WILLIAM STALLINGS

EFFECTIVE CYBERSECURITY

A Guide to Using Best Practices and Standards

Effective Cybersecurity

This page intentionally left blank

Effective Cybersecurity

Understanding and Using Standards and Best Practices

William Stallings

Addison-Wesley

Upper Saddle River, NJ • Boston • San Francisco • New York
Toronto • Montreal • London • Munich • Paris • Madrid
Cape Town • Sydney • Tokyo • Singapore • Mexico City

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2018941168

ISBN-13: 978-0-13-477280-6
ISBN-10: 0-13-477280-6

1 18

Executive Editor
Brett Bartow

Development Editor
Marianne Bartow

Managing Editor
Sandra Schroeder

Senior Project Editor
Lori Lyons

Copy Editor
Kitty Wilson

Project Manager
Dhayanidhi Karunanidhi

Indexer
Ken Johnson

Proofreader
Jeanine Furino

Technical Reviewers
Akhil Behl
Michael Shannon

Cover Designer
Chuti Praertsith

Compositor
codemantra

To Tricia, my loving wife,
the kindest and gentlest person.

This page intentionally left blank

Contents at a Glance

Appendix C (Online Only): Answers to Review Questions

You can find Appendix C at informit.com/title/9780134772806.
Click the Downloads tab to access the PDF file.

Table of Contents

Preface

There is the book, Inspector. I leave it with you, and you cannot doubt that it contains a full explanation.

—*The Adventure of the Lion's Mane*, by Sir Arthur Conan Doyle

Background

Effective cybersecurity is very difficult. 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 created a huge number of security publications, including 9 Federal Information Processing Standards (FIPS) and well over 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Equally important is the International Organization for Standardization (ISO) 27000 series of standards on information security management systems. Other organizations that have produced cybersecurity standards and guidelines include:

- **ISACA/COBIT:** The COBIT-5 for information security and related documents are widely used by the industry.
- **ITU Telecommunication Standardization Sector (ITU-T):** Most important are the series X.1050 through X.1069 on security management.
- **Internet Society (ISOC):** A number of published standards and RFCs relate to cybersecurity.

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* (SGP), produced by the Information Security Forum (ISF). This almost 300-page document provides a wide range of best practices based on the consensus of industry and government organizations. Another key organization is the Center for Internet Security (CIS), which has published detailed lists of industry-approved security controls and metrics. Other respected organizations have also produced a number of similar documents.

Thus, there is an immense amount of practical, widely accepted material available. The problem is that the amount of information is so massive that it is difficult for cybersecurity practitioners to take advantage of it to build and maintain effective cybersecurity systems and policies.

The objective of this book is to organize, consolidate, and explain all this material to enable the security practitioner to make effective use of it.

This book is addressed to people in both IT and security management, people tasked with maintaining IT security, and a wide range of others interested in cybersecurity and information security.

Organization of the Book

The book consists of three parts:

- **Part I, "Planning for Cybersecurity":** This part of the book provides guidelines for effectively managing the cybersecurity mission, including security governance and security requirements. The ISF defines *security governance* as "the framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently." Part I of this book provides guidance in developing a set of risk and security requirements to ensure that there are no gaps in an organization's cybersecurity practices.
- **Part II, "Managing the Cybersecurity Function":** This part of the book examines in detail the security controls intended to satisfy the defined security requirements. The 13 chapters in this part encompass the broad range of management, operational, and technical means used to achieve effective cybersecurity.
- **Part III, "Security Assessment":** This part of the book discusses techniques for auditing and monitoring the performance of cybersecurity controls, with a view to spotting gaps in the system and devising improvements.

Supporting Websites

The author maintains a companion website at WilliamStallings.com/Cybersecurity that includes a list of relevant links organized by chapter and an errata sheet for the book.

WilliamStallings.com/Cybersecurity
Companion website

The author also maintains the Computer Science Student Resource Site at ComputerScienceStudent.com. The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into seven categories:

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites.
- **How-to:** Provides advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations.
- **Research resources:** Provides links to important collections of papers, technical reports, and bibliographies.
- **Other useful:** Provides a variety of other useful documents and links.
- **Computer science careers:** Lists useful links and documents for those considering a career in computer science.

ComputerScienceStudent.com
Computer Science Student
Resource Site

- **Writing help:** Provides help in becoming a clearer, more effective writer.
- **Miscellaneous topics and humor:** You have to take your mind off your work once in a while.

Register This Book

Register your copy of *Effective Cybersecurity* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780134772806) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

Acknowledgments

This book has benefited from review by a number of people, who gave generously of their time and expertise. I especially thank Akhil Behl and Michael Shannon, who each devoted an enormous amount of time to a detailed review of the entire manuscript. I also thank the people who provided thoughtful reviews of the initial book proposal: Steven M. Bellovin, Kelley Dempsey, Charles A. Russell, Susan Sand, and Omar Santos.

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Sohail Awad, Vinay Banakar, Vilius Benetis, Rodrigo Ristow Branco, Michael Brown, Herve Carpentier, Jim Fenton, Adri Jovin, Joseph Kellegher, Adnan Kilic, Edward Lane, Junior Lazuardi, Matt Nichols, Omar Olivos, ShanShan Pa, Venkatesh Ramamoorthy, Antonius Ruslan, Jose Samuel, Jigar Savla, Matias Siri, and Dauda Sule. Nikhil Bhargava developed the review questions and answers.

Finally, I would like to thank the many people at Pearson responsible for the publication of the book. This includes the staff at Pearson, particularly Executive Editor Brett Bartow, Development Editor Marianne Bartow, and Senior Project Editor Lori Lyons. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in front of you.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all the quotations.

About the Author and Contributors

Dr. William Stallings has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking, and computer architecture. He has authored 18 textbooks, and, counting revised editions, a total of 70 books on various aspects of these subjects.

His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE* and *ACM Computing Reviews*. He has 13 times received the award for the best computer science textbook of the year from the Text and Academic Authors Association.

With more than 30 years in the field, he has been a technical contributor, a technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. Currently, he is an independent consultant whose clients have included computer and networking manufacturers and customers, software development firms, and leading-edge government research institutions.

He created and maintains the Computer Science Student Resource Site at ComputerScienceStudent.com. This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of *Cryptologia*, a scholarly journal devoted to all aspects of cryptology.

Dr. Stallings holds a Ph.D. from M.I.T. in computer science and a B.S. from Notre Dame in electrical engineering.

Technical Editors

Akhil Behl, CCIE No. 19564, is a passionate IT executive with a key focus on cloud and security. He has more than 15 years of experience in the IT industry, working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil is a published author. Over the past few years, Akhil has authored multiple titles on security and business communication technologies. He has contributed as a technical editor for more than a dozen books on security, networking, and information technology. He has published several research papers in national and international journals, including IEEE Xplore, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passions.

Akhil holds CCIE (Collaboration and Security), CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's in business administration.

Michael J. Shannon began his IT career when he transitioned from being a recording studio engineer to a network technician for a major telecommunications company in the early 1990s. He soon began to focus on security and was one of the first 10 people to attain the HIPAA Certified Security Specialist designation. Throughout his 30 years in IT, he has worked as an employee, a contractor, a trainer, and a consultant for a number of companies, including Platinum Technologies, Fujitsu, IBM, State Farm, Pearson, MindSharp, Thomson/NetG, and Skillsoft. Mr. Shannon has authored several books and training manuals, published articles, and produced dozens of CBT titles over the years as well. For security purposes, he has attained the CISSP, CCNP Security, SSCP, Security+, and ITIL Intermediate SO and RCV certifications. He is also a licensed insurance agent, specializing in cyber insurance on behalf of large insurers and numerous companies throughout Texas.

Chapter 2

Security Governance

A prince or general can best demonstrate his genius by managing a campaign exactly to suit his objectives and his resources, doing neither too much nor too little. But the effects of genius show not so much in novel forms of action as in the ultimate success of the whole.

—*On War*, Carl Von Clausewitz

Learning Objectives

After studying this chapter, you should be able to:

- 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.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, defines information security governance as follows:

> **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.

2.1 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.

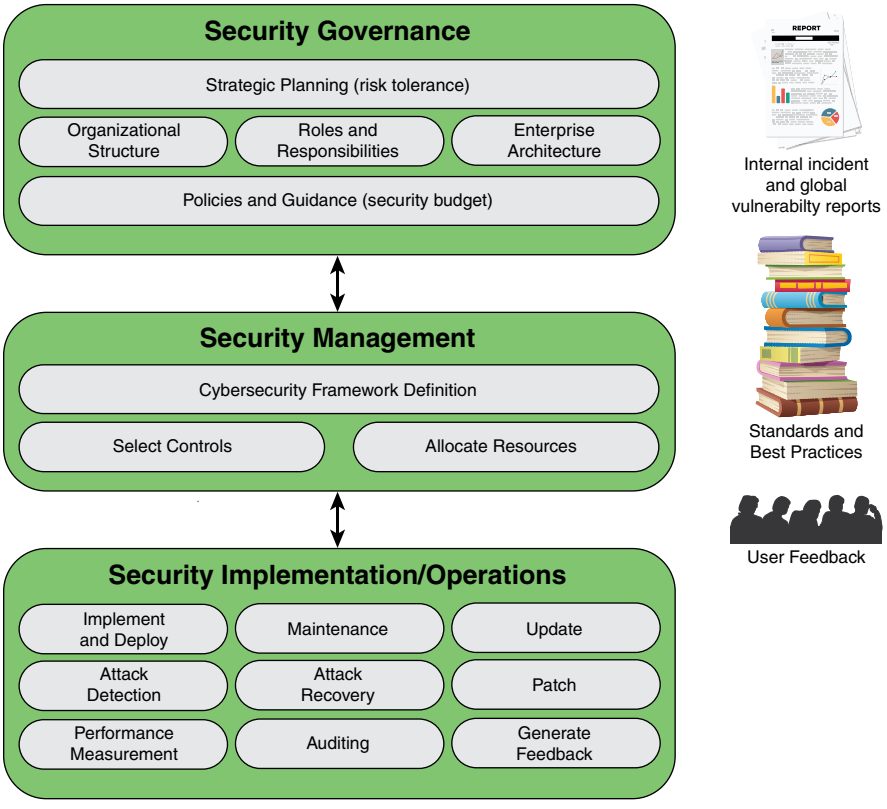

FIGURE 2.1 Information Security Management System Element

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.

This chapter is devoted to security governance. Chapter 3, "Information Risk Assessment," covers security management, and the succeeding chapters cover security implementation/operations.

2.2 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.
- **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

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.

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.

should take the lead in promoting a positive information security culture, which includes requiring and supporting security education, training, and awareness programs.

- **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.

2.3 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.

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

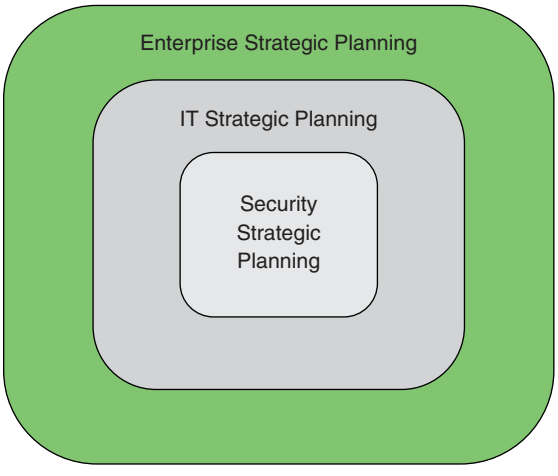

FIGURE 2.2 Strategic Planning

Enterprise strategic planning involves defining long-term goals and objectives for an organization (for example, business enterprise, government agency, or nonprofit

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.

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.

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 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.

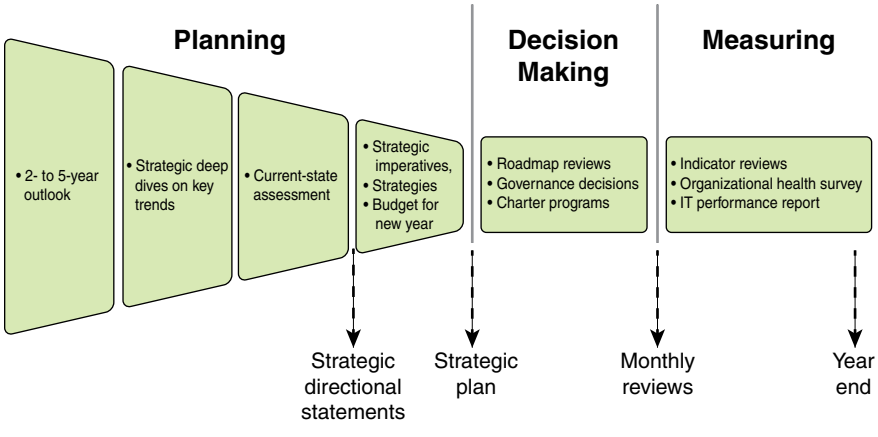

FIGURE 2.3 Intel's IT Strategic Planning Process

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.

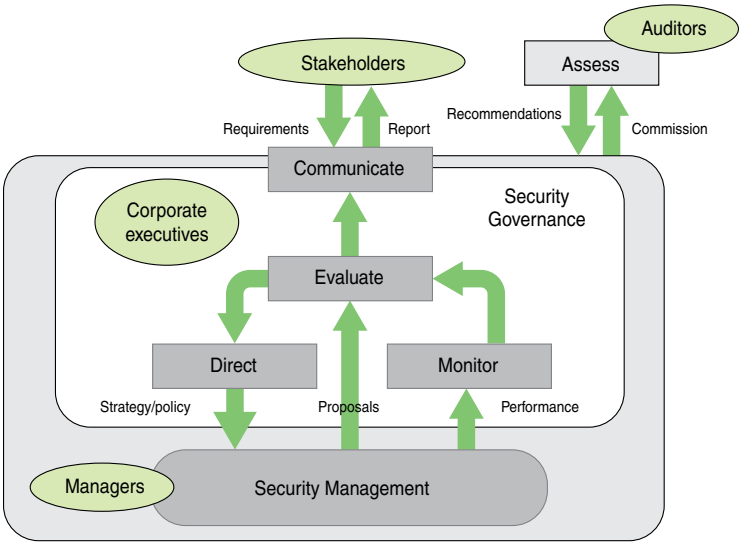

FIGURE 2.4 Framework for Security Governance

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 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.

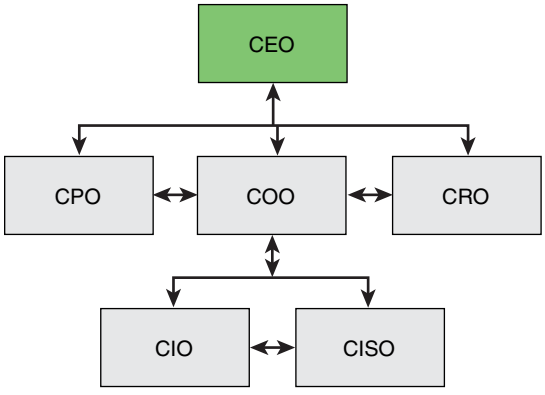

FIGURE 2.5 Possible Reporting Relationships for Security Governance

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.

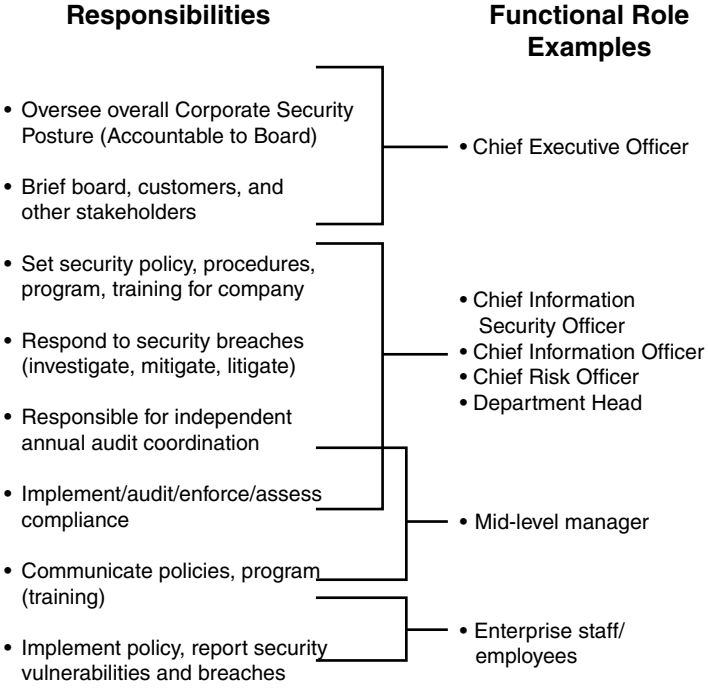

FIGURE 2.6 Security Governance Roles and Responsibilities Example

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?

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 environment activities, remedial actions, policy and procedure compliance, security and control test results

Governance/ Business Drivers	Roles and Responsibilities	Metrics/Audit
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

Integration with Enterprise Architecture

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.

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.

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.

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

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

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.

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

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

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

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 illustrates the interactions among the reference models.

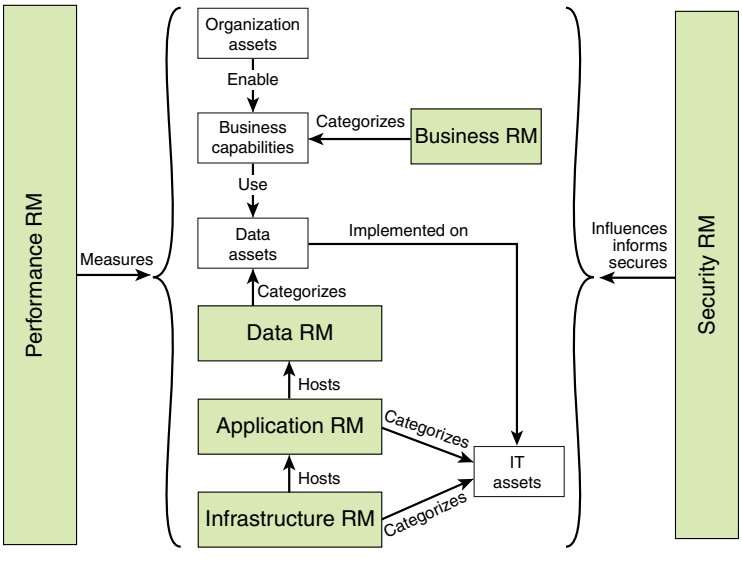

FIGURE 2.7 Relationships Between RM Components

These reference models operate on four categories of assets:

- **Organization assets:** These assets include investments, programs, processes, applications, infrastructures, and individuals.
- **Business capabilities:** A business capability represents the ability of an organization to perform an activity that results in an outcome of value. A business capability can be viewed as an assembly of organization assets for a specific purpose.
- **Data assets:** Data assets include databases, files, and other data resources available to the organization.
- **IT assets:** IT assets include devices, peripherals, systems, applications, and IT capital investments.

Figure 2.8 shows in more detail the interaction between the security reference model and the other reference models.

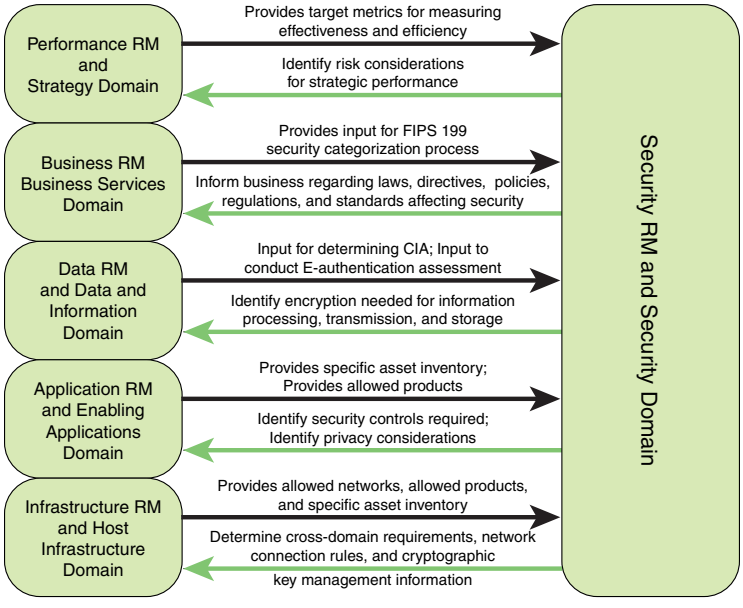

FIGURE 2.8 Interactions Between the Security Reference Model and Other Reference Models

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.

2.4 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:
  - Establishing and maintaining an ISMS
  - Defining and managing an information security risk treatment plan
  - 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

2.5 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 Chapter 3. 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.

2.6 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.

2.7 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

architecture
C-level
chief executive officer (CEO)
chief information officer (CIO)
chief information security officer (CISO)
chief operating officer (COO)
chief privacy officer (CPO)
chief risk officer (CRO)
chief security officer (CSO)
enterprise architecture
enterprise risk management (ERM) committee
Federal Enterprise Architecture Framework (FEAF)
governance
information security architecture
information security governance
information security implementation/operations
information security steering (ISS) committee
information security management
information security strategic planning
information technology (IT)
IT strategic planning

RACI chart
security governance
security implementation/ operations
security management
security program
stakeholder
strategic plan

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

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.

2.8 References

BSA03: Business Software Alliance, *Information Security Governance: Toward a Framework for Action.* 2003. https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf

CGTF04: Corporate Governance Task Force, *Information Security Governance: A Call to Action.* U.S. Department of Homeland Security, 2004.

EAPA17: The EA Pad. *Basic Elements of Federal Enterprise Architecture.* https://eapad.dk/gov/us/common-approach/basic-elements-of-federal-enterprise-architecture/

HAYD08a: Haydamack, C., "Strategic Planning Processes for Information Technology," *BPTrends*, September 2008.

HAYD08b: Haydamack, C., & Johnson, S., *Aligning IT with Business Goals Through Strategic Planning.* Intel Information Technology White Paper, December 2008.

ISAC08: ISACA, *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*. 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

JOHN09: Johnston, A., & Hale, R., "Improved Security Through Information Security Governance." *Communications of the ACM*, January 2009.

JUIZ15: Juiz, C., & Toomey, M., "To Govern IT, or Not to Govern IT?" *Communications of the ACM*, February 2015.

OHKI09: Ohki, E., et al., "Information Security Governance Framework." *First ACM Workshop on Information Security Governance (WISG)*, November 2009.

OMB13: Office of Management and Budget, *Federal Enterprise Architecture Framework.* 2013.

PETE12: Peters, C., & Schuman, B., *Achieving Intel's Strategic Goals with IT.* Intel Information Technology White Paper, February 2012.

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.

TOG11: The Open Group, *The Open Group Architecture Framework (TOGAF).* 2011. http://www.opengroup.org/subjectareas/enterprise/togaf

ZIA15: Zia, T., "Organisations Capability and Aptitude Towards IT Security Governance." *2015 5th International Conference on IT Convergence and Security (ICITCS)*, August 2015.

Index

Numbers

A

B

C

D

E

F

G

H

I

J - K

L

M

N

O

P

Q

R

S

T

U

V

W

X - Y - Z