, February 2015.

RUBE14: Rubenking, N. “Trustwave Global Security Report Is Bursting with Valuable Data.” PCMag, May 22, 2014.

SADO03: Sadowsky, G. et al. Information Technology Security Handbook. Washington, DC: The World Bank, 2003 http://www.infodev.org/articles/information-technology-security-handbook

SCHN14: Schneier, B. “The Internet of Things is Wildly Insecure—and Often Unpatchable.” Wired, January 6, 2014.

SCOT07: Scott, C. “Auditing and Securing Multifunction Devices.” SANS Institute, January 25, 2007.

SESS07: Sessions, R. “A Comparison of the Top Four Enterprise-Architecture Methodologies.” Microsoft Developer Network, May 2007. http://www3.cis.gsu.edu/dtruex/courses/CIS8090/2013Articles/A%20Comparison%20of%20the%20Top%20Four%20Enterprise-Architecture%20Methodologies.html

SGM17: Strategic Management Group. Strategic Planning Basics. http://www.strategymanage.com/strategic-planning-basics/retrieved April 6, 2017.

SHAR15: Sharma, S., and Coyne. B. DevOps for Dummies. Hoboken, NJ: Wiley, 2015.

SHER09: Sherwood, J.; Clark, A.; and Lynas, D. Enterprise Security Architecture. SABSA White Paper, 2009. http://www.sabsa.org

SHOR10: Shore, M., and Deng, X. "Architecting Survivable Networks using SABSA." 6th International Conference on Wireless Communications Networking and Mobile Computing, 2010.
SOLO06: Solove, D. A Taxonomy of Privacy. GWU Law School Public Law Research Paper No. 129, 2006. http://scholarship.law.gwu.edu/faculty_publications/921/

SPRA95: Sprague, R. "Electronic Document Management: Challenges and Opportunities for Information Systems Managers." MIS Quarterly, March 1995.

STAL16: Stallings, W. "Comprehensive Internet Email Security." Internet Protocol Journal, November 2016. Available at http://williamstallings.com/Papers/

STAL17: Stallings, W. Cryptography and Network Security: Principles and Practice, Seventh Edition. Upper Saddle River, NJ: Pearson, 2017.

STAL18: Stallings, W., and Brown, L. Computer Security: Principles and Practice. Englewood Cliffs, NJ: 2018.

TIMM10: Timmer, J., "32 Million Passwords Show Most Users Careless About Security." Ars Technica, January 21, 2010.

TOG11: The Open Group. The Open Group Architecture Framework (TOGAF). 2011. http://www.opengroup.org/subjectareas/enterprise/togaf

VERA17: Veracode. State of Software Security 2017. 2017 https://info.veracode.com/report-state-of-software-security.html

VERI17: Verizon. 2017 Data Breach Investigations Report. 2017. http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

WAG15: Western Australian Government. Business Continuity Management Guidelines. June 2015. https://www.icwa.wa.gov.au/__data/assets/pdf_file/0010/6112/Business-Continuity-Management-Guidelines.pdf

WAGN00: Wagner, D., & Goldberg, I., "Proofs of Security for the UNIX Password Hashing Algorithm." Proceedings, ASIACRYPT '00, 2000.

WASC10: Web Application Security Consortium. WASC Threat Classification. January 2010. http://www.webappsec.org/

WEIR09: Weir, M., et al., "Password Cracking Using Probabilistic Context-Free Grammars." IEEE Symposium on Security and Privacy, 2009.

WEIR10: Weir, M., et al. "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords." Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010.

WILD13: Wilding, R. "Classification of the Sources of Supply Chain Risk and Vulnerability." Richard Wilding Blog, August 2013. http://www.richardwilding.info/blog/the-sources-of-supply-chain-risk

YEE17: Yee, G. "Security Metrics: An Introduction and Literature Review." Computer and Information Security Handbook. Vacca, J., ed. Cambridge MA: Elsevier. 2017.

ZHAN10: Zhang, Y., Monrose, F., & Reiter, M., "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis." ACM Conference on Computer and Communications Security, 2010.

ZIA15: Zia, T. "Organisations Capability and Aptitude towards IT Security Governance." 2015 5th International Conference on IT Convergence and Security (ICITCS), August 2015.

ZIND17: Zindel, A. "IAM Best Practices to Reduce Your Attack Surface." Centrify Blog, August 30, 2017. https://blog.centrify.com/reduce-attack-surface-iam/

NIST Documents

FIPS-140-2: Security Requirements for Cryptographic

Modules, May 2001 FIPS-140-2A: Approved Security

Functions for FIPS PUB 140-2, January 2018 FIPS-186: Digital

Signature Standard, July 2013

FIPS-199: Standards for Security Categorization of Federal Information and Information

Systems, February 2004 FIPS 200: Minimum Security Requirements for Federal Information

and Information Systems, March 2006

IR 7359: Information Security Guide for Government

Executives, January 2007 IR 7564: Directions in Security

Metrics Research, April 2009

IR 7621: Small Business Information Security: The Fundamentals, November 2016

IR 7622: Notional Supply Chain Risk Management Practices for Federal Information

Systems, October 2012 IR 7874: Guidelines for Access Control System Evaluation

Metrics, September 2012

IR 7946: CVSS Implementation Guidance, April 2014

IR 7956: Cryptographic Key Management Issues & Challenges in Cloud

Services, September 2013 IR 8023: Risk Management for Replication Devices,

February 2015

IR 8112: Attribute Metadata, August 2016

IR 8144: Assessing Threats to Mobile Devices & Infrastructure, September 2016

IR 8062: An Introduction to Privacy Engineering and Risk Management in Federal

Systems, January 2017 SP 800-12: Introduction to Information Security, January

2017

SP 800-16: A Role-Based Model for Federal Information Technology/Cybersecurity

Training, March 2014 SP 800-18: Guide for Developing Security Plans for Federal

Information Systems, February 2006

SP 800-27: Engineering Principles for Information Technology Security (A Baseline for

Achieving Security), June 2004 SP 800-30: Guide for Conducting Risk Assessments,

September 2012

SP 800-32: Introduction to Public Key Technology and the Federal PKI

Infrastructure, February 2001 SP 800-34: Contingency Planning Guide for

Federal Information Systems, May 2010

SP 800-37: Risk Management Framework for Information Systems and

Organizations, September 2017 SP 800-39: Managing Information Security Risk,

March 2011

SP 800-40: Guide to Enterprise Patch Management

Technologies, July 2013 SP 800-41: Guidelines on Firewalls

and Firewall Policy, September 2009

SP 800-45: Guidelines on Electronic Mail Security, February 2007
SP 800-50: Building an Information Technology Security Awareness and Training

Program, October 2003 SP 800-53: Security and Privacy Controls for Federal

Information Systems and Organizations, August 2017

SP 800-53A: Assessing Security and Privacy Controls in Federal Information Systems and

Organizations, December 2014 SP 800-55: Performance Measurement Guide for Information

Security, July 2008

SP 800-57: Recommendation for Key Management—Part 1: General, January 2016

Recommendation for Key Management—Part 2: Best Practices for Key Management

Organization, August 2005 Recommendation for Key Management—Part 3: Application-

Specific Key Management Guidance, January 2015

SP 800-60: Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008

SP 800-61: Computer Security Incident Handling Guide,

August 2012 SP 800-63: Digital Identity Guidelines,

June 2017.

SP 800-63B: Digital Identity Guidelines—Authentication and Lifecycle

Management, June 2017. SP 800-64: Security Considerations in the System

Development Life Cycle, October 2008

SP 800-65: Integrating IT Security into the Capital Planning and Investment Control

Process, January 2005 SP 800-82: Guide to Industrial Control Systems (ICS) Security,

May 2015

SP 800-86: Guide to Integrating Forensic Techniques into Incident

Response, August 2006 SP 800-88: Guidelines for Media Sanitization,

December 2014

SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit

Generators, June 2015 SP 800-92: Guide to Computer Security Log Management, September

2006

SP 800-94: Guide to Intrusion Detection and Prevention Systems,

February 2007 SP 800-100: Information Security Handbook: A

Guide for Managers, October 2007

SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems

(PACS), December 2015 SP 800-122: Guide to Protecting the Confidentiality of Personally

Identifiable Information (PII), April 2010

SP 800-123: Guide to General Server Security, July 2008

SP 800-124: Guidelines for Managing the Security of Mobile Devices in the

Enterprise, June 2013 SP 800-125: Guide to Security for Full Virtualization

Technologies, January 2011

SP 800-125A: Security Recommendations for Hypervisor Deployment, September 2017

SP 800-130: A Framework for Designing Cryptographic Key Management Systems, August 2013

SP 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November 2015 SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, December 2011

SP 800-145: The NIST Definition of Cloud Computing, January 2011

SP 800-146: Cloud Computing Synopsis and Recommendations, May 2012

SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015 SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014

SP 800-163: Vetting the Security of Mobile Applications, January 2015

SP 800-164: Guidelines on Hardware-Rooted Security in Mobile Devices, October 2012 SP 800-177: Trustworthy Email, September 2017

SP 800-178: A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications, October 2016 SP 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview, June 2017

SP 1500-202: Framework for Cyber-Physical Systems: Volume 2, Working Group Reports, June 2017 SP 1800-3: Attribute Based Access Control, September 2017

SP 1800-4: Mobile Device Security: Cloud and Hybrid Builds, November 2015

ITU-T Documents

M.3400: Telecommunications Management Functions,

February 2000 X.816: Security Audit and Alarms

Framework, November 1995 X.1054: Governance of

Information Security, September 2012

X.1055: Risk Management and Risk Profile Guidelines for Telecommunication

Organizations, November 2008 X.1056: Security Incident Management Guidelines for

Telecommunications Organizations, January 2009 X.1205: Overview of Cybersecurity,

April 2014

ISO Documents

7498-2: Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture, February 1989

7498-4" : Open Systems Interconnection—Basic Reference Model—Part 4: Management

Framework, November 1989 27000: ISMS—Overview and Vocabulary, February 2016

27001: ISMS—Requirements, October 2013

27002: Code of Practice for Information Security Controls,

October 2013 27005: Information Security Risk

Management, June 2011

27014: Governance of Information Security, May 2013

27035-1: Information Security Incident Management—Part 1: Principles of Incident Management, November 2016

27035-2: Information Security Incident Management—Part 2:Guidelines to Plan and Prepare for Incident

Response, November 2016 29100: Privacy Framework, December 2011

This module has introduced students to the concept of Cybersecurity - Security Governance, frameworks, Information Security. It also focused on Security Management, Information Risk Assessment, Monitoring and best practices on improving security. Students are now well-equipped with the technical skills and knowledge required to manage organization’s network and protect them from security breaches and cyber threats.

The IT qualification at Richfield College stands as a beacon of academic innovation and professional readiness. It equips students with the skills and credentials necessary for thriving in the IT industry.
By combining foundational knowledge, practical expertise, and global recognition, the program not only prepares students for immediate employment but also sets them on a trajectory for long-term career success